

CSI 2911 W2011
Professional Practice in Computer Science
Winter 2011

Privacy

Guest Lecture, January 26, 2011



Tamir Israel
Staff Lawyer, CIPPIC
Email: tisrael@uottawa.ca
Website: www.cippic.ca

INTRODUCTION TO PRIVACY

- PRIVACY – WHAT IS IT?
- WHY IS IT IMPORTANT?

“As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed.”

-- Lawrence Lessig, Code 2.0

(NY: Basic Books, 2006), at 77, online: Codev2 <<http://pdf.codev2.cc/Lessig-Codev2.pdf>>

INTRODUCTION TO PRIVACY

PRIVACY – WHAT IS IT?
– WHY IS IT IMPORTANT?

“Privacy is a protean concept” – Justice Binnie, Supreme Court of Canada

R. v. Tessling, [2004] 3 S.C.R. 432 (S.C.C.) <<http://csc.lexum.umontreal.ca/en/2004/2004scc67/2004scc67.html>>

Implicates other values:

- Personal autonomy/dignity
- Democracy
- Freedom
- Control

(Theoretical) Hierarchy of Privacy: Territorial > Bodily > Informational

INTRODUCTION TO PRIVACY

- PRIVACY – WHAT IS IT?
- WHY IS IT IMPORTANT?

INFORMATIONAL PRIVACY

Privacy as informed control over your personal information:

“Beyond our bodies and the places where we live and work, however, lies the thorny question of how much information about ourselves and activities we are entitled to shield from the curious eyes of the state...Informational privacy has been defined as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” [Alan Weston, 1967]. Its protection is predicated on ‘the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain ... as he sees fit.’...Privacy is a protean concept, and the difficult issue is where the “reasonableness” line should be drawn.”

R. v. Tessling, (S.C.C. 2004), Binnie, J.

INFORMATIONAL PRIVACY

PRIVACY – WHAT IS IT?
– WHY IS IT IMPORTANT?

Territorial: Information about what occurs within the home is sensitive
Bodily: Information about the ‘body’ is sensitive (medical information, DNA, biodata).

!Territorial: Can you have privacy in public spaces?

Informational privacy is often about contextual integrity

“Most people have a robust sense of the information about them that is relevant, appropriate, or proper to particular circumstances, situations, or relationships...For the myriad transactions, situations and relationships in which people engage, there are norms—explicit and implicit—governing how much information and what type of information is fitting for them. Where these norms are respected I will say that contextual integrity is maintained; where violated, I will say that contextual integrity has been violated.”

H. Nissenbaum, “Protecting Privacy in an Information Age: The Problem of Privacy in Public”, <<http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>>.

INFORMATIONAL PRIVACY

- PRIVACY – WHAT IS IT?
- WHY IS IT IMPORTANT?

INFO PRIVACY @ LAW

Absolute control over all personal information in all contexts?

The Law Protects:

- Data Protection: knowledge and consent over the collection, use, and disclosure of personal information in a commercial context
 - Consent-based protection
- Reasonable Expectations of privacy
 - What is reasonable?
- Intentional and culpable violations of privacy
 - Wireless surveillance
 - Unauthorized access of a computer system
 - Interception of an electronic communication

INFORMATIONAL PRIVACY

- PRIVACY – WHAT IS IT?
- WHY IS IT IMPORTANT?

PRIVACY 'HARMS'

'Information is power':

- Economics:
 - information asymmetries lead to market inefficiencies (market of lemons)
- Can lead to other harms: identity theft/fraud, loss/lack of employment, proliferation of 'Facebook evidence' in lawsuits/criminal trials, political repression, embarrassment (medical information, private 'affairs')
- General 'creep' factor
 - Knowledge that you are being watched chills free expression
 - U.S. Federal Trade Commission: *"for some consumers, the actual range of privacy related harms is much wider and includes reputational harm, as well as the fear of being monitored or simply having private information 'out there.'"*

Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change", December 2010, <<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>>

- Panoptican

INFORMATIONAL PRIVACY

PRIVACY – RELEVANCE TO COMP SCI?

1. Building Confidence/Trust

- Macro: Confidence *still* affects adoption
- Micro: trust is integral to maintaining customers as well as to encouraging adoption of new features
 - Google WiFi Collection
 - RFIDs

2. Cost Efficiency/Savings

- Build privacy into the product
- Avoids costly/difficult ex post redesigns
 - Facebook Developers API
 - Google Street View

3. Threat of Democratic/Legal Action

- There are existing legal ramifications to ignoring privacy (more below)
- Democratic/legal developments are often driven by violations

4. Privacy Enhancing Technologies (PETs)

- Developing privacy tools can give products a competitive advantage
- There is a potentially developing market for privacy-oriented applications

INFORMATIONAL PRIVACY

PRIVACY – RELEVANCE TO COMP SCI?



CC-BY-SA 2.0 Douglas Maas, <<http://www.geograph.org.uk/photo/1441214>>

INFORMATIONAL PRIVACY

PRIVACY – RELEVANCE TO COMP SCI?

The screenshot shows the Kickstarter project page for 'Decentralize the web with Diaspora'. The page features a navigation bar with the Kickstarter logo, a search bar, and links for 'Discover great projects', 'Start your project', 'BLOG', 'FAQ', 'SIGN UP', and 'LOG IN'. The project title is 'Decentralize the web with Diaspora', with project creators 'Daniel G. Maxwell S. Raphael S. Ilya Z.' listed below. The project has 17 updates, 6479 backers, and 895 comments. A 'Quick Note On Alpha Invites' update is highlighted, dated December 8. The update text discusses the strategy of sending invites at a slower rate to 6,479 backers. On the right, a funding progress summary shows 6,479 backers, \$200,641 pledged of a \$10,000 goal, and 0 seconds to go. A green banner indicates 'FUNDING SUCCESSFUL' with a checkmark, stating the project successfully raised its funding goal on June 1. Below this, a 'PLEDGE \$5 OR MORE' section is visible, with the text 'Once the software is released as open'.

?! What is Kickstarter? We're the largest funding platform for creative projects in the world. [Learn more!](#)

KICKSTARTER Discover great projects Start your project

BLOG FAQ SIGN UP LOG IN

Decentralize the web with Diaspora

Project by [Daniel G. Maxwell S. Raphael S. Ilya Z.](#)

PROJECT HOME UPDATES 17 BACKERS 6479 COMMENTS 895

GET UPDATES BY RSS

Quick Note On Alpha Invites

Update #17 posted on December 8

Hi Everyone,

We wanted to let everyone know how the alpha invites are working.

After some thinking before we started sending invites out, we decided that it would be more useful for everyone if we gave out invites at a slower rate, but gave more invites to those invited. If we gave one give one invite to all 6,479 backers the first day, that would not be helpful for anyone. We wouldn't be able to see how people were really using Diaspora, and people would not be able to have their real friends on the site.

Instead, we started giving ten invites to a smaller number of backers, and increasing that number as we can handle it. After all, a social network is only fun if you can talk to your friends.

We are working as fast as we can to get invites out to our backers, and rest

6,479
BACKERS

\$200,641
PLEGGED OF \$10,000 GOAL

0
SECONDS TO GO

FUNDING SUCCESSFUL

This project successfully raised its funding goal on June 1.

PLEDGE \$5 OR MORE

Once the software is released as open

<<http://www.kickstarter.com/projects/196017994/diaspora-the-personally-controlled-do-it-all-distr/posts>>

INFORMATIONAL PRIVACY

PRIVACY – EMERGING CHALLENGES

TECH CONTEXT

1. Uniqueness of Digital Data:

- Metadata, the Semantic Web
- Instantaneous, permanent, searchable, & easily copyable
- Obscure, unintuitive, invisible processes
 - UI design is integral ('viscosity' – how much effort does it take to protect privacy?)
L. Church & A. Whitten, "Generative Usability: Security and User Centered Design Beyond the Appliance", (2009) NSPW '09, 2010 ACM
<<http://www.nspw.org/papers/2009/nspw2009-church.pdf>>
 - 'Architecture': people do not (often can not) know what happens behind the scenes
- Aggregation/Analytical Capacity [Perceived Anonymity, Predictive technologies]

2. Everything is now more 'social'

3. Digital data is now a commodity

4. New Technologies:

- 'Internet of Things'
- Geo-locational
- Cloud Computing
- Online Tracking

INFORMATIONAL PRIVACY

PRIVACY – THE LAW

LEGAL PROTECTIONS

1. DATA PROTECTION:

- *Personal Information Protection and Electronic Documents Act (PIPEDA)*
 - Provides fair information practices for commercial entities
 - Federal statute
- Some Provinces (B.C., Alberta, Quebec) have ‘substantially similar’ versions
- Some sectors (health) have special protections

2. COMMON LAW (judge made law):

- Things you may be sued for
- Invasion of privacy (?)
 - Class action in initial stages against Facebook for violation of privacy

3. CRIMINAL LAW (?):

- Acts that may send you to jail
- Italy: Google charged for criminal invasion of privacy (charges later dropped)
- US: Husband faces criminal charges for reading wife’s emails

INFORMATIONAL PRIVACY

PRIVACY – THE LAW

LEGAL PROTECTIONS

COMMON LAW INVASION OF PRIVACY:

Courts increasingly willing to impose liability for invasions of informational privacy

“With advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly), and disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual's personal information. The traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy interests ... would be consistent with Charter values and an "incremental revision" and logical extension of the existing jurisprudence.”

Somwar v. McDonalds (Ont. S.C. 2006), <<http://www.canlii.org/en/on/onsc/doc/2006/2006canlii202/2006canlii202.html>>

Likely will involve two parts:

- Has a reasonable expectation of privacy been invaded?
- Is it justified by freedom of expression?

INFORMATIONAL PRIVACY

PRIVACY – THE LAW
DATA PROTECTION/PIPEDA

PIPEDA

“The purpose of [PIPEDA] is undoubtedly directed at the protection of an individual's privacy; but it is also directed at the collection, use and disclosure of personal information by commercial organizations. It seeks to ensure that such collection, use and disclosure are made in a manner that reconciles, to the best possible extent, an individual's privacy with the needs of the organization. There are, therefore, two competing interests within the purpose of the PIPED Act: an individual's right to privacy on the one hand, and the commercial need for access to personal information on the other. However, there is also an express recognition...that the right of privacy is not absolute. The PIPED Act is a compromise both as to substance and as to form.”

Englander v. TELUS Communications, F.C.A. 2004, <<http://www.canlii.org/en/ca/fca/doc/2004/2004fca387/2004fca387.html>>

INFORMATIONAL PRIVACY

PRIVACY – THE LAW DATA PROTECTION/PIPEDA

APPLICATION: PIPEDA applies to any collection, use, and disclosure of personal information that is conducted in the course of commercial activity.

“personal information” means information about an identifiable individual...

PIPEDA, section 2, Definitions

- IP Addresses?

- Bell’s DPI

http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm

- Aggregate information?

- Facebook?

- Anonymized data?

“An examination of these pharmacy data indicated that out of 3,510 patient visits during which the hospital pharmacy dispensed a prescription, 99.6 percent were unique on age, gender, FSA, admission date, and discharge date.”

K. El-Emam & P. Kosseim, “Privacy Interests in Prescription Data, Part 2”,

http://www.ruor.uottawa.ca/fr/bitstream/handle/10393/12985/El_Emam_Khaled_2009_Privacy_interests_in_prescription_data_2.pdf

INFORMATIONAL PRIVACY

PRIVACY – THE LAW DATA PROTECTION/PIPEDA

“Information will be about an identifiable individual if there is a serious possibility that someone could identify the available information. It is not necessary...to demonstrate that someone would necessarily go to all lengths to actually do so. Consequently, de-identified data will not constitute “truly anonymous information” when it is possible to subsequently link the de-identified data back to an identifiable individual.”

OPC Case Summary #2009-018, *Psychologist’s anonymized peer review notes are the personal information of the patient,*
<http://www.priv.gc.ca/cf-dc/2009/2009_018_0223_e.cfm>

“...Bell assigns its subscribers a dynamic IP address when a Sympatico subscriber connects to the network. Bell has indicated that it binds each dynamic IP address to an invariable “subscriber id” that can be traced back to an individual Sympatico subscriber. In this way, Bell can determine which Sympatico subscriber is associated with a dynamic IP address at a given time. Given that Bell can link its Sympatico subscribers, by virtue of their subscriber ID, with Internet activities (in this case, type of application being used) associated with their assigned IP addresses, in my view, IP addresses in this context are personal information.”

OPC Case Summary #2009-010, *Assistant Commissioner recommends Bell Canada inform customers about Deep Packet Inspection (DPI),*
<http://www.priv.gc.ca/cf-dc/2009/2009_010_rep_0813_e.cfm>

INFORMATIONAL PRIVACY

PRIVACY – THE LAW DATA PROTECTION/PIPEDA

PUBLICLY AVAILABLE INFORMATION?

Applies to MOST publicly available information, except as expressly specified:

- I.e. name, address and phone number listed in a phone directory, where the subscriber may refuse to have her number listed
- Implied consent

PIPEDA Case Summary #2005-297

- An organization collected a business e-mail address from employer's website directory service, sent email asking if individual wished to purchase tickets to sporting events.
- Organization A's purpose for collecting/using the email address was unrelated to the purpose for which the directory was created.
- Violation of Principle 4.3, collection/use of PI w/out consent.

PIPEDA Case Summary #2005-297, Unsolicited e-mail for marketing purposes, <http://www.priv.gc.ca/cf-dc/2005/297_050331_01_e.cfm>

INFORMATIONAL PRIVACY

PRIVACY – THE LAW
DATA PROTECTION/PIPEDA

Fair Information Principles

PIPEDA – Schedule 1

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

INFORMATIONAL PRIVACY

PRIVACY – THE LAW
DATA PROTECTION/PIPEDA

PIPEDA – Schedule 1

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

Accountability (Principle 4.1):

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

“Due to the engineer's failure to forward his design document to the Product Counsel, the Counsel was unable to assess the privacy implications of the code designed to collect WiFi data.”

OPC Preliminary Letter of Findings [Google and WiFi], October 19, 2010,
<http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.cfm>

INFORMATIONAL PRIVACY

PRIVACY – THE LAW
DATA PROTECTION/PIPEDA

PIPEDA – Schedule 1

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

CONSENT: PRINCIPLE 4.3.2

“The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.”

FORM OF CONSENT:

- Can have UI implications
- Can be implied, opt-out, opt-in
- Based on sensitivity of information involved, reasonable expectations of users, whether purpose is primary/secondary

INFORMATIONAL PRIVACY

PRIVACY – THE LAW
DATA PROTECTION/PIPEDA

PIPEDA – Schedule 1

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

EXTENT?

- Mandatory encryption?
- Facebook API
- Retention + Aggregation

SAFEGUARDS/RETENTION:

- Organizations must retain personal information only as far as is necessary to achieve the purposes for which it was collected (4.5, 4.5.2)
- Organizations must implement technical and non-technical safeguards to protect personal information from unauthorized access or disclosure (4.7, 4.7.1)
- *PRINCIPLE 4.7: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.*

INFORMATIONAL PRIVACY

PRIVACY – THE LAW
DATA PROTECTION/PIPEDA

PRIVACY COMMISSIONERS

- Investigative mandate
- Ombudsman v. ‘Rights-defender’
- Incentives for Compliance?
- Education/Research Mandate

“I would also like to take a few moments to talk about incentives for compliance. I am increasingly of the view that we may need stronger powers in order to be an effective privacy guardian for Canadians. We’ve become one of the few major countries where the data protection regulator lacks the ability to issue orders and impose fines.”

-- Jennifer Stoddart, Privacy Commissioner of Canada, 2011,
http://www.priv.gc.ca/speech/2011/sp-d_20110119_e.cfm