



# Privacy in Organizations

Anupam Datta (CMU)

Helen Nissenbaum (NYU)

**NSF Workshop on Organizations  
and Innovation**

**July 23, 2008 | Arlington, VA**

# Privacy

- An increasingly important concern for individuals and enterprises



# Modeling Privacy

- From a social viewpoint
  - Contextual Integrity (CI): A conceptual framework for privacy
- From a computer science viewpoint
  - Computer language for expressing and enforcing CI norms
- Study *privacy* issues in *information-rich organizational processes*
  - Examples of organizations:
    - Hospitals, financial institutions, universities, etc.
  - Examples of privacy regulations
    - HIPAA, GLBA, COPPA, SB1386
  - Privacy-preserving information sharing
    - AOL search query case

# Contextual Integrity [Nis2004]

{*bringing the social layer into view in interpreting privacy*}

What? CI is a measure of how closely the flow of personal information conforms to context-relative informational norms. CI is violated when these norms (rules) are breached.

{**Contexts** are: structured social settings, Characterized by **roles**, relationships, power structures, canonical activities, strategies, **norms**, enforcement mechanisms, and internal **values** (goals, ends, purposes) E.g. health-care, education, politics, religious observance}

**Context relative informational norms:** the flow of information of a certain type (attributes) about a subject (acting in a particular capacity/role) from a sender (possibly the subject, acting in a particular capacity/role) to a recipient (acting in a particular capacity/role) is governed by a particular transmission principle.

Key Parameters--**contexts**, attributes, actors, transmission principles

# Informational Norms Embedded in Law: Example (GLB Act)

Sender role

Subject role

Financial institutions must notify consumers

if they share their non-public personal Attribute

information with non-affiliated companies, Recipient role

*but the notification may occur either before or after the information sharing occurs*

Transmission principle



In our formal computer language,

$\square \forall p_1, p_2, q : P. \forall m : M. \forall t : T.$

$\text{incontext}(p_1, c) \wedge \text{send}(p_1, p_2, m) \wedge \text{contains}(m, q, t) \rightarrow$

$\text{inrole}(p_1, \text{institution}) \wedge \text{inrole}(p_2, \text{non-affiliate}) \wedge \text{inrole}(q, \text{consumer}) \wedge (t \in \text{npi}) \rightarrow$

$\diamond \text{send}(p_1, q, \text{privacy-notice}) \vee \diamond \text{send}(p_1, q, \text{privacy-notice})$

# Formal theory

[BDMN2006,BDMS2007]

- Model of interacting agents in roles
  - Concurrent game structure
- Language for specifying *norms* and *purpose*
  - Based on temporal logic (LTL, ATL)
  - *Positive norms* (HIPAA) and *negative norms* (COPPA)
- Policy enforcement
  - Model-checking (assuming agents *responsible*)
  - Auditing (to identify agents *accountable* for policy violation)
- Case study
  - Vanderbilt University Medical Center

# Research Challenges

- Interaction across organizational boundaries
  - {important for cross-organizational collaboration and information sharing}
  - Law enforcement in a hospital (relationships between contexts)
  - Private set intersection: airline passengers with suspected terrorist list
  - Sanitizing databases with personal information, e.g. AOL debacle, health data
- Data provenance
- How to embed informational norms in automated processes
- Compliance vs. risk-based models incorporating concepts from economics
  - Internal measures and inspections: cost, effectiveness
  - External auditing: frequency, penalties

Work supported by:

NSF ITR-0331542:

*Sensitive Information in a Wired World  
(PORTIA)*

*<http://crypto.stanford.edu/portia/>*

\*

*NSF Science and Technology Center  
TRUST*

*<http://www.truststc.org>*

\*

*ARO Perpetually Available and Secure  
Systems Grant to Carnegie Mellon CyLab*

# Related Languages

Model	Sender	Recipient	Subject	Attributes	Past	Future	Combination
RBAC	Role	Identity	×	×	×	×	•
XACML	Flexible	Flexible	Flexible	o	×	o	•
EPAL	Fixed	Role	Fixed	•	×	o	×
P3P	Fixed	Role	Fixed	•	o	×	o
LPU	Role	Role	Role	•	•	•	•

- Legend:

- × unsupported

- o partially supported

- fully supported

- LPU fully supports attributes, combination, temporal conditions

Utility not  
considered

## Transmission Principles\*\* e.g.

Consent (subject controls)

Notice (subject is/is not aware of transmission)

Compulsion (e.g. earnings to IRS)

Confidentiality

Fiduciary

Sale

Barter

Reciprocity

Entitlement, desert

Need

Secrecy?

Etc...