Privacy in Context: Contextual Integrity

Peter Radics
Papers


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

- Messages $M$,
  - $k \rightarrow p, q, m \rightarrow k', k' := k \cup q \times \text{content}(m)$

- Roles $R$, contexts $C$ (partition of $R$)

- Role state

- Trace: sequence of triples $(k, p, a)$
Temporal Logic Grammar

\[ \varphi ::= \text{send}(p_1, p_2, m) \mid \text{contains}(m, q, t) \mid \]
\[ \text{inrole}(p, r) \mid \text{incontext}(p, c) \mid t \in t' \mid \]
\[ \varphi \land \varphi \mid \neg \varphi \mid \varphi U \varphi \mid \varphi S \varphi \mid \diamondsuit \varphi \mid \exists x : \tau . \varphi \]

\( \diamondsuit \) for “eventually,” \( \square \) for “henceforth,” \( \diamondsuit \) and \( \square \) for the past versions of \( \diamondsuit \) and \( \square \), respectively, and \( \mathcal{W} \) for “wait for.” The formula \( \varphi \mathcal{W} \psi \) holds if either \( \square \varphi \) holds or \( \varphi U \psi \) holds.

\[ \sigma \models \square \forall p_1, p_2, q : P. \forall m : M. \forall t : T. \]
\[ \text{incontext}(p_1, c) \land \text{send}(p_1, p_2, m) \land \text{contains}(m, q, t) \rightarrow \bigvee_{\varphi^+ \in \text{norms}^+(c)} \varphi^+ \land \bigwedge_{\varphi^- \in \text{norms}^-(c)} \varphi^- \quad (1) \]

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

**negative norm:** \( \text{inrole}(p_1, \hat{r}_1) \land \text{inrole}(p_2, \hat{r}_2) \land \text{inrole}(q, \hat{r}) \land (t \in \hat{t}) \land \theta \rightarrow \psi \)
Model Checking

- Consistency
- Entailment
- Compliance
Example: HIPAA

\[
\begin{align*}
\text{inrole}(p_1, \text{covered-entity}) & \land \text{inrole}(p_2, \text{individual}) \land (q = p_2) \land (t \in \phi) \\
\text{inrole}(p_1, \text{covered-entity}) & \land \text{inrole}(p_2, \text{provider}) \land \text{inrole}(q, \text{patient}) \land (t \in \phi) \\
\text{inrole}(p_1, \text{covered-entity}) & \land \text{inrole}(p_2, \text{individual}) \land (q = p_2) \land (t \in \text{psychotherapy-notes}) \rightarrow \\
& \quad \bigotimes \exists p : P. \text{inrole}(p, \text{psychiatrist}) \land \text{send}(p, p_1, \text{approve-disclose-psychotherapy-notes}) \\
\text{inrole}(p_1, \text{covered-entity}) & \land \text{inrole}(p_2, \text{individual}) \land \text{inrole}(q, \text{individual}) \land (t \in \text{condition-and-location}) \land \\
& \quad \bigotimes \exists m' : M. \text{send}(p_2, p_1, m') \land \text{contains}(m', q, \text{name}) \\
\text{inrole}(p_1, \text{covered-entity}) & \land \text{inrole}(p_2, \text{clergy}) \land \text{inrole}(q, \text{individual}) \land (t \in \text{directory-information})
\end{align*}
\]

\textbf{Figure 2. Norms of Transmission from the HIPAA Privacy Rule}
Comparison to Other Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Sender</th>
<th>Recipient</th>
<th>Subject</th>
<th>Attributes</th>
<th>Past</th>
<th>Future</th>
<th>Combination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBAC</td>
<td>Role</td>
<td>Identity</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>×</td>
<td>●</td>
</tr>
<tr>
<td>XACML</td>
<td>Flexible</td>
<td>Flexible</td>
<td>Flexible</td>
<td>○</td>
<td>×</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>EPAL</td>
<td>Fixed</td>
<td>Role</td>
<td>Fixed</td>
<td>●</td>
<td>×</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>P3P</td>
<td>Fixed</td>
<td>Role</td>
<td>Fixed</td>
<td>●</td>
<td>○</td>
<td>×</td>
<td>○</td>
</tr>
<tr>
<td>CI</td>
<td>Role</td>
<td>Role</td>
<td>Role</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

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?