



uOttawa

L'Université canadienne
Canada's university



Privacy, Security & Technology: A Canadian Perspective

Gjøvik University College
Guest Lecture, 10 April 2008

Philippa Lawson
Director, Canadian Internet Policy & Public Interest Clinic
University of Ottawa, Faculty of Law
Canada
www.cippic.ca



Definition of Privacy

“the ability to determine for ourselves when, how, and to what extent information about us is communicated to others”

- Alan Weston, 1967

Why Privacy?



- essential to human:
 - dignity
 - autonomy
 - freedom
 - democracy
- underpins relations of mutual trust & confidence, healthy social fabric

Aspects of Privacy



- Physical/territorial privacy
 - freedom from surveillance
 - “right to be let alone”
- Psychological privacy
 - right to hold secrets
- Informational privacy
 - right to control collection/use/disclosure of one’s personal information

Privacy vs. Security



- Informational Privacy:
 - individual control over personal data
 - informed consent
 - openness
 - access to information + correction rights
 - limiting collection/retention
 - to what is necessary
 - limiting use/disclosure
 - to what was agreed
 - to what is reasonable
 - security safeguards

Challenges to Privacy



- New technologies:
 - photography, tape-recording (late 1880s)
 - video cameras; cell phone cameras
 - geo-locational devices
 - computers: data collection, storage, manipulation/analytics
 - internet: clickstream data; e-transactions, search engines
 - digital rights management systems
 - spyware, rootkits, keystroke loggers
 - intelligent sensor devices

Challenges to Privacy



“The electronic computer is to individual privacy what the machine gun was to the horse cavalry”

Schefflin and Opton, *The Mind Manipulators: A Non-Fiction Account* (1978)

Challenges to Privacy



- Practices:
 - data collection/mining
 - commodification of personal information
 - electronic transactions (data trails)
 - workplace screening & monitoring
 - single number identifiers (easy linking)
 - ID cards, smart cards
 - weak authentication
 - ID theft/fraud

Fair Information Principles



- OECD *Guidelines on the Protection of Privacy and Transborder Flows of Data* (1980)
 - www.oecd.org
- UN: *Guidelines Concerning Computerized Personal Data Files* (1990)
 - www.ohchr.org
- Council of Europe: *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (1980)
 - Convention 108
- EU: *Directive on the Protection of Personal Data with regard to the Processing of Personal Data and the Free Movement of such Data* (1990)
 - Directive 95/46/EC

OECD Guidelines



- Collection Limitation
- Data Quality
- Purpose Specification
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Cdn. Initiatives



- 1975: Quebec *Charter of Human Rights & Freedoms*
 - “every person has a right to respect for his private life”
- 1982: *Canadian Charter of Rights and Freedoms*
- 1980s: Public sector privacy laws
- 1990s: CSA Model Privacy Code
 - based on Fair Information Principles (FIPs)
 - adopted as formal standard in 1996
 - incorporated into federal law: PIPEDA
- 1994: Quebec private sector law
- 2001: Federal private sector law
- 2004: Alta, B.C. private sector laws

Privacy Commissioners



- Federal + some provincial
 - Ontario, B.C., Alberta
- Public sector vs. private sector
- Ombuds vs. binding powers
- Role as educators, advocates, watchdogs, dispute resolvers, reporters...

Charter of Rights



- s.7: *“Everyone has the right to life, liberty, and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice”*
 - emerging privacy right
- s.8: *“Everyone has the right to be secure against unreasonable search or seizure”*
 - protects an individual’s “reasonable expectation of privacy” (usually in criminal law context)
- s.1: Rights are subject to *“such reasonable limits as can be justified in a free and democratic society”*

Public Sector legislation



- Federal: *Privacy Act*
- Provincial:
 - Ontario *Freedom of Information and Protection of Privacy Act* (“FIPPA”)
 - similar statutes in other provinces

Private Sector Legislation



- PIPEDA
 - federally regulated
 - interprovincial or international data flows
 - where no “substantially similar” provincial law (3 of 13 provinces/territories have laws)
 - applies to “organizations” in the course of “commercial activities”

PIPEDA



- Purpose:
 - balancing individual’s “right of privacy” with “[legitimate] need of organizations”
- Protects:
 - “personal information”
 - = “information about an identifiable individual”

PIPEDA: Principles



1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention

6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance
11. Limiting Purposes

Consent



- may be explicit or implicit
 - implied consent
 - situationally obvious; consumer would agree if asked
 - no need to confirm via opt-in or opt-out process
 - express (opt in) consent
 - most reliable; must use for sensitive data or where consumer would reasonably expect
 - opt out consent
 - less reliable; OK for non-sensitive data/uses; proper notice is essential

Limiting Purposes



- subs.5(3): “An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.”
 - limits to employee monitoring, credit checks, private investigations....
 - marketing to children?

Security Safeguards



“Personal information shall be protected by security safeguards appropriate to the sensitivity of the information”

- Database protection
 - encryption standard
 - employee access
- Secure transmission

Security Safeguards



- Computer security measures:
 - laptops
 - encryption; passwords
 - public terminals
 - automatic log-off
 - employee access controls
 - disposal
 - ensure hard disk erased

Other Security Measures



- data minimization
 - limiting collection, retention
- limiting use/disclosure
 - to original purposes
 - only with informed consent
 - reasonableness

Statutory Deficiencies



- No breach notification requirements
 - inadequate incentives for strong security
 - inadequate mitigation of damages
- No explicit limits on collection/use/disclosure of kids' data
 - vague rule re: “appropriate purposes”
- Weak enforcement
 - inadequate incentives to comply with law

Other Initiatives



- Canadian *Principles for Electronic Authentication* (2004)
 - “....the collection, use and disclosure of personal information in the context of authentication should be minimized.”
 - applies to designers as well as those using authentication mechanisms

Other Initiatives



- “7 Laws of Identity”
 - by Kim Cameron, Microsoft Corp.
 - User control and consent
 - Minimal disclosure for a constrained use
 - Justifiable parties (“need to know” access)
 - Directed identity (protection and accountability)
 - Pluralism of operators and technologies
 - Human integration (user understanding)
 - Consistent experience across contexts



www.cippic.ca