Privacy as Restrictions on Personal Information Flow

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

Electrical & Computer ENGINEERING

Carnegie Mellon

Privacy as Restrictions on Personal Information Flow

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

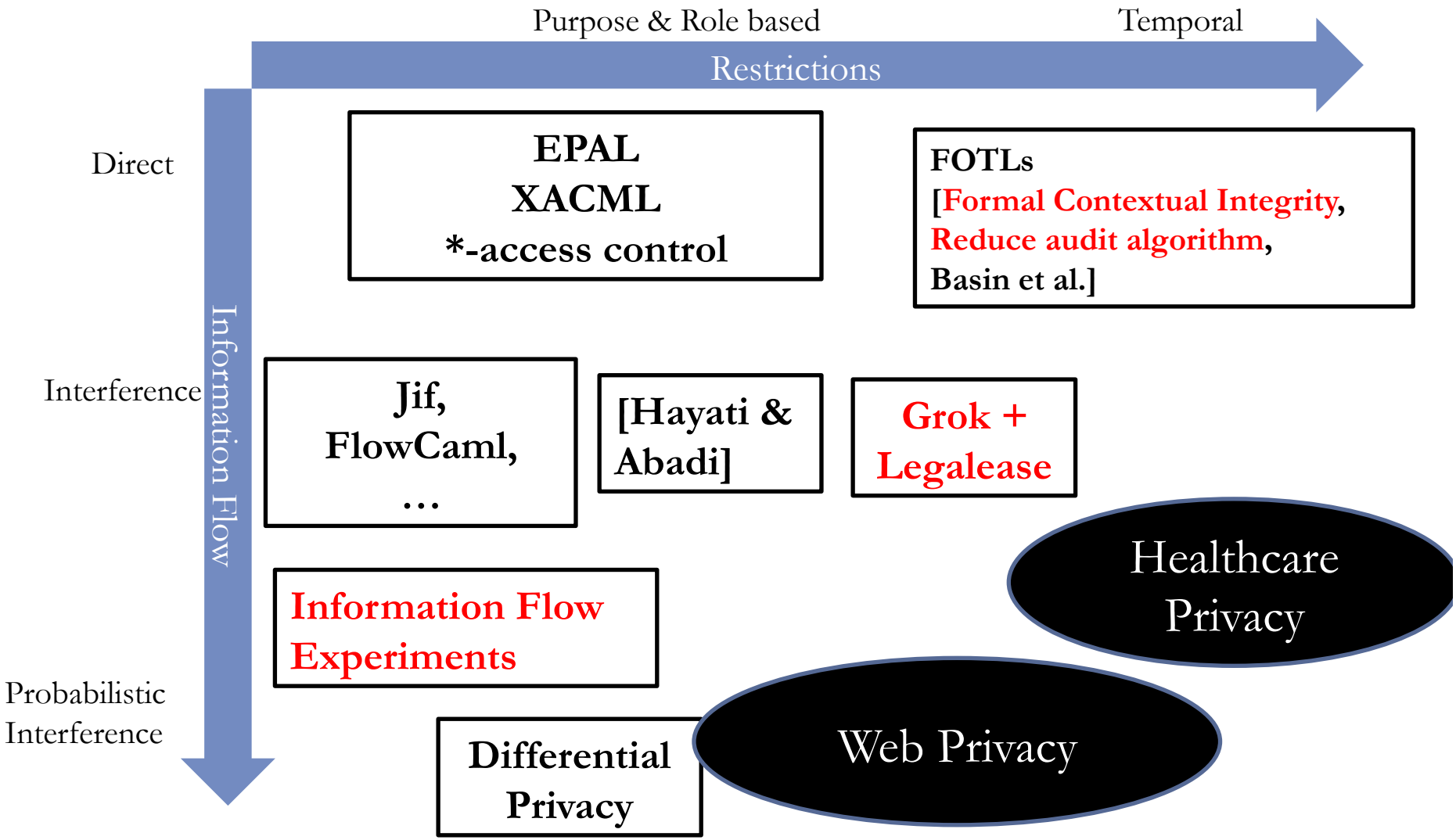
PrivacyLFP [WPES'10]

- **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?

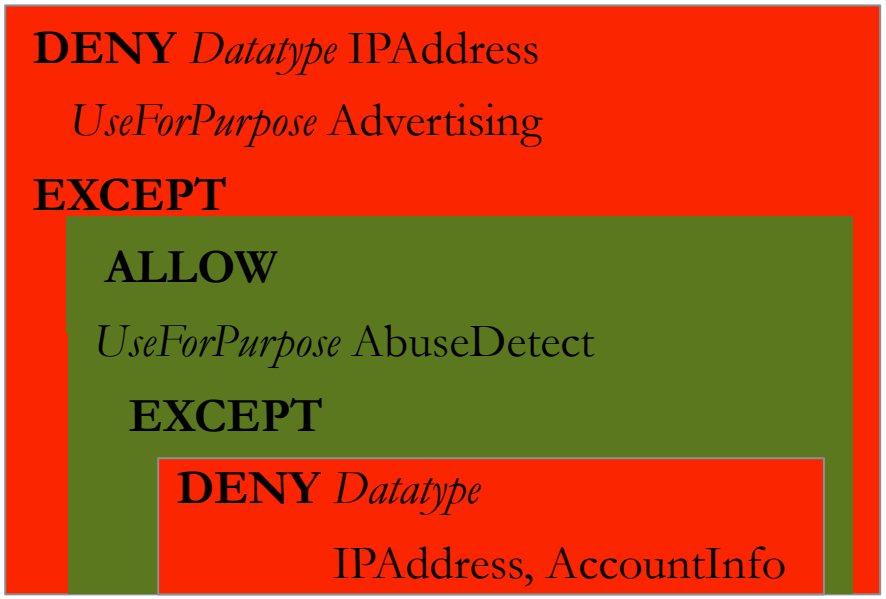
Challenges

- **Precision**
- **Expressiveness**
  - Semantics behind privacy policies is complex
  - Enforcement mechanisms need precise semantics
- **Usability**

Privacy as Restrictions on Personal Information Flow



Legalease: Example Policy [Oakland S&P 2014]



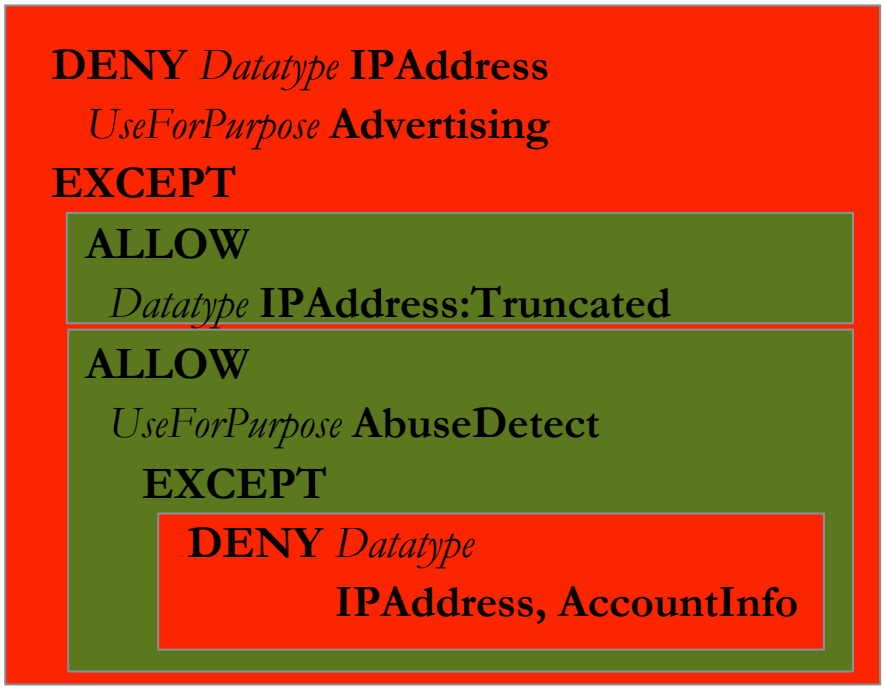
We will **not** use **full IP Address** for **Advertising**.

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

Designed for Usability



Exceptions

How legal texts are structured

One-to one correspondence

Local Reasoning

Each exception refines its immediate parent

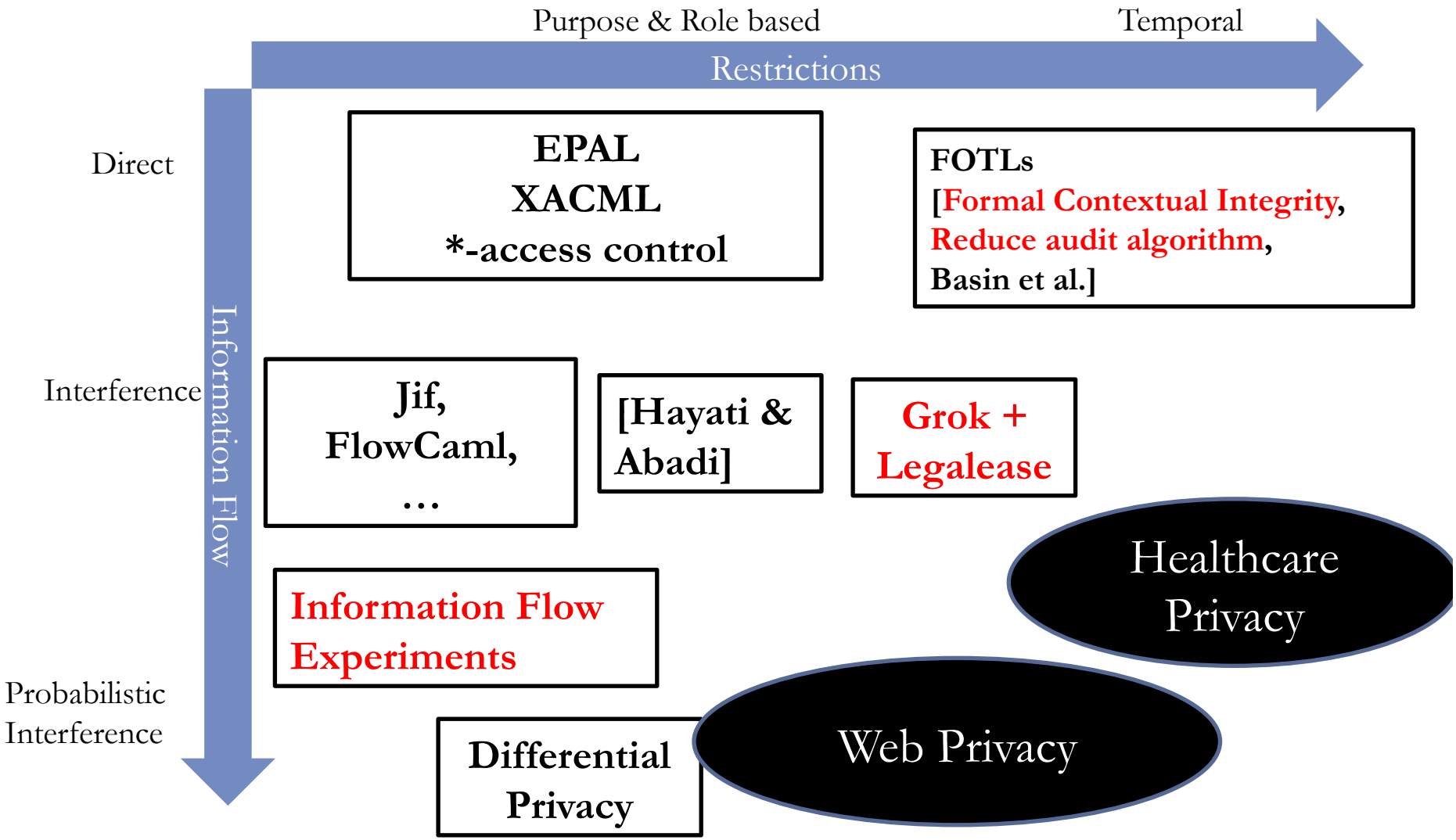
Formally proven property

Independent of Code

Legalease

Usable. Expressive. Precise.	Usable by lawyers and privacy champs.	Expressive enough for real-world policies.	Precise semantics for local reasoning.

Privacy as Restrictions on Personal Information Flow



References

- **Experiences in the Logical Specification of the HIPAA and GLBA Privacy Laws. In *WPES* 2010.**
- **Auditing over Incomplete Logs: Theory, Implementation and Applications. In *CCS* 2011.**
- **Temporal Mode-Checking for Runtime Monitoring of Privacy Policies. In *CAV* 2014.**
- **Bootstrapping Privacy Compliance in Big Data Systems. In *Oakland S&P* 2014.**
- **Equivalence-based Security for Querying Encrypted Databases: Theory and Application to Privacy Policy Audits. In *CCS* 2015.**
- **http://www.andrew.cmu.edu/user/danupam/privacy.html**