Legal Research Overview

Privacy Tools for Sharing Research Data Project

Summer 2015 Tutorial

What is privacy?

“The claim of individuals, groups, or institutions, to determine for themselves when, how, and to what extent information about them is communicated to others.”

- Alan Westin

What is privacy law?

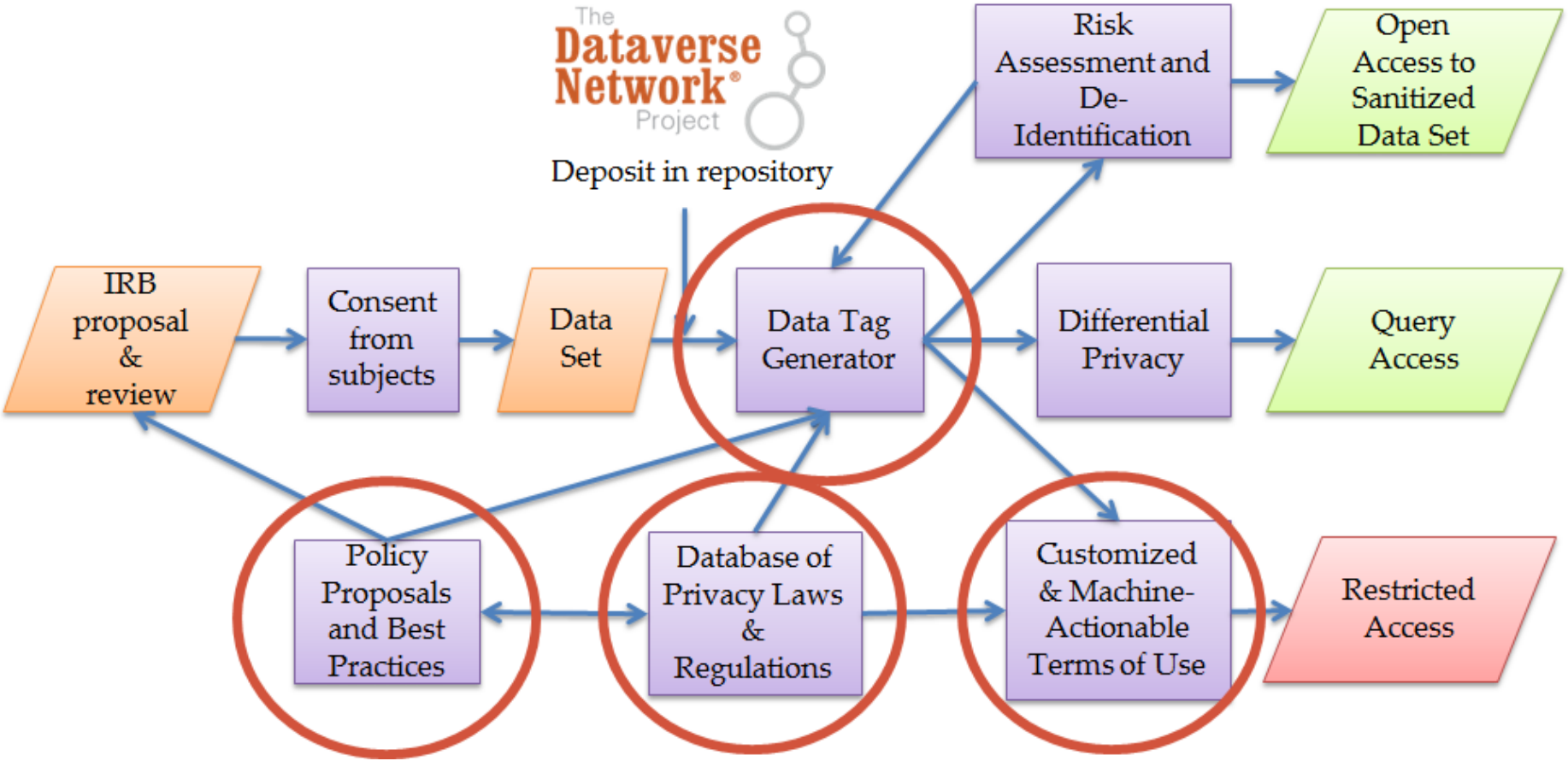
- Patchwork of constitutional provisions, tort laws, federal and state statutes, regulations, agency interpretations and guidance, judicial opinions, contracts . . .
- Restrict disclosures of identifiable or sensitive information about individuals

Project Goals

1. Develop improved conceptions, definitions, and measures of privacy and utility that bridge legal and technical approaches.
2. Develop finely-tailored suite of legal tools to complement new technical approaches to preserving privacy in the collection, storage, use, and sharing of sensitive human subject data.

Our Team

- **Principal Investigator** Prof. Urs Gasser
- **Senior Researcher** David O'Brien
- **Research Fellow** Alexandra Wood
- **Summer Interns** Rod Ghaemmaghami
  Grant Nelson
  Sandra Rubinchik
  Patrick Moore


The Dataverse Network® Project
Deposit in repository
IRB proposal & review
Consent from subjects
Data Set
Data Tag Generator
Risk Assessment and De-Identification
Open Access to Sanitized Data Set
Differential Privacy
Query Access
Policy Proposals and Best Practices
Database of Privacy Laws & Regulations
Customized & Machine-Actionable Terms of Use
Restricted Access

Contributions

- Database of privacy laws & scholarship
- Legal memos
- Policy research
- DataTags
- Data sharing licenses
- Privacy definitions

Database of privacy laws & scholarship

Cataloging federal and state statutes and regulations concerning information privacy

- Types of information and entities covered
- Privacy definitions
- Harms sought to prevent
- Enforcement mechanisms

Legal memos

Analyzing privacy laws and how they apply in the research context

- Human subjects protection laws: Common Rule
- Health records privacy laws: HIPAA Privacy and Security Rules & Substance abuse confidentiality regs.
- Education records privacy laws: FERPA & the Protection of Pupil Rights Amendment
- Government records privacy laws: CIPSEA, Privacy Act, Title 13 (Census Bureau)

Policy research

2014

- Submitted comments to federal agencies (OSHA, FTC, OSTP) on regulatory developments related to information privacy

2015

- Participated in UC Berkeley Open Data symposium
- Submitted a paper on a policy framework for privacy analysis in open government data

Open data paper

Identifies gaps in current practices

1. Most agencies address privacy by withholding or redacting records that contain certain pieces of directly or indirectly identifying information.
2. Agencies lack formal guidance on privacy protection.
3. Similar privacy risks (or even identical data) are treated differently by different government actors.

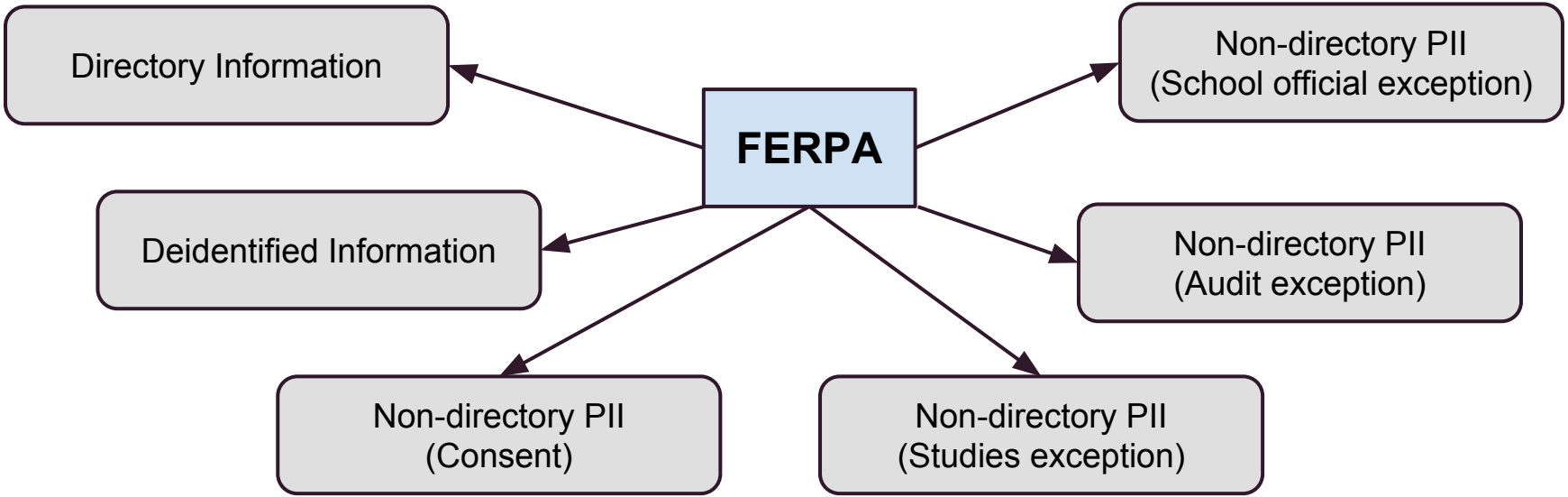
Open data paper

Proposes a new framework for privacy analysis

1. Identifying privacy vulnerabilities and threats
2. Identifying information uses and evaluating utility
3. Aligning use, vulnerabilities, and threats with privacy controls at each stage of the information lifecycle

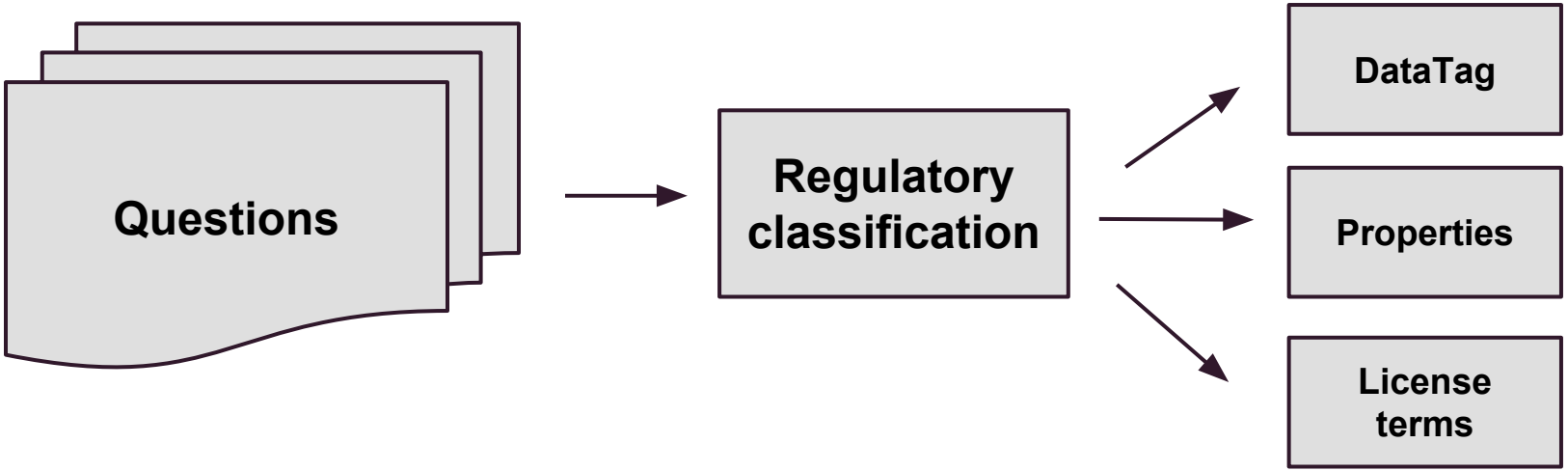
DataTags prototype development

1. Generating categories based on the regulations

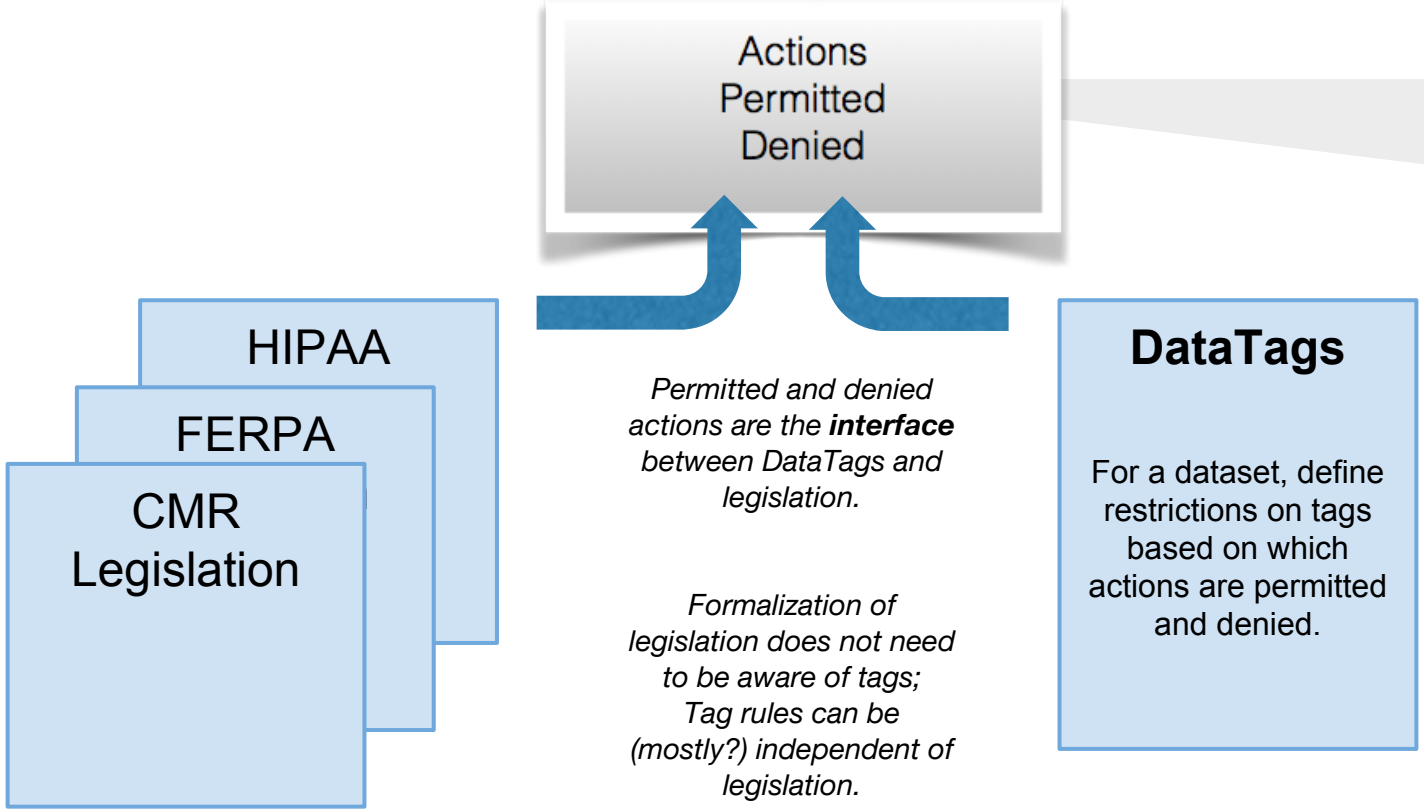


DataTags prototype development

2. Generating annotated questionnaires



DataTags formal framework



Data sharing licenses

Analyzing data use agreements

- Collecting and cataloging data use agreements, terms of services, and policies of data repositories, academic institutions, government agencies, and businesses

Data sharing licenses

Analyzing data use agreements

- Clustering license terms that address:
  - Data ownership
  - Conditions on sharing and use
  - Liability assignment
  - Enforcement mechanisms
  - De-identification standards
  - Security requirements

Data sharing licenses

Drafting modules of license terms for different classifications of data

- Medical records (HIPAA)
- Education records (FERPA & PPRA)
- Government records (CIPSEA, Privacy Act)

Definitions

Exploring legal and mathematical definitions of privacy

- Literature review of deidentification standards from regulations and guidance
- Educational document on privacy, deidentification, and differential privacy
- Differential privacy and the law: comparing definitions through threat modeling

Plans for this summer

Analyzing new laws and PII definitions

- State-level privacy laws: Massachusetts and New York
- White House's Consumer Privacy Bill of Rights

Plans for this summer

Refining formal framework for DataTags

- Testing application of framework to additional laws (FERPA, HIPAA, Common Rule)
- Incorporating license terms into the framework

Plans for this summer

Preparing legal memos and annotated questionnaires for publication

- Developing use cases to illustrate common approaches, gaps, and barriers within current legal and regulatory framework