“10 Things You Need To Know About Privacy”

April 5, 2011

Presented by: Catherine Coulter & Anneli LeGault

Update on Federal Privacy Law

Update on Federal Privacy Law:

- Proposed amendments to PIPEDA 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:

Recent PIPEDA Findings:

Case Summary #2010-001:

- The Commissioner will not make findings if she is satisfied that the complaint can more appropriately be dealt with by means of a procedure otherwise provided for at law
- Individuals who have been denied access to their personal information due to solicitor & client privilege must use court proceedings to obtain a ruling on the appropriateness of the privilege claim (follows S.C.C. ruling in *Blood Tribe* (2008))

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 #2010-018:

- Personal information which has been de-identified (had all personally indentifying information removed) does not qualify as anonymous information if it is still possible to link the de-identified data back to an identifiable individual
- An access request for personal information does not grant the requester the right to information that reflects discussions taken in preparation for possible litigation

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

Provincial Privacy Law – What to Watch Out For With Substantially Similar Legislation

Provincial Privacy Law:

Quebec – An Act Respecting the Protection of Personal Information in the Private Sector (1994)

- Similar to PIPEDA
- Applies to all enterprises in Quebec
- Covers information in the private sector, including health information
- Violations of the Act are punishable by fines ranging from $1,000 to $10,000 for a first offence, and $10,000 to $20,000 for subsequent offences
- Binding orders by the Commissioner are permitted

Provincial Privacy Law:

Quebec – An Act Respecting the Protection of Personal Information in the Private Sector (1994)

- Those binding orders can be made into binding orders of the provincial court
- Offending parties are generally named in any published findings

Provincial Privacy Law:

Alberta – Personal Information Protection Act ("PIPA")

- Similar to PIPEDA
- Separate legislation for personal health information (Health Information Act, 2001)
- Under PIPA Alberta, there is a class of non-profit organizations for which the legislation only applies to their commercial activities
- Under PIPA Alberta, there are special provisions for professional regulatory organizations to follow an approved privacy code in place of certain sections of the legislation

Provincial Privacy Law:

Alberta – Personal Information Protection Act ("PIPA")

- Binding orders by the Commissioner are permitted
- Those binding orders can be made into binding orders of the provincial court
- Offending parties are generally named in any published findings
- Violations of the Act are punishable by fines

Provincial Privacy Law:

B.C. – Personal Information Protection Act ("PIPA")

- Similar to PIPEDA
- Extremely similar legislation to PIPA Alberta, but for the following:
  - Commissioner has audit powers
  - no provision for the filing of the Commissioner's orders in provincial court and having them enforced as orders of that court
  - Actions only permitted for "actual damages" suffered

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
- In an early finding of the Alberta Privacy Commissioner, customer personal information was disclosed to a purchaser without consent during the course of the transaction. Although the disclosure was found to be in compliance with the legislation, the Commissioner noted that all business transaction agreements should specifically address the anticipated use of any transferred personal information, and parties should only undertake to use personal information for the purpose for which it was collected

Privacy in Corporate Transactions:

- In a subsequent 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

Privacy in Corporate Transactions:

For business transactions in Alberta or B.C.:

- Determine whether or not the information sought to be collected, used or disclosed meets the Business Transaction exemption
- Only use or disclose that information for the same purpose for which it was collected
- If the above is not possible, obtain consent

For business transactions in Ontario and elsewhere:

- Obtain consent

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.

Cross-border Data Flow

Obligations of a Canadian organization

- Accountability
- Safeguards
- Openness

Typical Cross Border Scenarios

- Storage of data on servers in USA – e.g. SAP installation
- Email service provider has no Canadian data centre
- SPAM service provider located in USA or UK
- Email run through USA
- Data processed in USA
- Bidding on government work, for example, in BC and NS

Risk Levels

European Union

USA

Non-APEC or non-OECD member countries

European Union

- EU member states have passed Data Directives prohibiting transfer of personal information to another jurisdiction unless the European Commission has determined that the other jurisdiction offers adequate protection

United States

- US Patriot Act
- Section 215 allows FBI to access records held in USA by applying for an order of the *Foreign Intelligence Surveillance Act* Court
- Company subject to a Section 215 order cannot reveal that the FBI has sought or obtained information from it
- US has Safe Harbor accord with EU (2000)
  - Companies can opt in
- US has sector specific laws and some US states have enacted laws

APEC/OECD Member Countries

- Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) – 31 member countries
- Asia – Pacific Economic Cooperation Privacy Framework (2004) – 21 member countries

Rulings Concerning Canada-USA Cross-Border Data Transfers

British Columbia

- BCGEU v. The Minister of Health Services and Maximus
- US Company, Maximus, selected by B.C. Ministry of Health Services for administration of B.C.'s public health insurance program
- BCGEU files complaint under FOIPPA
- Personal health information of B.C. residents accessible to US authorities under US Patriot Act

British Columbia (cont'd)

- Privacy Commissioner initiates public process
  - >500 submissions received
- FOIPPA amended to require a public body to ensure that personal data under its control is stored only in Canada and accessed only in Canada (with certain exceptions)
- New requirement to report any foreign demand for disclosure to Minister

Alberta

- Outsourcing email services to Google
- University of Alberta spends a year investigating the possibility of a single campus email system using Google's Gmail
- Users of University email system must be informed that their emails will reside in a foreign jurisdiction and be subject to the laws of that jurisdiction such as US Patriot Act
- U of A agrees to inform students and employees it cannot guarantee protection against disclosure of emails residing in US

Alberta PIPA amended May 1, 2010

- Duty to notify individual if a service provider outside of Canada will collect PI or PI will be transferred to service provider
  - Written or oral notice re:
    - how to access information about company's policies/practices on non-Canadian service providers
    - name or title of person who can answer questions

Use of Service Provider in USA – Ruling 313

- VISA credit card information to be processed in US
- Canadian customer data stored on U.S. based software system
- VISA cardholder agreement amended
- No opt-out
- US authorities may access the data

Ruling 313 (cont'd)

- Ruling:
  - Bank had contract with U.S. data processor to maintain comparable level of security and protection
  - Bank appropriately notified customers

Security System Provider Shares Customer Data – Ruling 333

- Security system company tells Canadian customers of intention to share customer contact information with U.S. parent company
- If catastrophic event overwhelms Canadian customer monitoring centre, alarm signals routed to other North American monitoring centre
- Sharing of customer address, phone, emergency contacts
- No sharing of financial or credit data
- Customers could opt out and get reduced level of service

Ruling 333 (cont'd)

- Ruling:
  - Customer consent not required, not a disclosure
  - Personal data being used for same original purpose
  - Company was transparent and provided sufficient information about practices
  - Parent company must adhere to same level of data protection

Outsourcing – Ruling 394

- "canada.com" outsourcing e-mail services to U.S. based company
- Customers requested to consent as condition of on-going services
- *U.S. Patriot Act* issues

Ruling 394 (cont'd)

- Ruling
  - Sharing with a third-party subcontractor is a "use" not a "disclosure"
  - Consent is required to the use
  - Best practice is to notify
  - Must take contractual measures to ensure security
    - oversight
    - monitoring
    - auditing
  - Should provide notice that foreign-based service provider will be subject to foreign laws, which may be different than Canadian law

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

Best Practices

- When bidding on a RFP involving data processing and storage, review the bid's terms and be ready to explain where data will be stored and processed

Privacy Remedies & Risks – What's Your "Real" Exposure?

What are the Remedies and Risks?

Under PIPEDA:

1. Investigations & Findings

2. Section 14 Applications

3. Judicial Review

1. Investigations:

- Investigator will require a response from your organization
- Employees may be interviewed without your consent
- Company files may be requested
- Through the Privacy Commissioner, investigators have the authority to receive evidence, enter premises where appropriate and obtain copies of records
- After the investigator prepares a report, the Privacy Commissioner will make a finding

Investigations:

- The Privacy Commissioner can make the following findings:
  - Not Well-Founded
  - Well-Founded
  - Resolved
  - Discontinued
- The Commissioner can make recommendations to your organization and ask you to respond in writing with your organization's plans for implementing the recommendations
- Findings of the Commissioner can be publicly posted
- Although organizations can be publicly named, it only occurs when the Commissioner deems it to be in the public interest

Investigations:

- There is an offence provision under PIPEDA
- Under that provision, the Commissioner can levy fines for obstruction of an investigation, destroying personal information after an access request has been made and disciplining a whistleblower
- Fines of up to $10,000 or $100,000
- In addition, the Commissioner has the power to summon witnesses, administer oaths and compel the production of evidence
- The Commissioner is required under PIPEDA to issue any findings within a year of the complaint

2. Section 14 Applications:

- Section 14 applications are hearing requests to the Federal Court regarding the way in which an organization handles personal information. They can only be brought after the Commissioner has investigated the matter and issued her findings
- The most common reason for a Section 14 application is to ask the Court to have the Commissioner's findings/recommendations enforced against the organization

Section 14 Applications:

- The Court may:
  - Order an organization to correct its practices to comply with PIPEDA
  - Order an organization to publish a notice of actions taken or proposed to be taken in order to comply with PIPEDA
  - Order an organization to pay damages, including damages for humiliation suffered by the complainant

- In December 2010, Justice Zinn of the Federal Court ordered Transunion to pay total damages of $5,000 to a complainant (*Nammo v. Transunion of Canada Inc.*)

Section 14 Applications:

- The Court found that both the question of whether damages should be awarded and the question of the quantum of damages should be answered with regard to: (i) whether awarding damages would further the general objects of PIPEDA and uphold the values it embodies; and (ii) deterring future breaches and the seriousness or egregiousness of the breach
- In another 2010 Federal Court decision, Justice Mosely declined to award damages because he did not find the breach to be egregious (*Randall v. Nubodys Fitness Centres*)

3. *Judicial Review:*

- Under section 18.1 of the *Federal Court Act*, an application can also be brought for judicial review in order to challenge the findings of the Commissioner
- The grounds for judicial review are limited and include the following:
  - an allegation that the Commissioner refused to exercise her discretion
  - an allegation that the Commissioner acted without jurisdiction
  - an allegation that the Commissioner surpassed the boundaries of the jurisdiction outlined in PIPEDA

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:

PIPEDA:

- Although PIPEDA does not currently have a breach notification provision, it is encouraged in certain circumstances
- The Privacy Commissioner of Canada has prepared Guidelines which outline the "Key Steps for Organizations in Responding to Privacy Breaches"

PIPA Alberta:

- PIPA was amended in 2010 to require breach notification in cases where "a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure" of personal information

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.
- Some of the Atlantic provinces have similar health information protection legislation and similar breach notification requirements.

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