



Protecting Consumer Privacy and the Right to Know

Philippa Lawson, Director
Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law

www.cippic.ca

*Conference Board of Canada Conference:
Cyber Security: Proactive Defence of Critical Systems and Information
Gatineau, Quebec
Nov. 5-6th 2008*

Online Threats to Consumers



- Viruses, malware
- Spyware, botnets...
- ID Theft/Fraud
- Spam – phishing
- Fraudulent websites
- Stalking
- Preying on children
- Covert monitoring and/or profiling
 - by employers, insurers, marketers
 - by LEAs and other government agencies
- Social sorting
 - differential treatment based on personal data collected surreptitiously

Privacy Rights

- International Law:
 - *Universal Declaration of Human Rights* (1948)
 - *Int'l Covenant on Civil & Political Rights* (1966)
- *Canadian Charter of Rights and Freedoms*
- *Criminal Code*
- Data Protection laws:
 - Public sector (e.g., *Privacy Act*)
 - Private sector (e.g., *PIPEDA*)

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”
 - REP exists in “core biographical” information, that tends to “reveal intimate details of the lifestyle and personal choices of the individual”
 - REP = a normative, not merely descriptive, concept

Charter of Rights

- s.1: Rights are subject to “*such reasonable limits as can be justified in a free and democratic society*”
 - Pressing and substantial goal
 - Proportionality test:
 - Rational connection
 - Minimal impairment
 - Proportionality: effects not so harmful as to outweigh potential benefits of measure



Privacy Act (fed gov)

- Collection of personal data:
 - must relate directly to an operating program
 - must inform individual of purpose
- Use or Disclosure w/o consent OK if:
 - for original or consistent purpose
 - statutorily authorized
 - instit'n head believes that public interest in disclosure outweighs invasion of privacy
 -

PIPEDA

- Limit collection/use/disclosure to purposes that a reasonable person would consider appropriate in the circumstances (objective test)
- Collect & retain only as necessary
- Protect with appropriate safeguards
- Obtain informed consent
 - Unless emergency threatening an individual; law enforcement; national security; required by law;...
 - No “consistent use” exception

PIPEDA Deficiencies

- **Weak enforcement**
 - inadequate incentives to comply with law
 - widespread non-compliance
 - over-collection and retention = major contributors to ID theft
- **No breach notification requirements**
 - inadequate incentives for strong security
 - inadequate mitigation of damages
- **Weak consent rule**
 - widespread use of ineffective opt-out consent
- **No explicit limits re: children's data**
 - vague rule re: “appropriate purposes”

Online Privacy Issues

- “PIPEDA searches”
- Validity of “consent” via terms of service
- Lawful Access
- Outsourcing to USA
- WHOIS policy
- ISP Traffic-shaping
- Behavioural Targeting
- Security Breach Notification

“PIPEDA searches”

- *Charter* → warrant required where “reasonable expectation of privacy” exists
- PIPEDA → consent required unless... for legitimate law enforcement purposes
 - police improperly treating exception to consent requirement in PIPEDA as justification for warrantless searches
 - *Charter* always applies, regardless of PIPEDA

REP in “Subscriber Name and Address”?



- *R. v. Kwok* (Ont.C.J., Jan. 2008):
 - *YES: Subscriber “name and address is information from which intimate personal details of lifestyle and choices can be obtained”; warrant therefore required*
- *R. v. Ward* (Ont.C.J., Aug. 2008):
 - *“It cannot in every case be said that a person's name and address represents seed information likely to lead to intimate personal details of lifestyle, habits and choices.”*
 - TSP Terms of Service are relevant to whether the individual’s expectation of privacy is reasonable



Adequacy of Notice/Consent

- Should REP determination turn on notice via Terms of Service?
 - Is consent via lengthy, all-inclusive Terms of Service that few people read, valid?
 - sufficiently brought to subscriber's attention?

Lawful Access

- *Modernization of Investigative Techniques Act*
 - would permit warrantless access to “subscriber data” upon request to TSPs
 - would require TSPs to construct networks so as to better facilitate state surveillance
 - would establish “suspicion” (vs. “belief”) threshold for searches of “envelope” information (to, from, time, location, server...)

Outsourcing to Foreign Countries



- Legal and cultural differences re: privacy
 - PIPEDA 4.1.3
 - Global Network Initiative
 - *Principles on Freedom of Expression and Privacy*
- *US Foreign Intelligence Security Act (FISA)* - amended July 2008
 - permits gathering of data re: foreigners without any grounds other than reasonable basis to believe that it's a foreigner

WHOIS policy

- Domain name registrants
 - name, address, contact info.
- ICANN policy: full transparency
 - facilitates LEA and private investigation of online threats, but exposes individuals, activists to harassment and persecution
- CIRA policy: partial transparency
 - Individual registrant data hidden but available upon request to LEAs + others claiming fraud, IP infringement

ISP Traffic-Shaping

- Use of “Deep Packet Inspection” technology to identify and “throttle” certain kinds of heavy-use traffic, so as to avoid network congestion
 - violation of common carrier rule (*Telecom Act*)?
 - violation of *PIPEDA*?
 - violation of s.184, *Crim Code*?

Behavioural Targeting

- Is there no limit to the data that commercial entities are permitted to collect about us for target marketing purposes?
 - “hyper-targeting” and consumer profiling
 - Social networking sites
 - Children’s data
 - ISPs now getting in on the act with deep packet inspection technology



Security Breach Notification

- Purposes:
 - allow individuals to mitigate harm
 - create incentive for better security
 - track incidents to inform future policy-making
- Not just a private sector issue
- Threshold for notification?



www.cippic.ca