Personal Data Protection and Security: What are the Issues You Need to Know?

February 27, 2008

Association of Corporate Counsel
Québec Chapter

ACC CANADA
Association of Corporate Counsel

OSLER

Welcome

- **Anita Fineberg**, Corporate Counsel and Chief Privacy Officer, IMS HEALTH Canada and Latin America
  afineberg@ca.imshealth.com – Tel: (905) 816-5080/816-5000

- **Caroline Poirier**, Senior Legal Counsel and Chief Privacy Manager, Emergis - a Telus Company
  Caroline.Poirier@emergis.com – Tel: (450) 928-6387

- **Michel Généreux**, Osler (Montréal)
  mgenereux@osler.com – Tel: (514) 904-5370

- **Patricia Wilson**, Osler (Ottawa)
  pwilson@osler.com – Tel: (613) 787-1004

Today

- Overview of relevant legislation in Canada – Pat
- 5 current issues:
  - M&A transactions – Pat & Michel
  - Cross-border data flow – Pat & Michel
  - Contractual aspects – Caroline
  - Breach and notification – Anita
  - Employee related – Pat

Overview of relevant legislation in Canada

- Canada has eight (8) privacy laws that apply to the private sector:
  - four (4) general privacy laws (PIPEDA, QPPIPS, B.C./ Alta. PIPAs)
  - four (4) personal health information laws (Ontario PHIPA, Alta. HIA; Sask. HIPA; Man. PHIA
- Non-exclusive application and co-extensive jurisdiction complicate compliance

Overview of relevant legislation in Canada

- Québec *Act Respecting the Protection of Personal Information in the Private Sector* (QPPIPS) and privacy provisions in the Québec *Civil Code* enacted in 1994
- *Personal Information and Electronic Documents Act* (PIPEDA) enacted in 2001 (applied to federal sector organizations) and applied to all organizations in commercial activity as of 2004

Overview of relevant legislation in Canada

- QPPIPS declared "substantially similar" to PIPEDA in 2003:
  - QPPIPS applies, and PIPEDA does not apply, within Québec
  - Québec A.G. launches reference challenging federal authority to enact PIPEDA with application within provinces
  - QPPIPS has extra-territorial application in respect of transfers outside Québec

Overview of relevant legislation in Canada

- PIPEDA applies:
  - Within Québec to federal works, undertakings or businesses
  - To inter-provincial and trans-border transfers in the course of commercial activity

Overview of relevant legislation in Canada

QPPIPS / Québec Civil Code Overview

- Civil Code establishes civil right of action for privacy breaches
  - Specific rights to notification of purposes for collection, consent to disclosure and access to personal information
  - Provides protection against misappropriation of personality

Overview of relevant legislation in Canada

QPPIPS Overview (cont'd)

- QPPIPS provides statutory regime for privacy compliance by organizations, access rights and complaint investigation and enforcement by the *Commission d'accès à l'information*
- Applies to information about identifiable individuals
- Requires legitimate purposes and clear, specific notice for collecting personal information
- Requires manifest, free, enlightened and specific consent to disclosure of personal information, with limited exceptions (allows opt-outs for marketing purposes)

Overview of relevant legislation in Canada

QPPIPS Overview (cont'd)

- Prohibits tied consent
- Limits collection and use to that relevant to the purposes
- Requires accuracy, limited retention and security
- Establishes rights of access to and correction of personal information, with limited exceptions

Overview of relevant legislation in Canada

QPPIPS Overview (cont'd)

- Applies to "enterprises"
    - limits use within enterprises and by mandataries to that necessary for stated purposes
- Limits disclosure or transfer outside Québec to situations where disclosure to third parties without consent will not occur except as allowed by QPPIPS
- Enforced by the *Commission d'accès à l'information* – Order making authority
- Offences for breach up to $100,000

Overview of relevant legislation in Canada

PIPEDA Overview

Based on CSA Model Code for the Protection of Personal Information – 10 Principles

- Applies to information about identifiable individuals
- Requires appointment of Privacy Officer and adoption of Privacy Policies
- Specific provision for transfers to service providers (no consent required) and contractual protection of p.i.

Overview of relevant legislation in Canada

PIPEDA Overview (cont'd)

- Requires appropriate purposes and specific, clear notice of purposes for collection of p.i.;
- Consent required for collection, use and disclosure of p.i.; allows for implied consent based on sensitivity of p.i. and expectations of individual, with limited exceptions
- Prohibits tied consent

Overview of relevant legislation in Canada

PIPEDA Overview (cont'd)

- Requires accuracy, limited retention and security
- Provides rights of access and correction, with limited exceptions
- Enforced by Privacy Commissioner of Canada through complaint investigations – PCC can make recommendations only
- PCC has audit powers based on grounds for suspecting non-compliance

Overview of relevant legislation in Canada

PIPEDA Overview (cont'd)

- Rights to review by the Federal Court –broad order making authority; damages remedy (including unlimited damages for mental distress)
- Limited offences in PIPEDA (retaliation against whistleblowers and destruction of p.i. that is subject to an access request) – fines up to $100,000 on indictment

M&A transactions

B.C./ Alta. PIPAs

- No consent required in respect of "necessary" p.i. for third party analysis
- NDA with third party limiting collection, use and disclosure of p.i. to transaction context
  notice of transfer must be given after closing
- *caveat*: sale of p.i. as a primary asset

M&A transactions

PIPEDA

- Currently silent + implied consent
- Considering amendments in line with provincial PIPAs
- Current approach (if no express consent):
  - NDA: collection, use and disclosure limited to transaction
  - p.i. to be returned if no transaction
  - clients to be informed ex post facto
- *caveat*: sale of p.i. as a primary asset

M&A transactions

QPPIPS

- Currently silent
- “manifest” and “specific” consent requirement
- Possible approaches:
  - obtaining express consent in advance
  - anonymizing data
  - hiring third party to review p.i. “on behalf of purchaser” (Section 20 QPPIPS)
- Post-transaction

Cross-border data flow

PIPEDA

- Objective: principle 4.1.3 – requirement to “use contractual or other means to provide a comparable level of protection”
- Patriot Act not a bar to transfer – s. 7(3)(c) PIPEDA
- Appropriate contractual provisions with third party: control, audit, retrieval and destruction
- Principle 4.8 – transparency

Cross-border data flow

Personal health information laws

- Ont., s.50 – can’t disclose without consent
- Alb., s. 107(5.1) – offence for disclosure to foreign law enforcement or third party without consent

Cross-border data flow

QPPIPS – Section 17

- Must first:
  - Take all reasonable steps to ensure that p.i. will only be used for purpose and not be communicated to t.p. without consent of individual or as contemplated by QPPIPS
  - In case of lists, provide persons concerned with opportunity to refuse that p.i. be used for purposes of commercial or philanthropic prospection / have p.i. deleted from the list

Cross-border data flow

QPPIPS – Section 17

- If consider that p.i. will not receive this protection, must refuse to communicate outside Québec
- Increased fines (up to $100,000 for 2nd offences (s.91))
- Target: Patriot Act
- s.18(2)(3)(4)(6) QPPIPS vs. s. 7(3)(c) PIPEDA
- Constitutionnal issue

Contractual aspects

- It all started with:

  " Each party shall be responsible to comply with applicable privacy laws… "

- Has now evolved to:

  Detailed description of each party's rights and obligations for the collection, usage and disclosure of personal information

Contractual aspects – Areas of discussion

- Valid consent for usage and/or disclosure of personal information (« chain of consent »)
- Level of security
- Liability with respect to privacy obligations (limited vs. unlimited)
- Dedicated systems vs. shared environment
- Audit
- Training of employees (customized or not)

Contractual aspects – Areas of discussion

- Usage of personal information data within testing and/or development environments
- Usage of subcontractors
- Signature of confidentiality agreement directly between service providers' employees and customer
- Privacy policies and practices
- Disaster recovery
- Territorial limitation

Breach and notification – Outline

- The issues
- Current legislation and guidelines
- Futures

Breach and notification – The issues

- The Question:
  - What are the obligations of an organization to notify: (i) affected individuals; and (ii) privacy regulators in the event that personal information in its custody or under its control is subject to unauthorized use, disclosure or modifications?

- Key Elements:

(1) Notification Trigger:

  - Individuals – primary purpose is to enable them to mitigate risk of harm that might result from a breach
  - Regulatory Authorities – primary purpose is to enable authorities to identify persistent or systemic problems and take necessary action to address them

Breach and notification – The Issues

- Key Elements (cont'd)

(2) Definition of Specified Personal Information

  - The types of information that could be used to cause "significant harm"
    - Identifiable, unencrypted that includes an individual's name together with one or more sensitive data elements (e.g. financial account information, SSN, medical insurance number

(3) Risk Determination

  - Assessment of the circumstances surrounding the incident
    - The causes of the breach
    - Potential for high risk of significant harm

Breach and notification – The Issues

- Key Elements (cont'd)

  (4) Timing and Method of Notification

  - Individuals:
    - as soon as reasonably possible following assessment and evaluation of the scope and nature of the breach, remedying any ongoing breach and identifying potentially affected individuals
    - flexible with respect to the method of notification, dependent upon circumstances re: the organization's relationship, if any, to the affected individuals, the manner in which the organization typically communicates with them, and the type and scope of the breach
  - Regulatory Authorities
    - Should reflect agency needs but not be so burdensome so as to cause delay in notifying individuals

Breach and notification – Current legislation and guidelines

- Ontario's *Personal Health Information Protection Act, 2004* (PHIPA)
  - Only Canadian legislation mandating breach notification
  - S.12: …a health information custodian that has custody or control of personal health information about an individual **shall notify** the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized individuals
  - Features:
    - Mandatory in all cases-> no 'notification trigger'
    - No direction on method of notification or 'drill down' of 'first reasonable opportunity'
    - No obligation to notify the Privacy Commissioner's Office
  - Commissioner's Office has issued *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector* http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf

Breach and notification – Current legislation and guidelines (cont'd)

- B.C. Resources for Business and Organizations
  - Key Steps in Responding to Privacy Breaches
    http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf
  - Privacy Breach Reporting Form (to the Commissioner's Office)
    http://www.oipc.bc.ca/forms/Privacy_Breach_Form_(Dec_2006).pdf
  - Breach Notification Assessment Tool (jointly produced with the Ontario Commissioner's Office)
    http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf
  - Key Steps for Physicians in Responding to Privacy Breaches
    http://www.oipc.bc.ca/pdfs/private/PhysicianKeyStepsPrivacyBreach.pdf

Breach and notification – Current legislation and guidelines (cont'd)

- Alberta
  - Key Steps in Responding to Privacy Breaches
    http://www.oipc.ab.ca/ims/client/upload/Key%20Steps%20in%20Responding%20to%20a%20Privacy%20Breach%202007.pdf
  - Reporting a Privacy Breach to the Office of the Information and Privacy Commissioner of Alberta
    http://www.oipc.ab.ca/ims/client/upload/Reporting%20Privacy%20Breaches%20to%20OIPC%202007.pdf
  - Both are adapted from the joint B.C./Ontario documentation

Breach and notification – Current legislation and guidelines (cont'd)

- Federal
  - Privacy Breach Guidelines

    http://www.privcom.gc.ca/information/guide/2007/gl_070801_01_e.asp
  - Key Steps for Organizations in Responding to Privacy Breaches
    http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp
  - Privacy Breach Checklist

    http://www.privcom.gc.ca/information/guide/2007/gl_070801_checklist_e.asp

Breach and notification – Futures

- Government consultations on the review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)
  - Government proposal:

    (1) Notification Trigger
    - That there be different notification thresholds for individuals and the authorities
      - Notification to individuals should occur when there is a high risk of significant harm from loss or theft of personal information
      - Privacy Commissioner should be notified in the event of any major loss or theft of personal information within a specified time-frame to allow for oversight of organizational practices and enable the Commissioner to track the volume and nature of breaches and steps taken by organizations
    - Commissioner *should not* have the responsibility to decide when notification should be given
      - Organizations are better positioned to understand/assess risks and make a prompt determination regarding whether and how to notify customers, business partners and/or the general public

Breach and notification – Futures

- Government proposal – (cont'd):
  - (2) Definition of Specified Personal Information
    - None provided but the Federal Privacy Commissioner's Guidelines are generally in line with the approach outlined in the issues
  - (3) Risk determination
    - None provided but the Federal Privacy Commissioner's Guidelines are in line with the approach outlined in the issues
  - (4) Timing and method of notification
    - None provided but guidelines of the Federal Privacy Commissioner generally reflect the desired flexibility
- Current status
  - Submissions deadline was January 15/08
  - All are posted on the website
  - Industry Canada likely to hold in-person stakeholder consultations on the issue

Breach and notification – Futures

- Alberta:
  - Government's response to the Select Special *Personal Information Protection Act* Review Committee Report recommendation:
    - Provide a framework within the Act for organizations to report certain privacy breaches to the Office of the Information and Privacy Commissioner and, if necessary, affected individuals, as well as an offence provision for failure to report a breach
- B.C.
  - Consideration of whether the issue will arise in the ongoing Statutory Review of the *Personal Information Protection Act*
- Ontario
  - Will the mandatory nature of s.12 of PHIPA be reconsidered in the legislative review which was to commence November 2007?

Employee related issues

- QPPIPS applies to employee p.i.; PIPEDA applies to employee p.i. in federal businesses only
- Consent requirement is difficult to apply to employees
  - when is implied consent appropriate
    - transactions
    - outsourcing of human resources functions
  - Alberta/ British Columbia PIPA approach is appropriate

Employee related issues

- How to handle employee refusals to consent
  - prohibition against tied consent in QPPIPS (not in PIPEDA)
- Permissible employee verification and monitoring
  - e-mail and internet use, video surveillance
  - employee identification
  - disability management and return to work

Questions?

Personal Data Protection and Security: What are the Issues You Need to Know?

February 27, 2008

Association of Corporate Counsel
Québec Chapter

ACC CANADA
Association of Corporate Counsel

OSLER