A Contextual Approach to Privacy: Theory and Application

Helen Nissenbaum
New York University

Institut Mines-Télécom

Paris 10.15.13

Why privacy? Why now?
TECHNOLOGY AND PRIVACY

- GPS, mobile, implantable devices
- RFID, “emanations”
- Biometrics
- Pervasive sensory networks
- Networked video and audio capture
- Web cookies, flash cookies, web bugs

- Databases, storage, retrieval
- Information aggregation, mining, profiling
- “Big data,” “data science, ‘...

- The Internet, the Web
- Social computing, Web 2.0
- Email, mobile media
Sociotechnical systems
What makes them privacy threats?
How is privacy protected?

• Diminished Control
• Control returned
• Increased exposure
• Increased secrecy
• Private/public dichotomy breached
• Protect privacy of private
Contextual Integrity

Respecting privacy does not mean ...
- subject controls data!
- data flow is stopped (secrecy)!
- no flow in private zone (and inverse)

it does mean ... 
- appropriate flow/sharing
- appropriate constraints
What is appropriate flow??
Privacy as Contextual Integrity: Key Concepts

**Contexts**
Structured social spheres defined by activities, practices, roles, ... e.g. healthcare, education, social & home-life, professional & work-life, commercial marketplace (e.g. Pierre Bourdieu)

**Informational Norms**
Context specific rules, customs, conventions, expectations, laws, defining appropriate flows of personal information

**Purposes and values**
General ethical and political + context specific ends, purposes and values
Informational norms model Appropriate Flow

In a job interview, the interviewer asks about a candidate’s past work experience but not about religious observance.

A priest never shares congregants’ confessions with others.

A citizen of the U.S. reveals gross income to the IRS, under strict conditions of confidentiality except as required by law.

You do not share a friend’s secrets with others, except, perhaps, with your spouse, unless your friend expressly requests otherwise.

Parents closely monitor their children’s academic performance.
Informational norms: Key Parameters

**Actors**
- Sender
- Recipient
- Subject

**Information types**
- Demographic, biographical
- Transactional, communications
- Medical status, financial

**Transmission Principles**
- Consent, coerce, steal, buy, sell
- Confidentially, stewardship
- With a warrant, surreptitiously
- [An indefinitely large domain]
Appropriate flows/constraints modeled by Context-specific Informational norms

<Information Type/Attributes> about <Data Subject> is transmitted from <Sender> to <Recipient> under <conditions defined by Transmission Principle>

Aoributes; Transmission Principles

Ideal norms promote values and purposes
Respecting Privacy means ...

Respecting entrenched context specific informational norms
Respecting Privacy means ...

Respecting entrenched context specific informational norms

This is a terribly conservative theory!
Evaluating disruption: how?

- Interests
- General moral, social, and political values
- Internal context-specific ends, purposes and values
Considerations

Interests – often conflicted

  Informational harms, benefits, risks
  Boundary control (Altman)

General moral, social, and political rights & values

  Unfair discrimination ...
  Liberty, autonomy ...
Considerations

Context specific purposes and values

healthcare: cure disease; alleviate suffering, equity ...
political: democracy; freedom from exploitation ...
home and social: trust, autonomy, stability ...
education: knowledge, intellect, fair distribution
“While the government does not know every source of income of a taxpayer and must rely upon the good faith of those reporting income, still in the great majority of cases this reliance is entirely justifiable, principally because the taxpayer knows that in making a truthful disclosure of the sources of his income, information stops with the government. It is like confiding in one’s lawyer.”

Secretary of the Treasury, Andrew Mellon, 1925
Respecting Privacy means

- Respecting **entrenched context specific** informational norms
- Accepting disruptive flows in place of entrenched i-norms only if:
  - Interests are balanced
  - general rights & values respected
  - context specific ends, purposes, values sustained

**Note:**
Privacy is not the opposite of sharing; it is the opposite of inappropriate sharing
Information is not yours, it is about you
The contours of privacy are socially (culturally) varied
Letting people choose may be neither in their interest nor morally required
The Obama Administration believes America must apply our timeless privacy values to the new technologies and circumstances of our times. Citizens are entitled to have their personal data handled according to these principles.

**Individual Control**
Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

**Access and Accuracy**
Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity and risk associated with the data.

**Transparency**
Consumers have a right to easily understandable and accessible information about privacy and security practices.

**Focused Collection**
Consumers have a right to reasonable limits on the personal data that companies collect and retain.

**Respect for Context**
Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent.

**Accountability**
Companies should be accountable to enforcement authorities and consumers for adhering to these principles.

**Security**
Consumers have a right to secure and responsible handling of personal data.
Applications

“where the rubber hits the road”

1. Test CI
2. Utilize Diagnostic + Prescriptive
Applications: Empirical + Analytical + Technical

✧ Disruptive flows?
✧ Locate nature and sources of disruption
✧ Evaluate disruptions [not all change is good/bad]
  ✧ Interests
  ✧ general ethical and political values
  ✧ context specific ends, purposes, values
Applications - Empirical

- eCommerce (Kirsten Martin)
- Placement of Court Records Online [RECAP study]
- Health IT and Privacy [SHARPS]
  - Anupam Datta, et. al.
  - Martin French, Heather Patterson: cardio patients expectations in mobile health tracking [Northwestern, UC Berkeley, NYU collaboration]
  - Heather Patterson: Mobile Apps (e.g. Fitbit) and user expectations
HIPAA excerpt

A covered entity may disclose an individual’s protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participating in a violent crime that the covered entity believes may have caused serious physical harm to the victim.
4.5 §164.510 A covered entity may use or disclose protected health information, provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the use or disclosure, in accordance with the applicable requirements of this section.

[[To whom?]]
Applications - Analytical

- Placement of court records on open Web
- Online Privacy
- “Respect for Context,” what it is and isn’t
- Privacy trouble with MOOCs
- Contextual expectations of privacy
  - Andrew Selbst – 4th Amendment
- Health IT and Privacy
  - Martin French: Privacy rules for HIEs [Working with the IL-HIE]
Contextual Integrity as applied to Court Records

- Previous work detailed how contextual integrity (CI) illuminates this shift.
  - Empirical study that searched for federal electronic records, New Jersey state court records.
Bankruptcy Court Records: The old days

Source: United States Bankruptcy Court, Northern District of California, San Jose Division, http://www.canb.uscourts.gov/court-information/locations/san-jose-division
Case Study: RECAP
Contextual Integrity as applied to Court Records

- Previous work detailed how contextual integrity (CI) illuminates this shift.
  - Empirical study that searched for federal electronic records, New Jersey state court records
Contextual Integrity as applied to Court Records

• Findings:
  o Different cost of flows of personal information between online and local access systems, based on:
    • Location of information system
    • Query interface and indexing mechanism
    • Linked information sources
    • Access restrictions
    • Record format
    • Human factors
Possible models to guide information flow

- “Fine-grained differential access”
  - Vary access based on, for example,
    - the roles of parties requesting access
    - the roles of information subjects
    - the types of information, and
    - the conditions under which information is granted.
IV. Work-in-progress: Tailored Rules for Privacy and Transparency?
Applications - Technical

- Context-Aware DNT: FF extension
  - automatically sets DNT header based on page content, using Adnostic ontology

- Cryptogram: privacy for photo sharing

- Compass

- Obfuscation
  - TrackMeNot (with V. Toubiana and D. Howe)
  - “AdNauseum” (with D. Howe)
Cryptagram
photo privacy for online social media
http://cryptagr.am

- Appropriate photo access and control
- Stops server side gleaning and facial recognition
- Retains key photo sharing experience

Matt Tierney, Ian Spiro, Chris Bregler, Lakshmi Subramanian | PRGLab | NSF IGERT
OBfuscation: Our Definition

“The production, inclusion, addition, or communication of misleading, ambiguous, or false data in an effort to evade, distract, or confuse data gatherers or diminish the reliability (and value) of data aggregations.”

"It took me back to Buffalo, to the pignoli, a Sicilian version of macarons studded with pine nuts that my Aunt Lili made in huge batches at Christmas.

... she kept her recipe secret, not by withholding it, but by slightly altering proportions of the ingredients in every retelling."

TrackMeNot

Created by: Daniel C. Howe (@danielchowe), Helen Nissenbaum (@HNissenbaum)
Maintained by: Vincent Toubiana (@vtoubiana)
Homepage: www.cs.nyu.edu/trackmenot/
Translations: Jens 'woelfchen'(German), Tommy Mejidal(Danish), markh van BabelZilla.org(Dutch), rlicul(Croatian), BruceH(Chinese), Edgard Dias Magalhaes(Portuguese)

2006 - ongoing

Search Engines
- Google Search
- Yahoo! Search
- Bing Search
- Baidu Search
- Aol Search

To add the engine url, search 'trackmenot' (without the quotes) on the engine you want to add, and copy/past the search url in the URL text box below.
Name URL

Avg. Query Rate:
Query Frequency 5 per min

Logging Options
- Disabled
- Persist

RSS Feed

Black List
- Use list: bomb,porn,pornographie
- Generate queries including keywords monitored by DHS
[AdNauseum] is a lightweight browser extension that helps protect users against surveillance and data-profiling by online advertisers and ad networks. It does so not by means of concealment and encryption (i.e. covering one's tracks), but instead, paradoxically, by the opposite strategy: noise and obfuscation. [AdNauseum] works silently in the background of your web browser by clicking all the ads on a page, thereby obscuring user interests in a cloud of decoy clicks. In light of the industry's failure to achieve consensus on a Do Not Track standard, [AdNauseum] allows individual users to take matters into their own hands, offering cover against certain forms of surveillance, profiling, and practices of discrimination.

For the past 1.5 years W3C has led an effort which has engaged NGOs, industry reps from advertising and tech attempting to achieve a consensus on a standard for Do Not Track (DNT). From several trusted sources, the ad industry continuously sabotages progress, often at the 11th hour, so much so that at least