“What You Need To Know About Privacy – Now!”

April 27, 2011

Presented by: Catherine Coulter

Update on Federal Privacy Law

What Laws Apply To Your Association?

- *Personal Information Protection and Electronic Documents Act* (PIPEDA) – private sector employer or federal work or undertaking (eg. banks, telecoms, railways)
- *Privacy Act* – Federal government departments and agencies
- *Personal Health Information Protection Act* ("PHIPA") – Ontario health information custodian

* Remember that PIPEDA only applies to personal information in connection with "commercial activities". Therefore, many non-profit organizations are not subject to PIPEDA because they do not engage in commercial activities

Update on Federal Privacy Law:

Proposed amendments to PIPEDA which recently died when Parliament prorogued included the following:

- mandatory reporting of material breaches to the Privacy Commissioner
- mandatory reporting of breaches to individuals where there is a real risk of significant harm
- Business Transaction exemption
- expanded carve-out of the definition of business contact information

Update on Federal Privacy Law:

Case Summary #2010-003:

- Requests for access to personal information are time-sensitive. Where an organization requires more than 30 days to fulfill the request, it must advise the individual of same, advise of the new time limit, advise of the reasons for the extension and advise the individual of his/her right to make a complaint to the Commissioner regarding the extension
- Whenever requests are made, organizations should ensure that the requested information is not deleted during the request period due to the organization's regular deletion/retention practices

Update on Federal Privacy Law:

Case Summary #2010-013:

- Unless and until the PIPEDA amendments are brought forward again and passed into legislation, business email addresses remain as personal information
- As a result, business email addresses may not be collected, used or disclosed unless they are publicly available
- If business email address lists are rented or purchased, care must be taken to ensure that they were collected with consent

Privacy in Corporate Transactions

Privacy in Corporate Transactions:

- Both *PIPA Alberta* and *PIPA B.C.* contain provisions which permit necessary personal information to be disclosed without consent for the purpose of a business transaction (the "Business Transaction exemption")

- Some of the recent proposed amendments to PIPEDA were aimed at adding a Business Transaction exemption to PIPEDA, but the Bill recently died when Parliament prorogued

Privacy in Corporate Transactions:

- In a finding of the Alberta Privacy Commissioner, employee personal information was submitted from one law firm to another as part of the due diligence process during an acquisition. Some of the information provided went above and beyond that required for due diligence purposes. In addition, the receiving law firm posted that information to the Systems for Electronic Document Analysis and Retrieval (SEDAR).
- The Commissioner found that: (i) the Business Transaction exemption did not apply to all of the transferred information (eg. home addresses, SIN's) and therefore there was a contravention of the legislation; and (ii) Stikeman Elliott had a duty to review the received information before publicly posting it to SEDAR
- If personal information will be disclosed in an Ontario business transaction, obtain consent first!

Privacy in Corporate Transactions:

Example consent paragraph in employment agreements:

> By accepting this offer, you voluntarily acknowledge and consent to the collection, use, processing and disclosure of personal data as described in this paragraph. The Company will hold certain personal information which may include your name, home address, home telephone number, date of birth, social insurance number, employee identification number, compensation, payroll deposit account, job title, attendance and work record, marital or family status, name of your spouse and dependents (if any), contribution rates and amounts, account balances, benefit selections and claims for the purpose of: (i) establishing, managing and/or terminating the employment relationship between you and the Company; (ii) making payroll deposits, preparing tax reports or administering benefit entitlements; or (iii) contacting others in the event of an emergency ("Data"). The Company, in accordance with its standard operating procedures, may disclose Data to its affiliates or with contracted third party outsourced services or benefit providers as necessary, for the purpose of human resources, payroll, retirement and benefit administration. The Company may also disclose Data to third parties for the purposes of exploring and carrying out mergers, acquisitions, financings, initial public offerings or similar transactions.

Canada-USA Cross-Border Data Transfers

Federal Privacy Commissioner Guidelines

- PIPEDA does not distinguish between domestic and international transfers of data
- An organization is responsible for personal information in its possession, including information that has been transferred to a third party for processing
- Where information is transferred for processing, it can only be used for the purposes for which the information was originally collected; for example, internet service provider transfers personal information to third party to ensure technical support is available 24/7
- A transfer for processing is not a disclosure; it is a use

Federal Privacy Commissioner Guidelines

- Processing means any use of the information by the third party processer for which the transferring organization can use it
- Comparable level of protection means that the third party processor must provide protection that can be compared to the level of protection the data would have received if it had not been transferred
- Primary means to protect personal information is through contract

Best Practices

- Be satisfied that the third party has policies and processes in place, including training and effective security measures, to ensure the data in its care is properly safeguarded
- Set out requirements for safeguards in written contract
- Retain the right to audit and inspect
- Assess risk when transferring outside of Canada

Best Practices

- Pay attention to the legal requirements of the jurisdiction in which the third party processor operates as well as the potential foreign, political, economic and social conditions and events that may reduce the service provider's ability to provide the service
- Make it clear to individuals that their information may be processed in a foreign country and it may be accessible to law enforcement and national security authorities
- Use clear and understandable language
- Ideally do so at the time the information is collected

Breach Notification

Breach Notification:

- If your organization finds itself in a breach situation:

  - work with experienced legal counsel to determine your course of action
  - with reference to the applicable legislation, also keep an eye on the federal Privacy Commissioner's breach Guidelines and the accompanying Privacy Breach Checklist and Privacy Breach Incident Report:

    http://www.priv.gc.ca/information/guide/index_e.cfm

Breach Notification:

Personal Health Information Protection Act (Ontario):

- Under PHIPA, there is also a positive obligation to notify affected individuals in circumstances where the privacy of their personal health information has been compromised. The obligation applies only to "health information custodians" (eg. hospitals, labs, doctors) but is required in every case of breach.

Breach Notification:

- The following are some of the key points to consider when dealing with a breach of personal information:

  (i) Contain the breach and conduct a preliminary assessment

  (ii) evaluate the risks associated with the breach (ie. the nature of the personal information involved; cause and extent of breach; individuals affected; foreseeable harm)

  (iii) Notify affected individuals if the breach "creates a risk of harm" to them

  (iv) Notify appropriate privacy commissioners of material breaches so that they are aware of the situation

  (v) Consider whether other notifications are also appropriate (eg. police, financial institutions, insurers, regulatory or professional bodies)

  (vi) Work to prevent similar future breaches

Late Breaking Developments

"Ontario court this week ruled that employees have a right to privacy for material contained on a work computer"

R. v. Cole, Ont. C. of A., March 22, 2011

- public sector employer governed by Charter
- pornography on school computer
- employee's Charter s. 8 rights (no unreasonable search or seizure) not breached by school technician, principal, school board
- warrantless police search and seizure of laptop breached s. 8

"No common law tort for invasion of privacy: Judge"

Jones v. Tsige, Ont. SCJ, March 23, 2011

- Bank employee, WT, accessed bank records of customer for purely personal reasons
- Court reviewed contradictory decisions
- concluded no free-standing right to privacy at common law
- relied on 2005 OCA decision involving complaint against police and Charter rights.

Thank you.

Questions?

MONTRÉAL

OTTAWA

TORONTO

EDMONTON

CALGARY

VANCOUVER