# Privacy in Context: Contextual Integrity

Peter Radics

# Papers

- H. Nissenbaum. Privacy as contextual integrity. *Washington Law Review*, 79(1):119–158, 2004.

- A. Barth, A. Datta, J. Mitchell, and H. Nissenbaum. Privacy and contextual integrity: framework and applications. In *Security and Privacy, 2006 IEEE Symposium on*, pages 15 pp.–198, May 2006.

# Privacy Scenarios

- Public Records Online
  - Local vs. Global access of data
- Consumer Profiling and Data Mining
  - Aggregation/analysis of data vs. single occurrence
- RFID Tags
  - Automated capture of enhanced/large amounts of information

# Current Practice in Law

- Three guiding principles:
  1. Protecting privacy of individuals against intrusive government agents
     - 1st, 3rd, 4th, 5th, 9th, 14th amendments, Privacy Act (1974)
  2. Restricting access to sensitive, personal, or private information
     - FERPA, Right to Financial Privacy Act, Video Privacy Protection Act, HIPAA
  3. Curtailing intrusions into spaces or spheres deemed private or personal
     - 3rd, 4th amendments

# Grey Areas of the Three  Principles

- USA PATRIOT Act
- Credit headers
- Private vs. public space
- Online privacy at the workplace

# Principles and Public Surveillance

- Public surveillance not covered by principles
  - No government agents pursuing access to citizens
  - No collection of personal/sensitive information
  - No intrusion personal/private spaces

➔ **No privacy problems!**

# Reasonable Expectation of Privacy

- Extension to principles

1. Person expects privacy
2. Expectation deemed reasonable by society

- But: Yielding privacy in public space!

# Downsides of Three Principles

- Not conditioned on additional dimensions
  - Time, location, etc.
- Privacy based on dichotomies
  - Private – public, sensitive – non-sensitive, government – private, …

# Contextual Integrity: Idea

- Main idea:
  - Everything happens within a certain context
  - Context can be used to provide normative account of privacy

# Contextual Integrity: Corner Stones

- Contextual Integrity based on two corner stones:
  - Appropriateness
    - Norms about what is appropriate within context
    - Norms about what is not appropriate within context
    - Allowable, expected, demanded information
  - Distribution
    - Norms about information flow
    - Free choice, discretion, confidentiality, need, entitlement, obligation

# Concerns

- Could be detrimentally conservative
- Loses prescriptive character through ties to practice and convention
- Favors status quo

# Solution

- Distinguish *actual* and *prescribed* practice
- Grounds for prescription can vary between different possibilities
- Norms can change over time/locations

# Change of Norms

- Compare current with proposed norm, compare social, political, and moral values

- Affected Values:
  - Prevention of information-based harm
  - Informational inequality
  - Autonomy and Freedom
  - Preservation of important human relationships
  - Democracy and other social values

# Privacy Scenarios (revisited)

- Public Records Online
  - Local vs. Global access of data
- Consumer Profiling and Data Mining
  - Aggregation/analysis of data vs. single occurrence
- RFID Tags
  - Automated capture of enhanced/large amounts of information

# Second paper

- Formalization of Contextual Integrity:
  - Linear Temporal Logic
- Agents *P*, attributes *T*, computation roles (t,t')
- Knowledge state $k \subseteq P \times P \times T$
- Messages *M*, $content\ m \subseteq P \times T$
  - *k* -> *p,q,m* -> *k'*, *k'* := *k* U *q* x *content(m)*
- Roles *R*, contexts *C* (partition of *R*) $C \subseteq P \times R$
- Role state
- Trace: sequence of triples (*k*, *p*, *a*)

# Temporal Logic Grammar

$$\begin{aligned}\varphi ::= \ & \mathrm{send}(p_1, p_2, m) \mid \mathrm{contains}(m, q, t) \mid \\ & \mathrm{inrole}(p, r) \mid \mathrm{incontext}(p, c) \mid t \in t' \mid \\ & \varphi \wedge \varphi \mid \neg\varphi \mid \varphi \mathcal{U} \varphi \mid \varphi \mathcal{S} \varphi \mid \bigcirc\varphi \mid \exists x : \tau.\varphi\end{aligned}$$

$\Diamond$ for "eventually," $\Box$ for "henceforth," $\Diamond\!\!-$ and $\Box\!\!-$ for the past versions of $\Diamond$ and $\Box$, respectively, and $\mathcal{W}$ for "wait for." The formula $\varphi \mathcal{W} \psi$ holds if either $\Box\varphi$ holds or $\varphi \mathcal{U} \psi$ holds.

$$\sigma \models \Box \forall p_1, p_2, q : P. \forall m : M. \forall t : T.$$

$$\mathrm{incontext}(p_1, c) \wedge \mathrm{send}(p_1, p_2, m) \wedge \mathrm{contains}(m, q, t) \rightarrow \bigvee_{\varphi^+ \in \mathrm{norms}^+(c)} \varphi^+ \wedge \bigwedge_{\varphi^- \in \mathrm{norms}^-(c)} \varphi^- \quad (1)$$

**positive norm:** $\mathrm{inrole}(p_1, \hat{r}_1) \wedge \mathrm{inrole}(p_2, \hat{r}_2) \wedge \mathrm{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \wedge \psi$

**negative norm:** $\mathrm{inrole}(p_1, \hat{r}_1) \wedge \mathrm{inrole}(p_2, \hat{r}_2) \wedge \mathrm{inrole}(q, \hat{r}) \wedge (t \in \hat{t}) \wedge \theta \rightarrow \psi$

# Model Checking

- Consistency
- Entailment
- Compliance

# Example: HIPAA

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge (q = p_2) \wedge (t \in \textit{phi}) \quad (2)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{provider}) \wedge \text{inrole}(q, \textit{patient}) \wedge (t \in \textit{phi}) \quad (3)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge (q = p_2) \wedge (t \in \textit{psychotherapy-notes}) \rightarrow$$
$$\diamondminus \exists p : P.\, \text{inrole}(p, \textit{psychiatrist}) \wedge \text{send}(p, p_1, \textit{approve-disclose-psychotherapy-notes}) \quad (4)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{individual}) \wedge \text{inrole}(q, \textit{individual}) \wedge (t \in \textit{condition-and-location}) \wedge$$
$$\diamondminus \exists m' : M.\, \text{send}(p_2, p_1, m') \wedge \text{contains}(m', q, \textit{name}) \quad (5)$$

$$\text{inrole}(p_1, \textit{covered-entity}) \wedge \text{inrole}(p_2, \textit{clergy}) \wedge \text{inrole}(q, \textit{individual}) \wedge (t \in \textit{directory-information}) \quad (6)$$

**Figure 2. Norms of Transmission from the HIPAA Privacy Rule**

# Comparison to Other Models

| Model | Sender | Recipient | Subject | Attributes | Past | Future | Combination |
|---|---|---|---|---|---|---|---|
| RBAC | Role | Identity | × | × | × | × | • |
| XACML | Flexible | Flexible | Flexible | ○ | × | ○ | • |
| EPAL | Fixed | Role | Fixed | • | × | ○ | × |
| P3P | Fixed | Role | Fixed | • | ○ | × | ○ |
| CI | Role | Role | Role | • | • | • | • |

**Figure 5. Comparison of various privacy languages. The symbol × indicates the feature is absent from the language, ○ indicates partial or limited functionality, and • indicates the feature is fully functional. Note, [6] gives an extension of EPAL that is closed under combination.**

# Discussion

- What are strengths/weaknesses of Contextual Integrity?
- Is a formal model of Contextual Integrity useful?
- How can an end-user benefit?