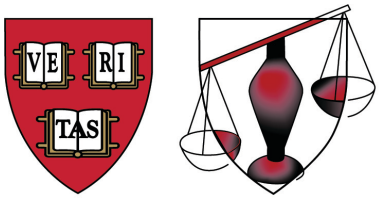


Berkman

The Berkman Center for Internet & Society
at Harvard University

Legal Work in Privacy Tools

David O'Brien
Alexandra Wood

overview

- team
- what is privacy?
- legal approaches to privacy
- law in the project
- goals for this summer

team

- Prof. Urs Gasser (co-PI)
- David O'Brien
- Alexandra Wood
- Chris Bavitz (cyberlaw clinic)
- 2014 summer interns:
  - Jeremy Merkel
  - Anna Myers
  - Brett Weinstein
  - Bryan Lee (arriving next week)

Prof. Urs Gasser (co-PI)

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 it for?

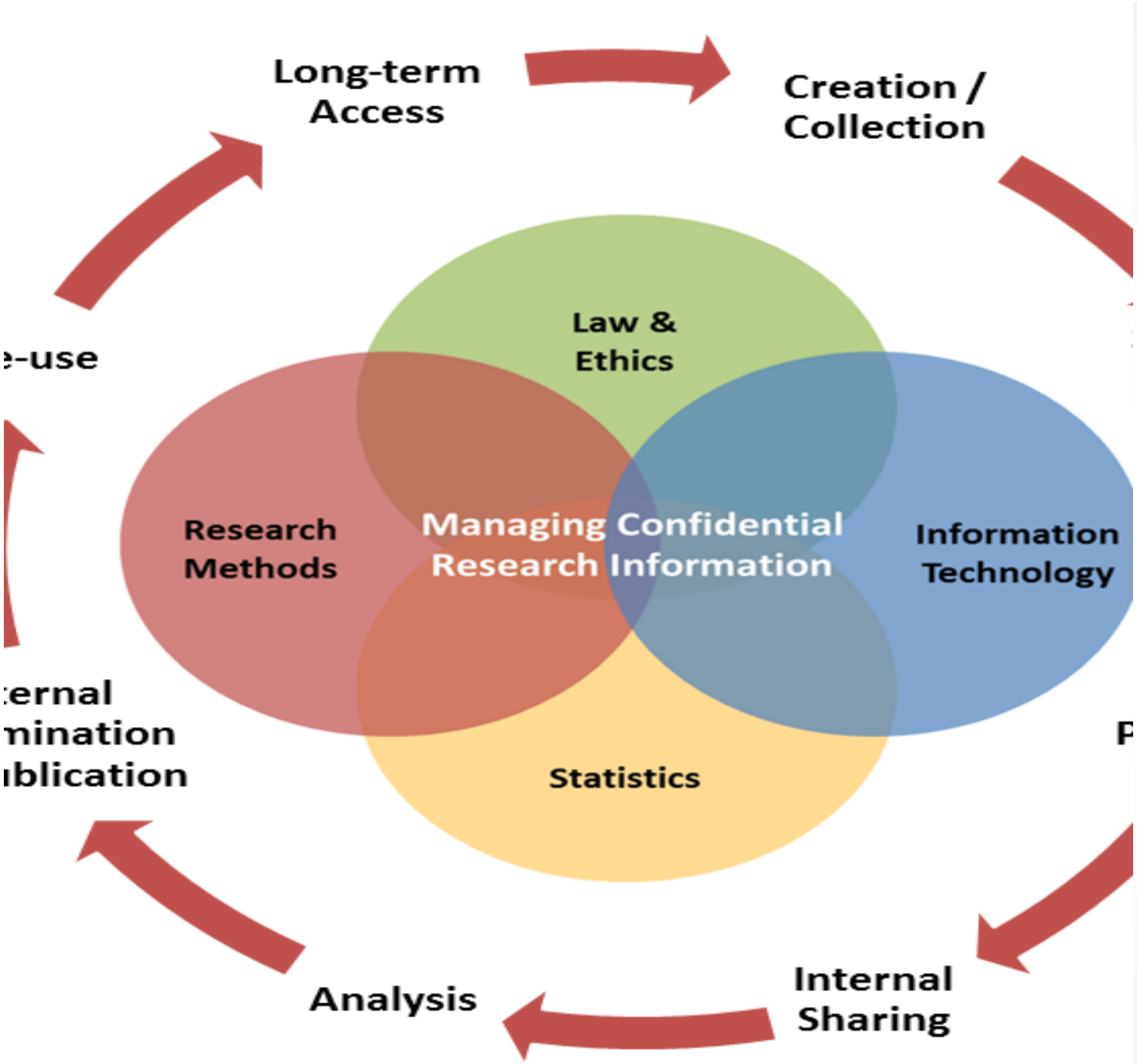
- a function of generally accepted social norms
- access to information about the self – gradients between *public* and *private*
- individuality, personhood, intimacy, dignity, reputation, and autonomy
- freedom to inquire
- enabler of creativity, counter-culture
- control over information; power

sources of governance

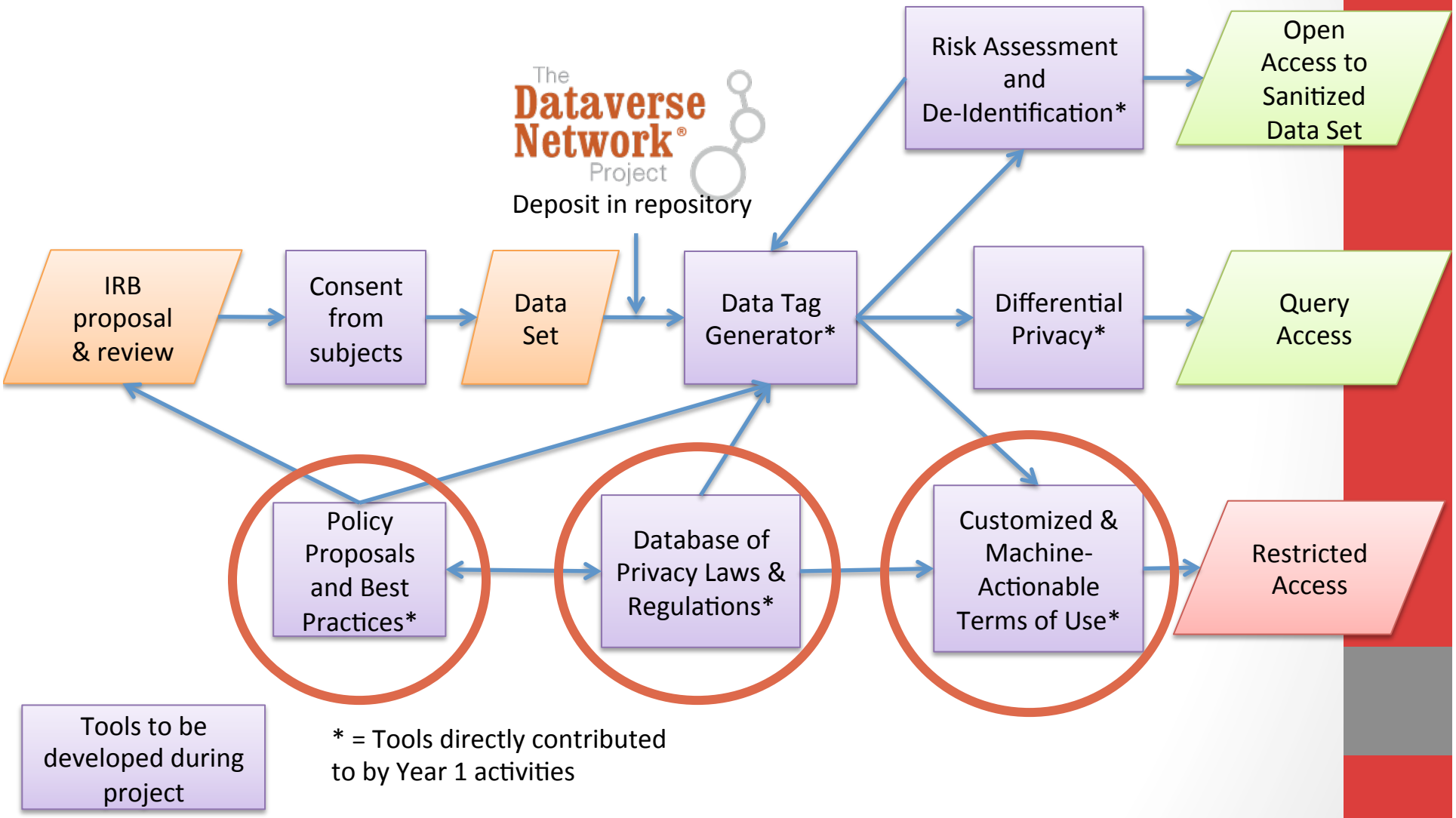
- constitutional Law (limits on government action)
  - fourth amendment
  - first amendment
- written law (statutes, regulations)
  - FERPA
  - HIPAA
  - common rule research regulations
  - various state laws
- common law (judicially developed)
  - judicial opinions, precedent of statutes
  - torts – civil injuries
  - contracts

sources of governance

- constitutional Law (limits on government action)
  - fourth amendment
  - first amendment
- written law (statutes, regulations)
  - FERPA
  - HIPAA
  - common rule research regulations
  - various state laws
- common law (judicially developed)
  - judicial opinions, precedent of statutes
  - torts – civil injuries
  - contracts


Long-term Access
Creation / Collection
Law & Ethics
Research Methods
Managing Confidential Research Information
Information Technology
Statistics
Internal Sharing
Analysis

BCIS contributions



BCIS goals

1. develop improved conceptions, definitions, and measures of privacy and data 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

current work – analyzing DUAs

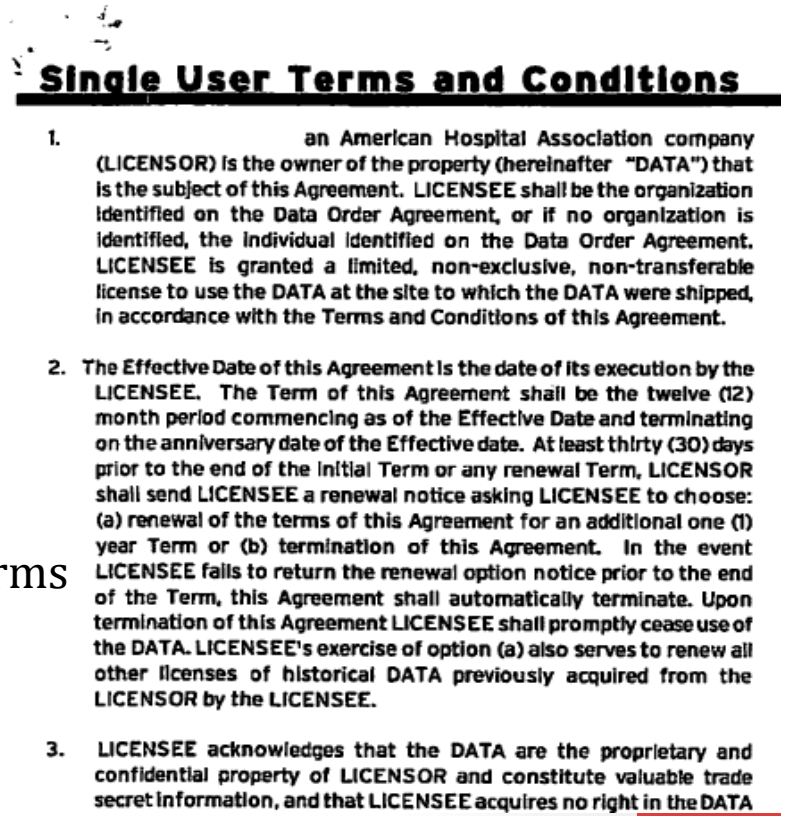
Collecting and analyzing data use agreements, terms of service, and policies of data repositories, academic institutions, government agencies, and businesses to assess practices towards:

- Data ownership
- Conditions on sharing, use
- Liability assignment
- Enforcement mechanisms
- Security and de-identification standards

Impact: Critical input for developing enhanced terms of service, DUAs, privacy tags, DUA generator, and other instruments. Helpful for understanding working definitions in practice

Output: Upcoming paper based on research

150+ DUAs collected and analyzed



Single User Terms and Conditions

1. an American Hospital Association company (LICENSOR) is the owner of the property (hereinafter "DATA") that is the subject of this Agreement. LICENSEE shall be the organization identified on the Data Order Agreement, or if no organization is identified, the individual identified on the Data Order Agreement. LICENSEE is granted a limited, non-exclusive, non-transferable license to use the DATA at the site to which the DATA were shipped, in accordance with the Terms and Conditions of this Agreement.

2. The Effective Date of this Agreement is the date of its execution by the LICENSEE. The Term of this Agreement shall be the twelve (12) month period commencing as of the Effective Date and terminating on the anniversary date of the Effective date. At least thirty (30) days prior to the end of the initial Term or any renewal Term, LICENSOR shall send LICENSEE a renewal notice asking LICENSEE to choose: (a) renewal of the terms of this Agreement for an additional one (1) year Term or (b) termination of this Agreement. In the event LICENSEE fails to return the renewal option notice prior to the end of the Term, this Agreement shall automatically terminate. Upon termination of this Agreement LICENSEE shall promptly cease use of the DATA. LICENSEE's exercise of option (a) also serves to renew all other licenses of historical DATA previously acquired from the LICENSOR by the LICENSEE.

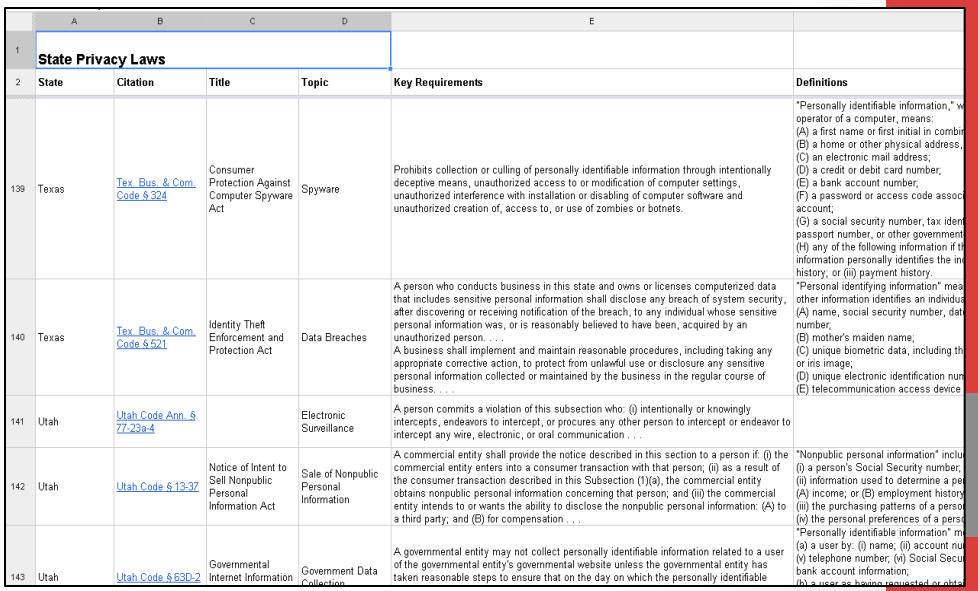
3. LICENSEE acknowledges that the DATA are the proprietary and confidential property of LICENSOR and constitute valuable trade secret information, and that LICENSEE acquires no right in the DATA

current work – fed/state laws

Cataloging existing federal and state statutes and regulations concerning information privacy, with an eye towards:

More than 200 laws reviewed

- Type of information governed
- Privacy Definitions
- Harms sought to prevent
- Enforcement mechanisms
- Other requirements



	A	B	C	D	E	
1	**State Privacy Laws**					
2	**State**	**Citation**	**Title**	**Topic**	**Key Requirements**	**Definitions**
139	Texas	Tex. Bus. & Com. Code § 324	Consumer Protection Against Computer Spyware Act	Spyware	Prohibits collection or culling of personally identifiable information through intentionally deceptive means, unauthorized access to or modification of computer settings, unauthorized interference with installation or disabling of computer software and unauthorized creation of, access to, or use of zombies or botnets.	"Personally identifiable information," w operator of a computer, means: (A) a first name or first initial in combi (B) a home or other physical address, (C) an electronic mail address; (D) a credit or debit card number; (E) a bank account number; (F) a password or access code associ account; (G) a social security number, tax iden passport number, or other governmen (H) any of the following information if th information personally identifies the in history; or (iii) payment history.
140	Texas	Tex. Bus. & Com. Code § 521	Identity Theft Enforcement and Protection Act	Data Breaches	A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. . . . A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. . . .	"Personal identifying information" mea other information identifies an individu (A) name, social security number, dat number; (B) mother's maiden name; (C) unique biometric data, including th or iris image; (D) unique electronic identification nu (E) telecommunication access device
141	Utah	Utah Code Ann. § 77-23a-4		Electronic Surveillance	A person commits a violation of this subsection who: (i) intentionally or knowingly intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic, or oral communication . . .	
142	Utah	Utah Code § 13-37	Notice of Intent to Sell Nonpublic Personal Information Act	Sale of Nonpublic Personal Information	A commercial entity shall provide the notice described in this section to a person if: (i) the commercial entity enters into a consumer transaction with that person; (ii) as a result of the consumer transaction described in this Subsection (1)(a), the commercial entity obtains nonpublic personal information concerning that person; and (iii) the commercial entity intends to or wants the ability to disclose the nonpublic personal information: (A) to a third party; and (B) for compensation . . .	"Nonpublic personal information" inclu (i) a person's Social Security number; (ii) information used to determine a pe (A) income; or (B) employment history (iii) the purchasing patterns of a perso (iv) the personal preferences of a pers
143	Utah	Utah Code § 63D-2	Governmental Internet Information	Government Data Collection	A governmental entity may not collect personally identifiable information related to a user of the governmental entity's governmental website unless the governmental entity has taken reasonable steps to ensure that on the day on which the personally identifiable	"Personally identifiable information" m (a) a user by: (i) name; (ii) account nu (v) telephone number; (vi) Social Secu bank account information;

current work – policy

Comments on **statutory and regulatory developments** related to information privacy

examples: OSHA and OSTP

OSHA® Occupational Safety and Health Administration
www.osha.gov

current work – data tags

Collaborating with IQSS/DPL and CRCS team members on the early stages of the data tags workstream

Data Tags: Tools to embed privacy characteristics into a dataset, and perhaps individual elements of data within the set, so they are persistent over the flow and lifecycle of that information.

current work – data tags

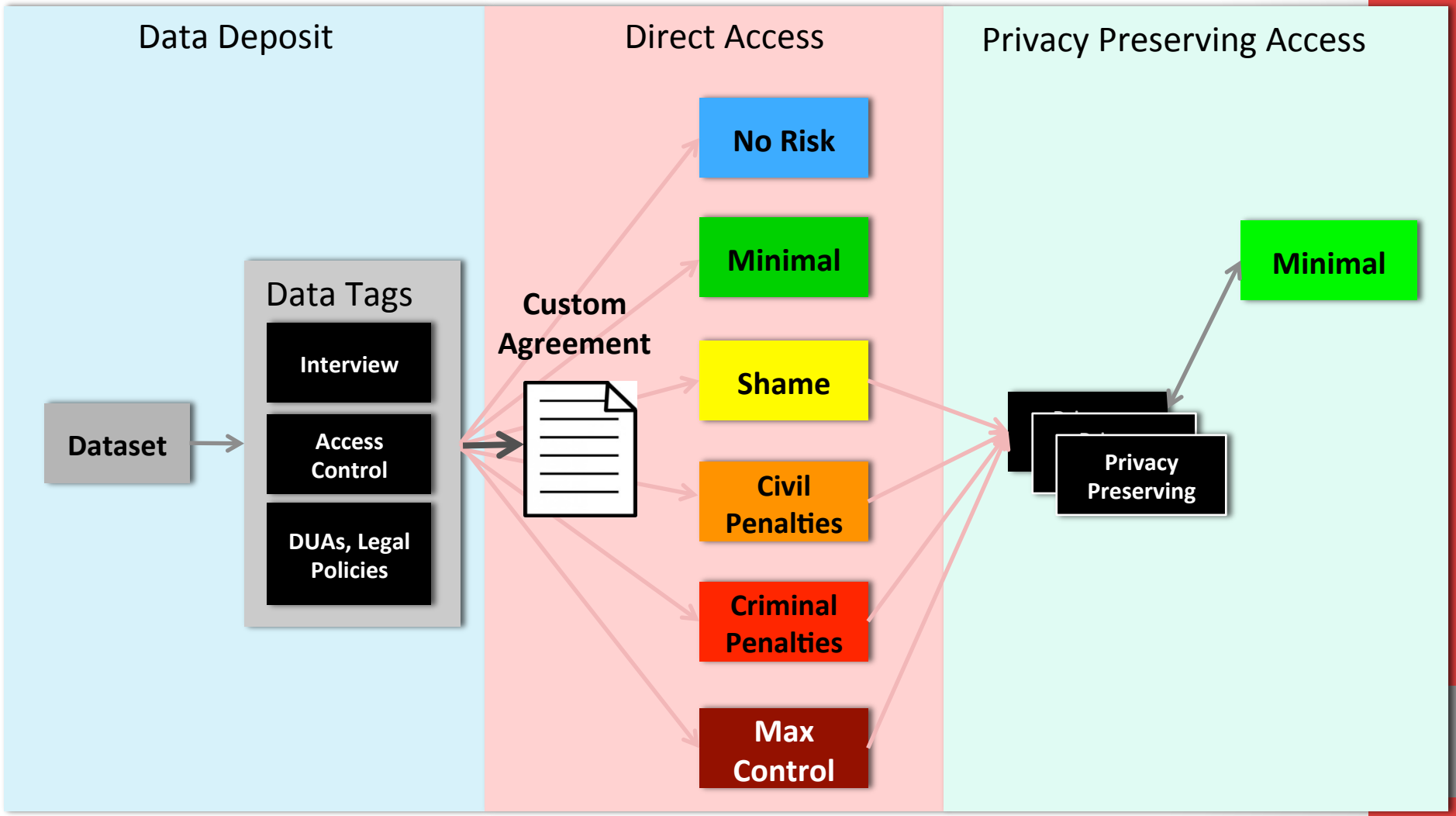
Interview wizard: question tool for assessing tags prior to data deposit

- Developing draft questions based on laws and common DUA terms

DUA generator: tool for generating customized legal code tailored for each dataset ingested

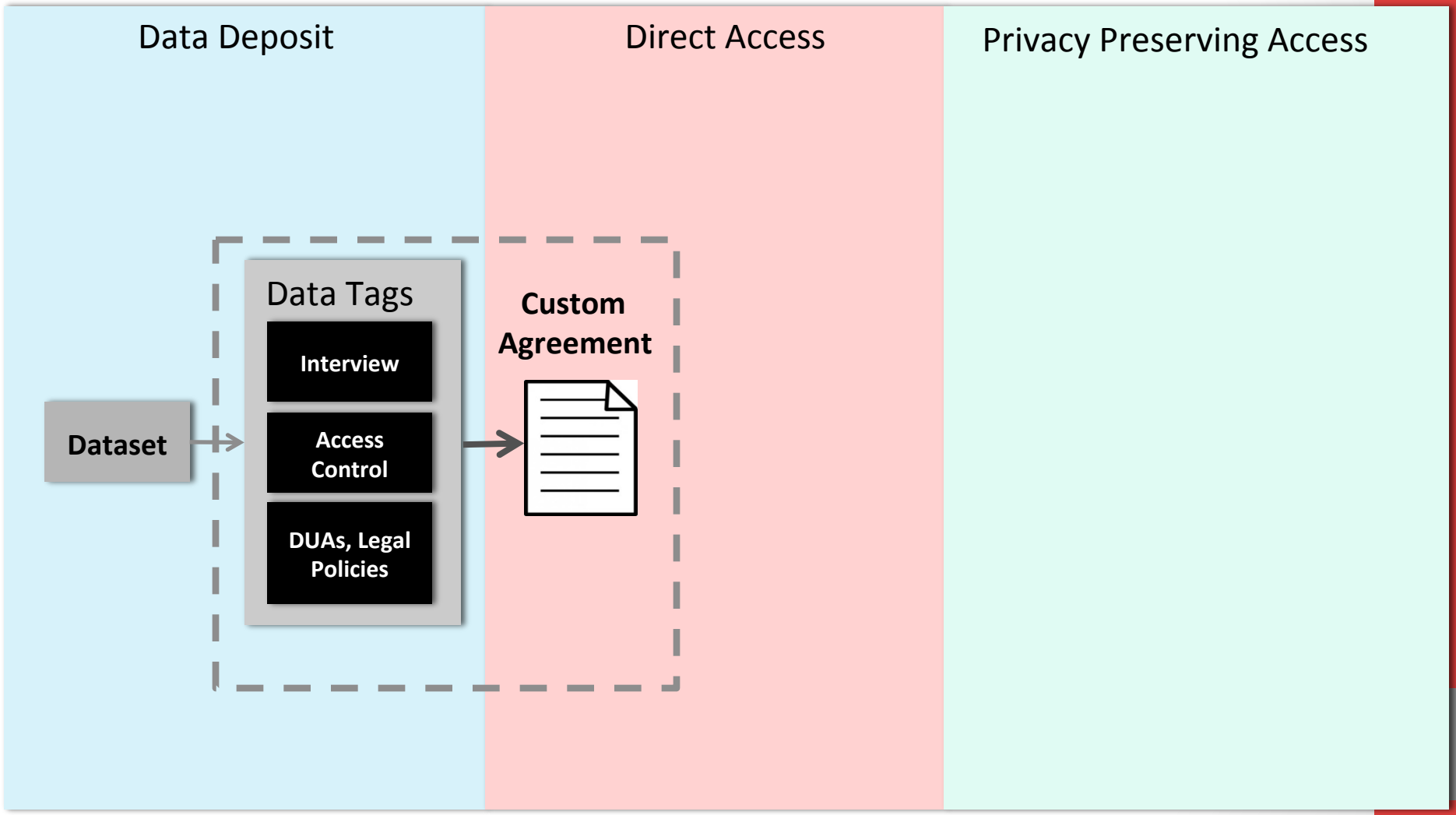
- Developing modularized contract provisions based on tags and researcher needs

current work – data tags



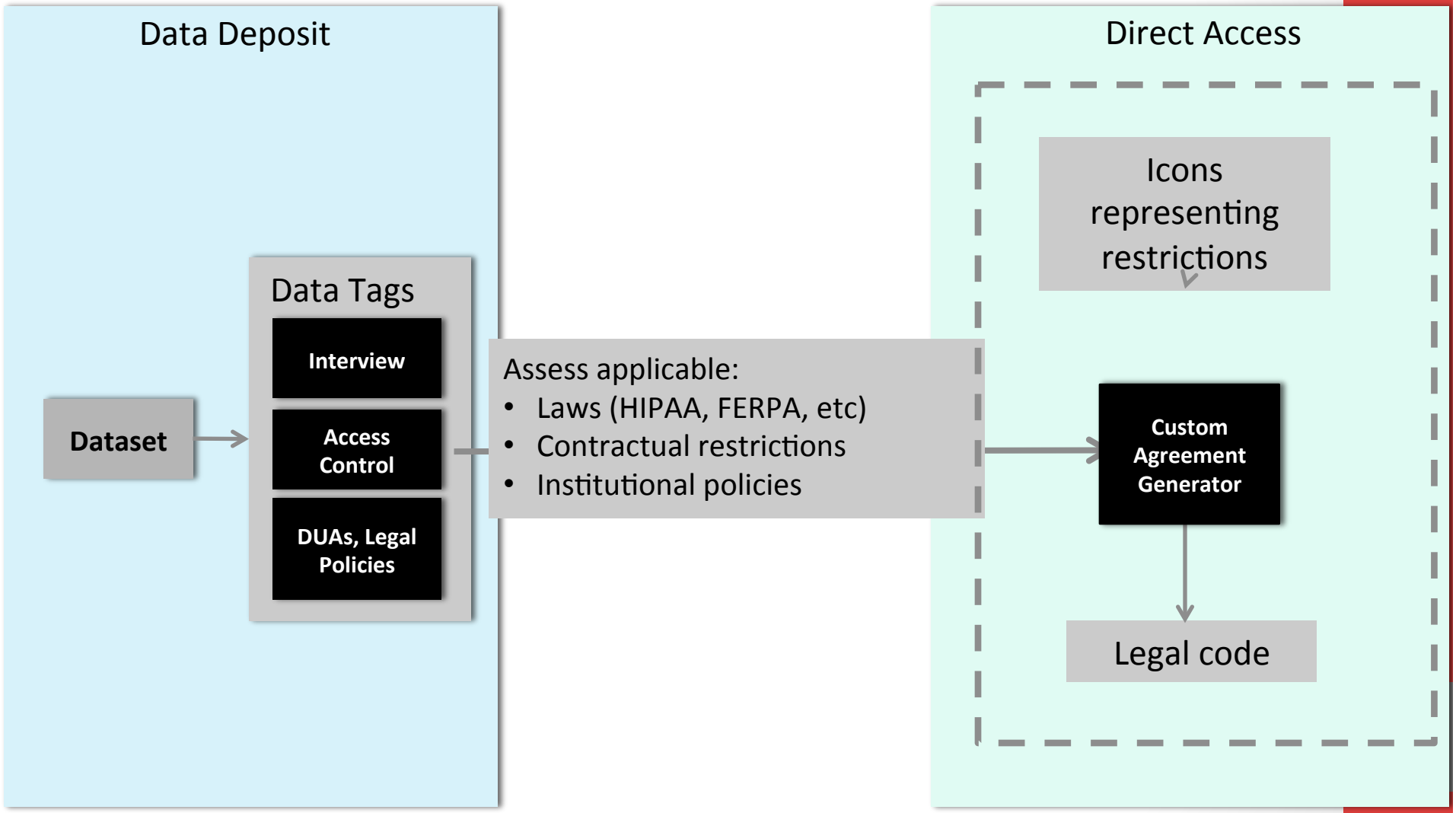
Data Deposit, transfer, storage and access through the **Dataverse Network**

current work – data tags



Data Deposit, transfer, storage and access through the **Dataverse Network**

current work – data tags



Data Deposit, transfer, storage and access through the **Dataverse Network**

goals for the summer

- Data Tags prototype
- Draft modular license agreement
- Foundational research on privacy definitions and frameworks

data tags prototype

- **Objective:** To develop a prototype of Data Tags that is ready for testing by users
- Creating an **annotated questionnaire** covering three categories of datasets:
  - Datasets containing **medical records**
  - Datasets containing **education records**
  - Datasets with preexisting **data use agreements**
- Beginning work on datasets containing **government records**

draft modular license agreement

- **Objective:** To develop a first draft of the modular license agreement
- Creating an agreement **template** based on the Dataverse 4.0 data use terms
- Drafting **modules** of terms for the following categories:
  - Medical records
  - Education records
  - Government records
  - Data use agreements

foundational research on privacy definitions and frameworks

- **Objective:** To begin mapping definitions, frameworks for, and approaches to privacy across disciplines
- Drafting a series of memos and briefing documents on
  - Privacy definitions from **statutes, regulations, and case law**
  - Privacy definitions from **other disciplines**