Privacy as Restrictions on Personal Information Flow

Limin Jia
ECE & INI
Carnegie Mellon University
liminjia@cmu.edu
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.

- **Privacy is beyond simple data access control**
- **Privacy as Restrictions on Personal Information Flow**
  - Restricting direct flow (direct disclosure)
  - Temporal restrictions
  - Restrictions backed by complex semantics
  - Purpose
Metric First-order Temporal Logic (MFOTL)

- Precise
  - Temporal restrictions are encoded using temporal connectives

- Expressive
  - Encoded all of GLBA and HIPAA disclosure related clauses

- Usable?
Challenges

- Precision
- Expressiveness
  - Semantics behind privacy policies is complex
  - Enforcement mechanisms need precise semantics
- Usability
Privacy as Restrictions on Personal Information Flow

Direct

Interference

Probabilistic Interference

Information Flow

Purpose & Role based

Temporal

Restrictions

EPAL
XACML
*-access control

FOTLs
[Formal Contextual Integrity,
Reduce audit algorithm,
Basin et al.]

Jif,
FlowCaml,
...

[Hayati &
Abadi]

Grok +
Legalease

Information Flow Experiments

Differential Privacy

Healthcare Privacy

Web Privacy

Differential
Privacy

Information Flow

Experiments

[Hayati &
Abadi]
We will **not** use full IP Address for Advertising. IP Address may be used for detecting abuse. In such cases, it will not be combined with account information.

**Encoded the entirety of Google’s privacy policies and Bing’s privacy**
Exceptions
How legal texts are structured
One-to one correspondence

Local Reasoning
Each exception refines its immediate parent
Formally proven property

Independent of Code
**Legalease**


| Usable by lawyers and privacy champs. | Expressive enough for real-world policies. | Precise semantics for local reasoning. |
Privacy as Restrictions on Personal Information Flow

- Direct Interference
  - EPAL
  - XACML
  - *-access control

- Interference
  - Jif, FlowCaml, ...
  - [Hayati & Abadi]

- Probabilistic Interference
  - Information Flow Experiments

- Temporal Restrictions
  - FOTLs
    - [Formal Contextual Integrity, Reduce audit algorithm, Basin et al.]

- Purpose & Role based
  - EPAL
  - XACML
  - *-access control

- Healthcare Privacy

- Web Privacy

- Differential Privacy
References

- http://www.andrew.cmu.edu/user/danupam/privacy.html