Global IT Law
Privacy
January 9, 2017

professor michael geist
university of ottawa, faculty of law

Canadian Privacy Law - The Start

- CSA Model Code negotiated in early 1990s as a model code for privacy
- Quebec only province with private sector privacy law
- EU Data Protection Directive creates pressure
- Canada hosts OECD Ministerial Conference on Electronic Commerce in 1998

Canadian Privacy Law - The Basics

- Bill introduced in 1998 to coincide with OECD meeting
- Took effect in 2001 (federally regulated orgs), 2004 (everyone else)
- Limited to commercial activity for constitutional reasons
- Shared responsibility with provinces - substantially similar
- Enforced by Privacy Commissioner of Canada in an ombuds+ role
- Complaints driven + audit power

Canadian Privacy Law - The Basics

Application - Subject matter

- **Personally identifiable information only** - includes information about employees
- Public domain exception
  - Telephone Directory
  - Professional or Business Directory
  - Registry Collected under Statutory Authority
  - Court Record
  - Information Appearing in the Media Where the Individual has Provided the Information
- Federal Privacy Act exempt
- Name, Title, Business address or Telephone number of an employee exempt

Canadian Privacy Law - The Basics

10 PRINCIPLES --

1. **Accountability**
   - organization is accountable for personal information
   - Includes privacy point person, training staff
2. **Identifying Purposes**
   - purpose of collection must be clear
   - Identify any new purposes
   - Grandfathering issue
3. **Consent**
   - individual has to give consent to collection, use, disclosure
   - “meaningful” consent -- will depend upon circumstances

Canadian Privacy Law - The Basics

10 PRINCIPLES (cont.) --

4. **Limiting Collection**
   - collect only information required for identified purpose
5. **Limiting Use, Disclosure and Retention**
   - consent required for other purposes
   - Destroy or anonymize information once no longer needed
6. **Accuracy**
   - keep as accurate as necessary for identified purpose

Canadian Privacy Law - The Basics

10 PRINCIPLES (cont.) --

7. **Safeguards**
   - protection and security required
8. **Openness**
   - policies should be available
   - Clear language
9. **Individual Access**
   - info available upon request, inaccuracies corrected
10. **Challenging Compliance**
   - ability to challenge all practices

Canadian Privacy Law - The Basics

Compromise statute -- Purpose clause (s.3)

The purpose of this Part is to establish... rules to govern the collection, use and disclosure of personal information in a manner that recognizes **the right of privacy** of individuals with respect to their personal information and the **need of organizations to collect, use or disclose personal information** for purposes that a reasonable person would consider appropriate in the circumstances.

Canadian Privacy Law - The Basics

- Shared responsibility with provinces
  - “Substantial similarity” - Quebec, Alberta, British Columbia, provincial health privacy
- Hundreds of OPC findings
- Statutory review every 5 years
  - Last review in 2006 leads to Digital Privacy Act
- Privacy Act - governs public sector privacy law
  - No updates since first enacted

Israeli Privacy Law

- Protection of Privacy Law 1981 (Privacy Law)
- Protection of Privacy Regulations (Determination of Databases Containing Non-Disclosable Data) 1987;
- Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies) 1986 (Data Possession Regulations);
- Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect) 1981 (Data Inspection Regulations);
- Protection of Privacy Regulations (Fees) 2000;
- Administrative Offences Regulations (Administrative Fine – Protection of Privacy) 2004;
- Protection of Privacy Regulations (Transfer of Information to Databases outside of the State's Boundaries) 2001 (Data Transfer Regulations);
- Protection of Privacy Order (Determination of Public Bodies) 1986;
- Protection of Privacy Order (Determination of the Investigatory Authority) 1998;
- Protection of Privacy Order (Establishment of Regulatory Unit) 1999
- Patients' Rights Law 1996 (medical information);
- Genetic Information Law 2000 (genetic information);
- Psychologists' Law 1977 (information disclosed in the context of psychological treatment);
- Banking Ordinance 1941 (financial data)
- Credit Information Service Law 2002 (credit information).

Israeli Privacy Law

- Privacy administered by ILITA (Israel Law Information Technology Authority)
  - Privacy
  - Electronic Signatures
  - Credit Reporting
- Law focused on databases
  - Consent
  - Opt-in consent for SMS and email marketing
  - Access rights
  - Data transfers largely based on accountability via contract
  - Security
  - Enforcement (penalties for violations)

Emerging IT Issues

Changing EU Law

- Regulation vs. Directive
- Subject to substantial lobbying pressures
- Substantial fines

Changing EU Law – Safe Harbour

- U.S. received special "treatment":
  - U.S. firms registered and were supervised by the FTC.
- In *Schrems*, the agreement was struck down.
  - Argument: insufficient redress w/r/t the risk of government surveillance.
    - Important lesson regarding the power of the individual.

Changing EU Law – Privacy Shield

- Supplemented by laws providing redress by EU citizens towards the USG
  - Main complaint against Safe harbour – too lax enforcement by the FTC:
    - Lack of incentives
    - Lack of manpower

Data Breach Disclosure

Canadian Digital Privacy Act security breach disclosure

- Rash of security breach disclosures - CIBC, Choicepoint, TJX (Homesense & Winners), Target, Ashley Madison
- Two possible reporting requirements in event of breach:
  - Requirement to report "material breach of security safeguards involving personal information under control" to Privacy Commissioner
  - Criteria to determine whether to report:
    - Sensitivity of information
    - Number of affected individuals
    - Cause of breach/systemic problem

Canadian Digital Privacy Act security breach disclosure

- Requirement to report breach to individuals if "it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual"
- What is significant harm?
  - bodily harm
  - humiliation
  - damage to reputation or relationships
  - loss of employment, business or professional opportunities
  - financial loss
  - identity theft
  - negative effects on the credit record and damage to or loss of property
- Risk factors - (1) sensitivity of info; (2) risk of misuse

Canadian Digital Privacy Act security breach disclosure

- Notifications
  - “ as soon as feasible”
  - Understandable to affected individuals
  - To other organizations who may be able to mitigate harm