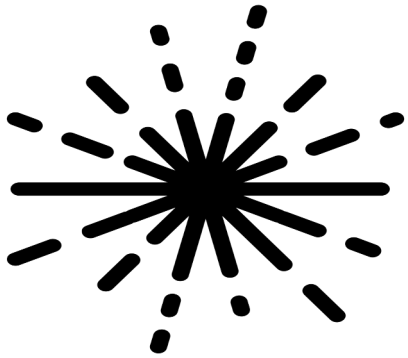


CS208: Applied Privacy for Data Science
Course Overview

Salil Vadhan, James Honaker, Wanrong Zhang,
Jayshree Sarathy, Mike Shoemate

School of Engineering & Applied Sciences
Harvard University

January 18, 2022

Important Announcement

- If you might attend the class *without formally registering this week* (e.g. you want to audit, or might add it later, or will be cross-registering), then please fill out the following Google form by end of today, 1/19: https://forms.gle/7aG5fvcCQTnH6zNj9

- Why?
  - To calibrate size of teaching staff & room
  - To inform you of Harvard COVID policies (esp. for non-Harvard auditors)

Plan for today

- First hour: course overview
  - Salil: motivation & definition of differential privacy
  - Wanrong: the theory of DP
  - James: from theory to practice
  - Jayshree: ethics, law, and society
  - Mike: programming and implementation
  - Salil: class structure
- Second hour: Q & A
  - Group discussion
  - Individual questions in breakout rooms

Data Privacy: The Problem

Given a dataset with sensitive information, such as:

- Census data
- Health records
- Social network activity
- Telecommunications data

- Academic research
- Informing policy
- Identifying subjects for drug trial
- Searching for terrorists
- Market analysis
- …

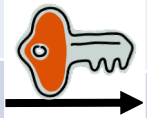
How can we:

- enable “desirable uses” of the data
- while protecting the “privacy” of the data subjects?

????

Approach 1: Encrypt the Data

Name	Sex	Blood		HIV?
Chen	F	B		Y
Jones	M	A		N
Smith	M	O		N
Ross	M	O		Y
Lu	F	A		N
Shah	M	B		Y

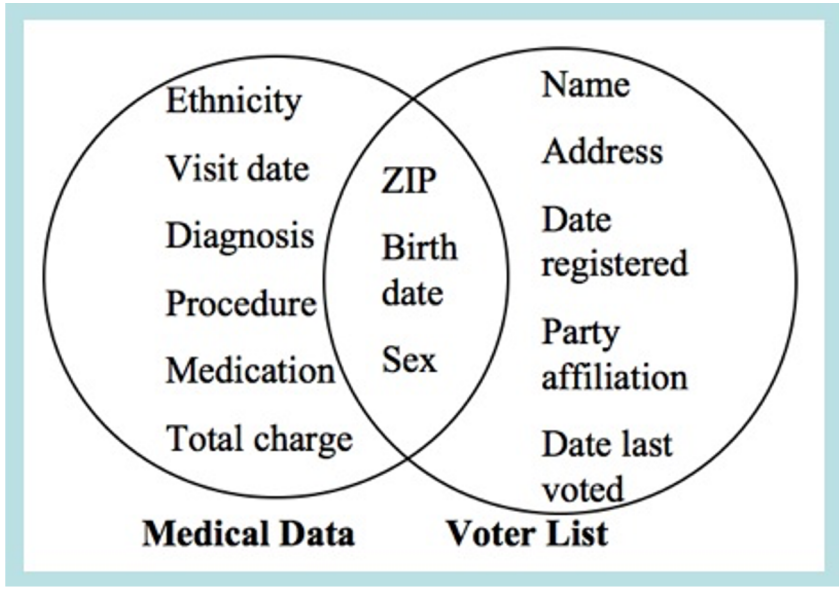


Name	Sex	Blood		HIV?
100101	001001	110101		110111
101010	111010	111111		001001
001010	100100	011001		110101
001110	010010	110101		100001
110101	000000	111001		010010
111110	110010	000101		110101

Problems?

Approach 2: Anonymize the Data

Name	Sex	Blood		HIV?
Chen	F	B		Y
Jones	M	A		N
Smith	M	O		N
Ross	M	O		Y
Lu	F	A		N
Shah	M	B		Y



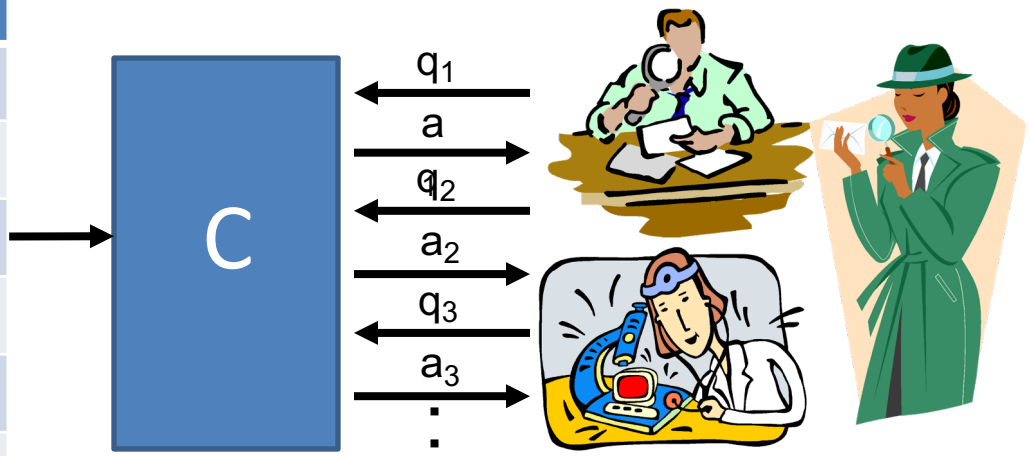
[Sweeney `97]

"re-identification" often easy

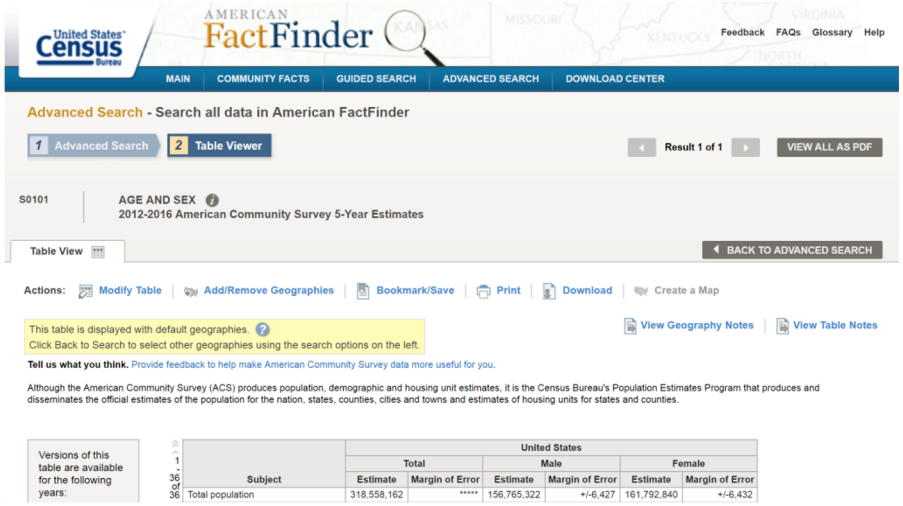
Problems?

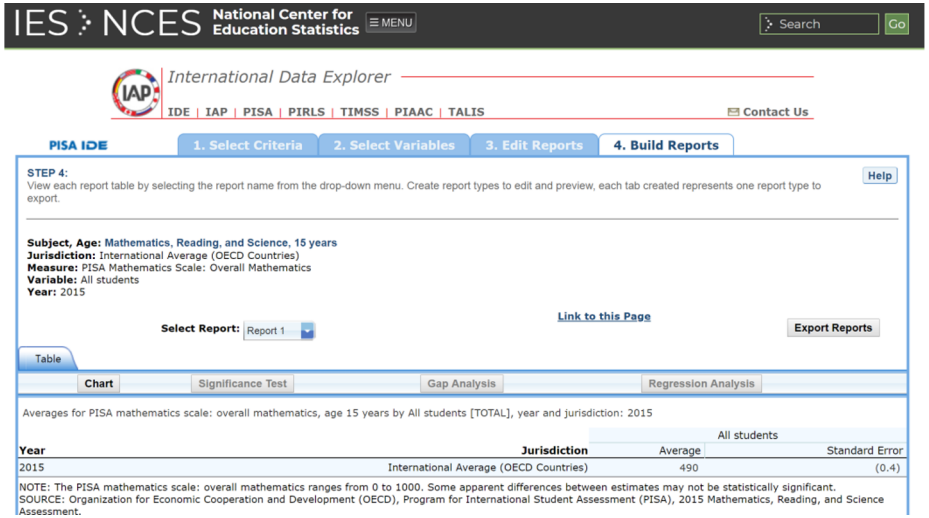
Approach 3: Mediate Access

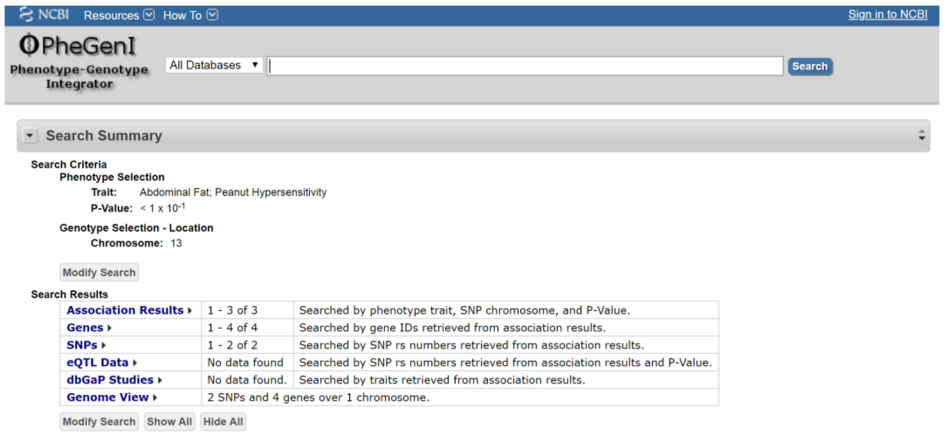
Name	Sex	Blood		HIV?
Chen	F	B		Y
Jones	M	A		N
Smith	M	O		N
Ross	M	O		Y
Lu	F	A		N
Shah	M	B		Y

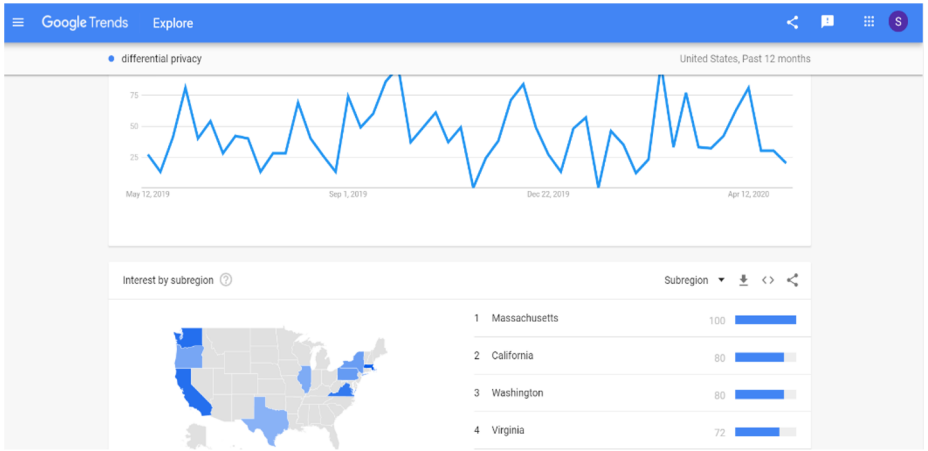


Existing Query Interfaces



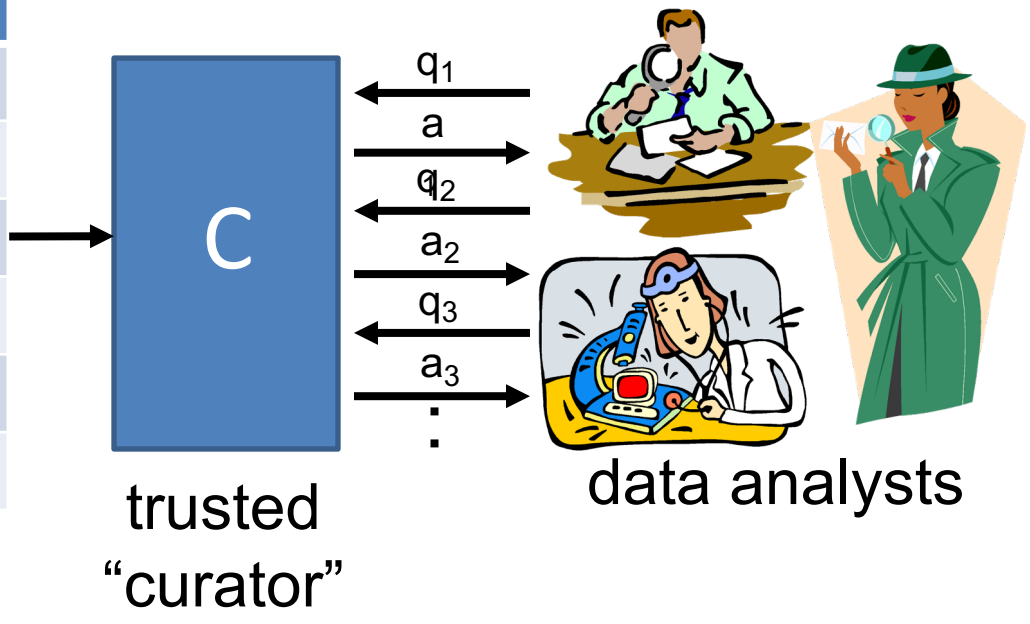






Approach 3: Mediate Access

Name	Sex	Blood		HIV?
Chen	F	B		Y
Jones	M	A		N
Smith	M	O		N
Ross	M	O		Y
Lu	F	A		N
Shah	M	B		Y



Problems?

Privacy Models from Theoretical CS

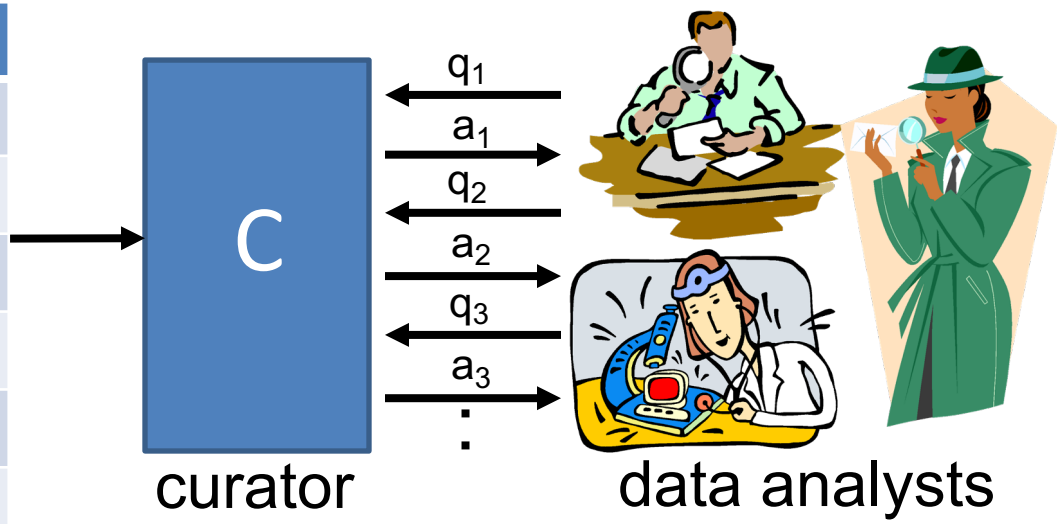
Model	Utility	Privacy	Who Holds Data?
Differential Privacy	statistical analysis of dataset	individual-specific info	trusted curator
Secure Multiparty Computation	any query desired	everything other than result of query	original users (or semi-trusted delegates)
Fully Homomorphic (or Functional) Encryption	any query desired	everything (except possibly result of query)	untrusted server

Differential privacy

[Dinur-Nissim ’03+Dwork, Dwork-Nissim ’04, Blum-Dwork-McSherry-Nissim ’05, Dwork-McSherry-Nissim-Smith ’06]

n

Sex	Blood		HIV?
F	B		Y
M	A		N
M	O		N
M	O		Y
F	A		N
M	B		Y

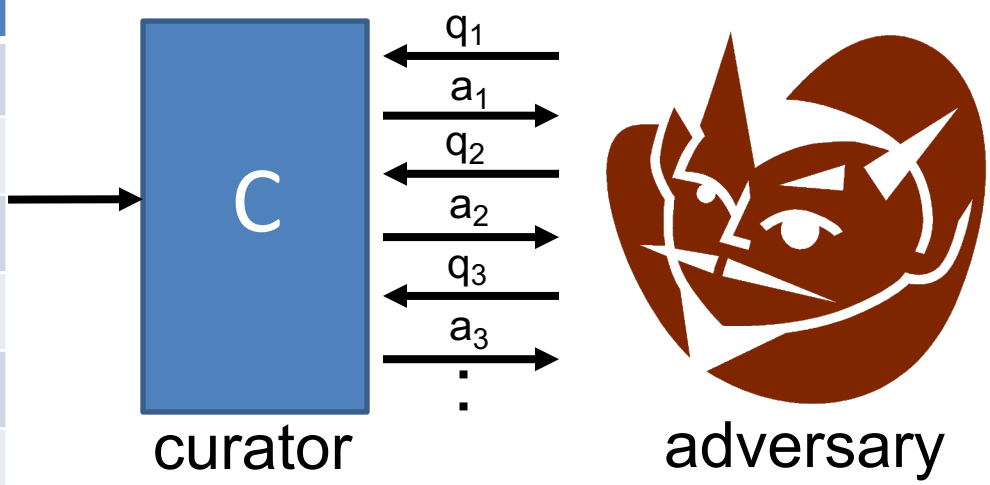


Requirement: effect of each individual should be “hidden”

Differential privacy

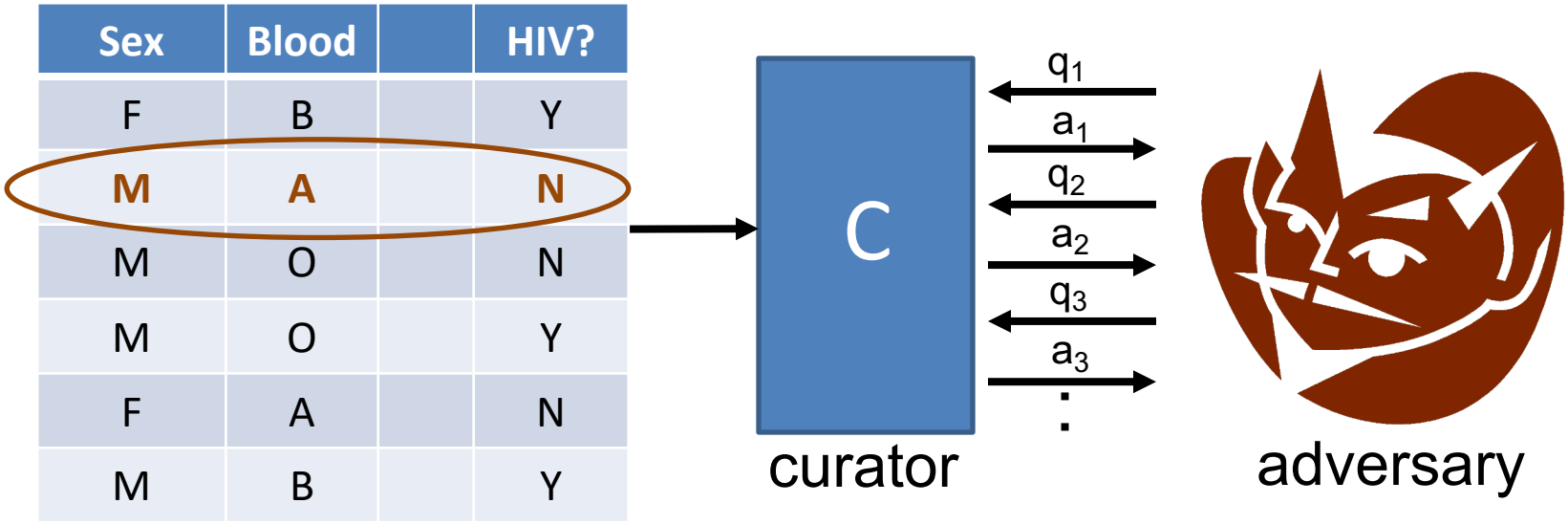
[Dinur-Nissim ’03+Dwork, Dwork-Nissim ’04, Blum-Dwork-McSherry-Nissim ’05, Dwork-McSherry-Nissim-Smith ’06]

Sex	Blood		HIV?
F	B		Y
M	A		N
M	O		N
M	O		Y
F	A		N
M	B		Y



Differential privacy

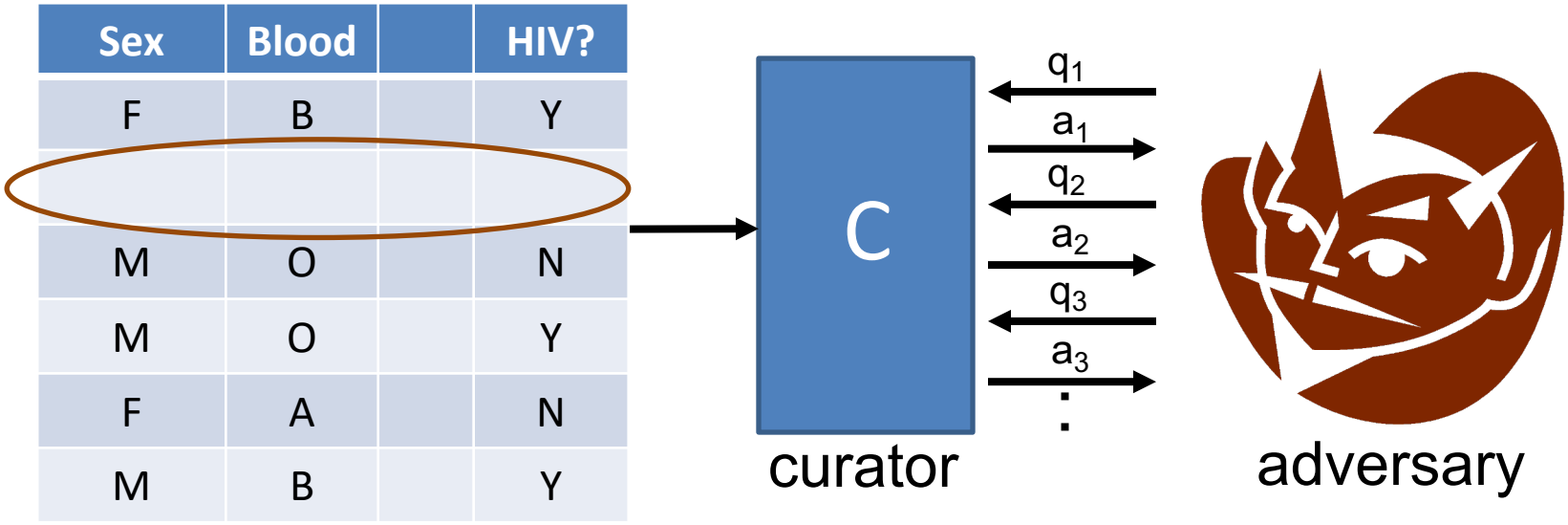
[Dinur-Nissim ’03+Dwork, Dwork-Nissim ’04, Blum-Dwork-McSherry-Nissim ’05, Dwork-McSherry-Nissim-Smith ’06]



Requirement: an adversary shouldn’t be able to tell if any one person’s data were changed arbitrarily

Differential privacy

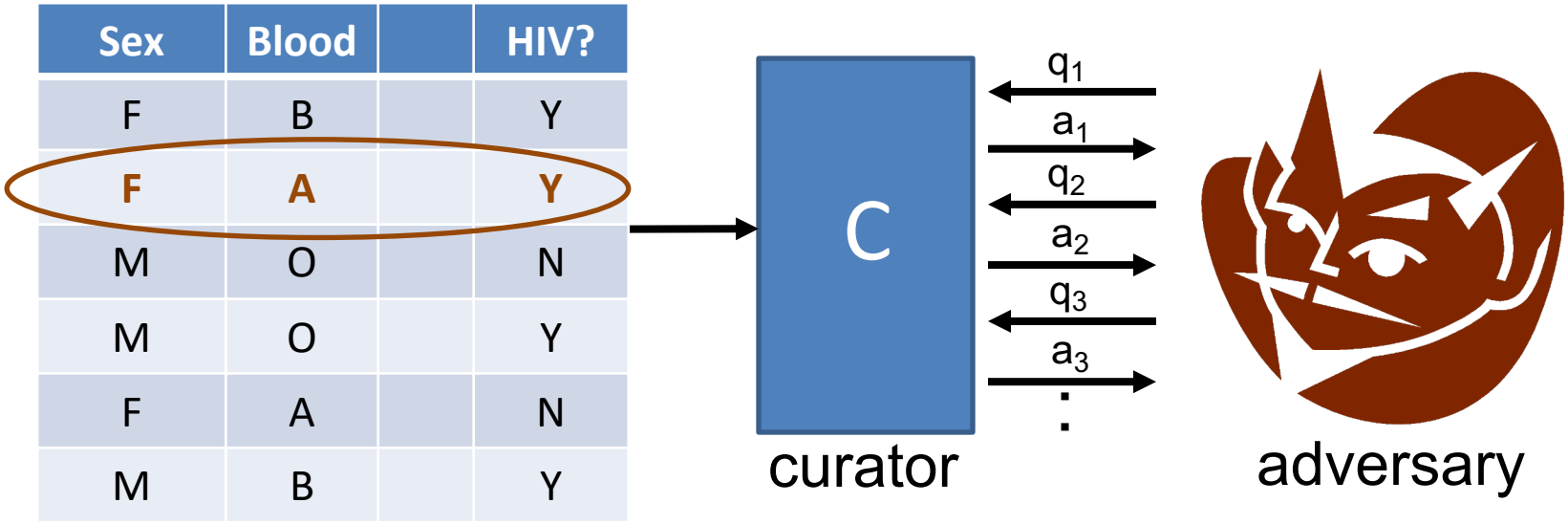
[Dinur-Nissim ’03+Dwork, Dwork-Nissim ’04, Blum-Dwork-McSherry-Nissim ’05, Dwork-McSherry-Nissim-Smith ’06]



Requirement: an adversary shouldn’t be able to tell if any one person’s data were changed arbitrarily

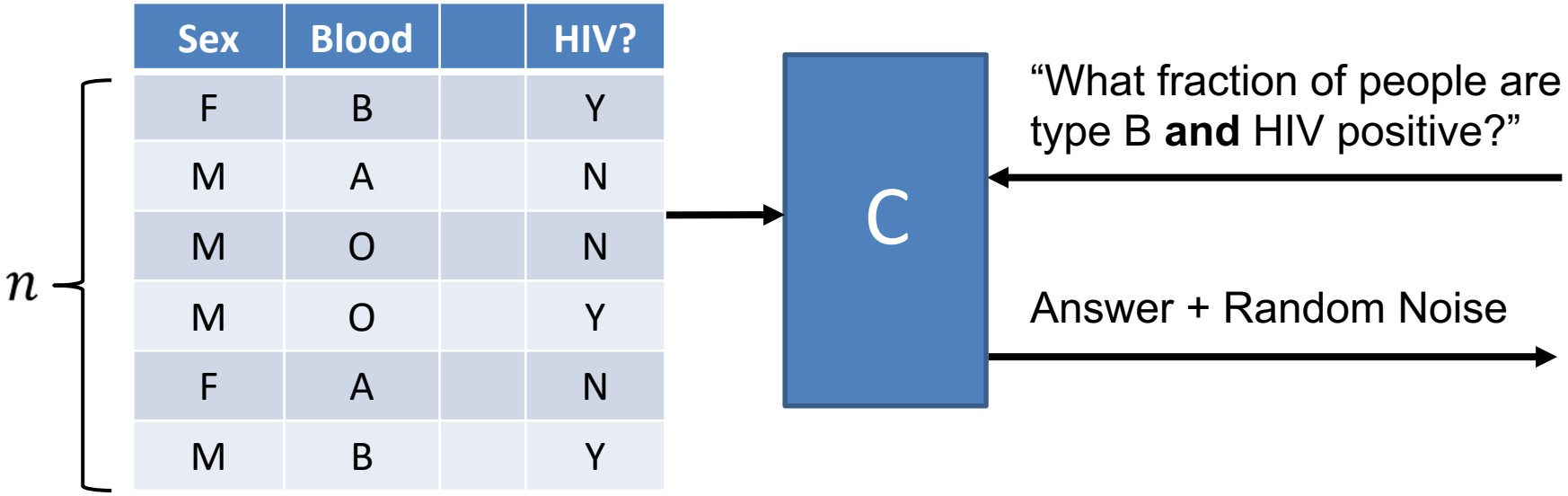
Differential privacy

[Dinur-Nissim ’03+Dwork, Dwork-Nissim ’04, Blum-Dwork-McSherry-Nissim ’05, Dwork-McSherry-Nissim-Smith ’06]



Requirement: an adversary shouldn’t be able to tell if any one person’s data were changed arbitrarily

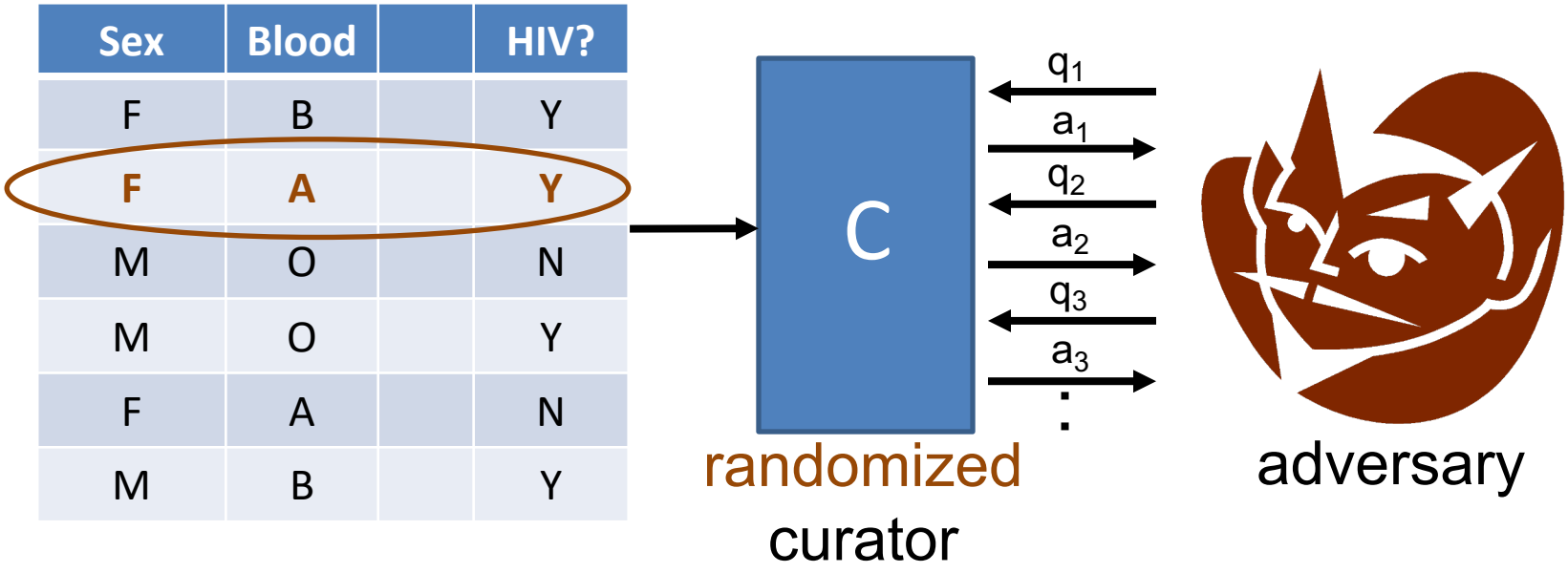
Simple approach: random noise



- Very little noise needed to hide each person as $n \to \infty$.

Differential privacy

[Dinur-Nissim ’03+Dwork, Dwork-Nissim ’04, Blum-Dwork-McSherry-Nissim ’05, Dwork-McSherry-Nissim-Smith ’06]



Requirement: for all D, D’ differing on one row, and all $q_1,\ldots,q_t$

Distribution of $C(D,q_1,\ldots,q_t) \approx_\varepsilon$ Distribution of $C(D',q_1,\ldots,q_t)$

Algorithm Implementation

- OpenDP Library

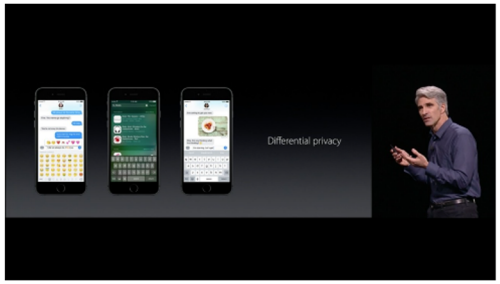
  https://docs.opendp.org

- Common themes:
  - Many algorithms for the same general class of estimator
  - Side-channel-safe sampling algorithms
  - Accounting for finite data representations

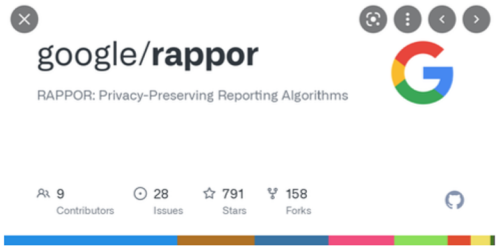
- High demand for robust DP algorithm implementations in industry


Apple will not
see your data

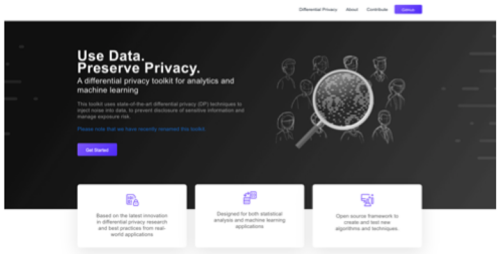
Differential Privacy Deployed



Apple



Google



Microsoft

United States™ Census Bureau

Census Bureau

Uber

Opacus

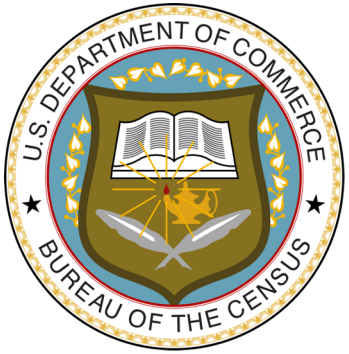
Train PyTorch models with Differential Privacy

Meta

Major Deployments of DP

U.S. Census Bureau

- “OnTheMap” commuter data (2006)
- Planned: all public-use products from 2020 decennial census



Google

- “RAPPOR” for Chrome Statistics (2014)

Microsoft

- SmartNoise (2020)

Apple

- iOS10 and Safari(2016) and PCM (2022)

Harvard Privacy Tools Project

http://privacytools.seas.harvard.edu/

Computer Science, Law, Social Science, Statistics

IQSS
The Institute for Quantitative Social Science
HARVARD UNIVERSITY

CRCS Center for Research on Computation and Society

BERKMAN KLEIN CENTER
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

DATA PRIVACY LAB

OpenDP

OpenDP

A **community effort** to build a **trustworthy** and **open-source** suite of differential privacy tools that can be **easily adopted** by custodians of sensitive data to make it available for **research and exploration** in the public interest.

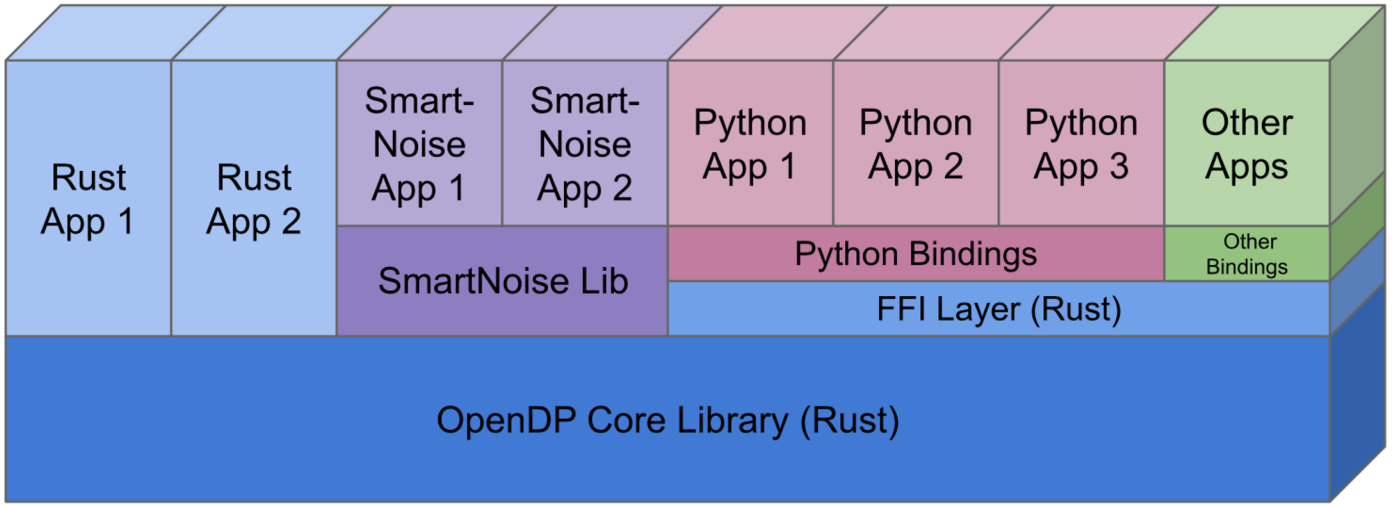
Why?

- Channel our collective advances on science & practice of DP
- Enable wider adoption of DP
- Address high-demand, compelling use cases
- Provide a starting point for custom DP solutions
- Identify important research directions for the field

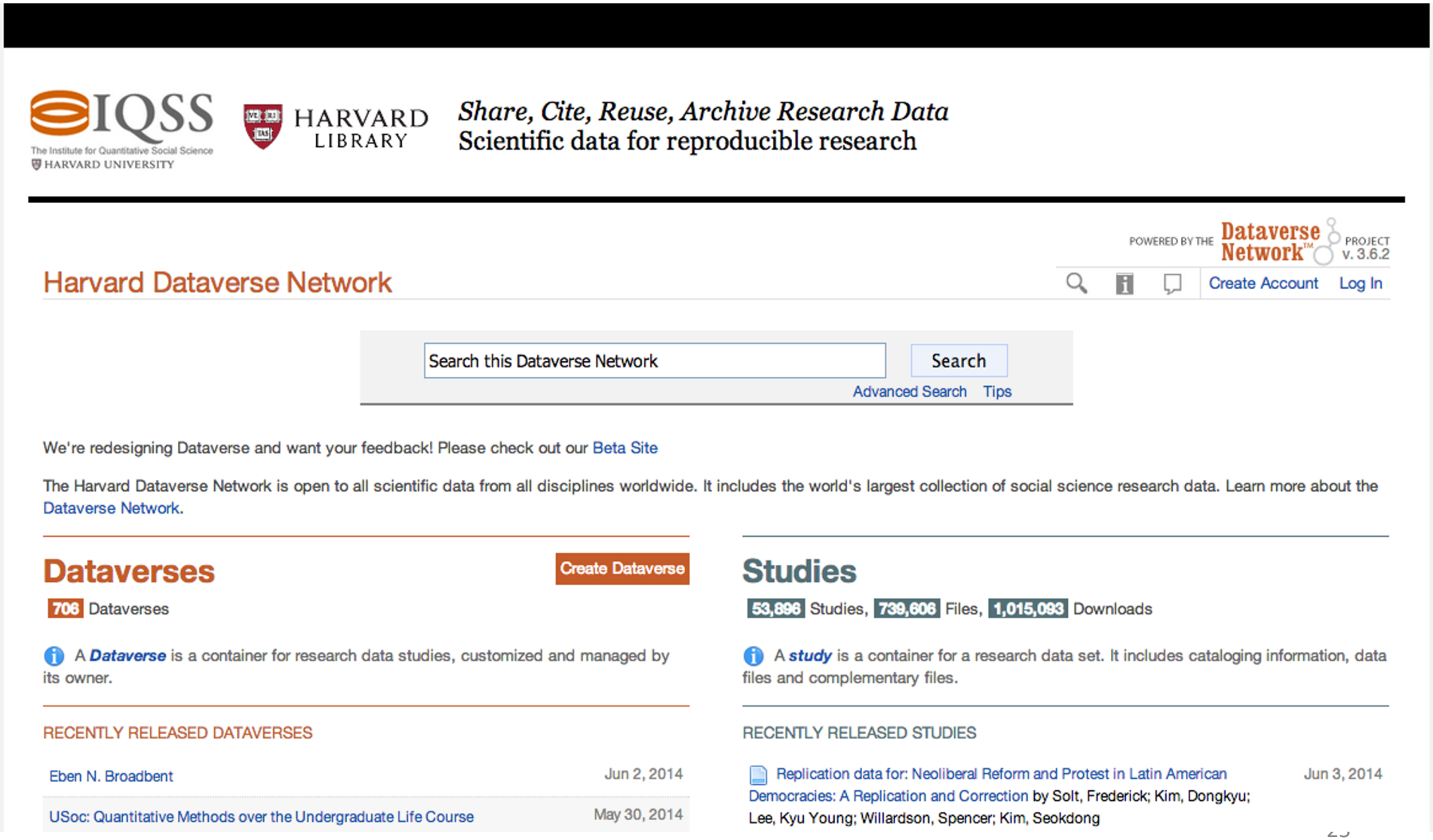
Project site: `http://opendp.io`

OpenDP

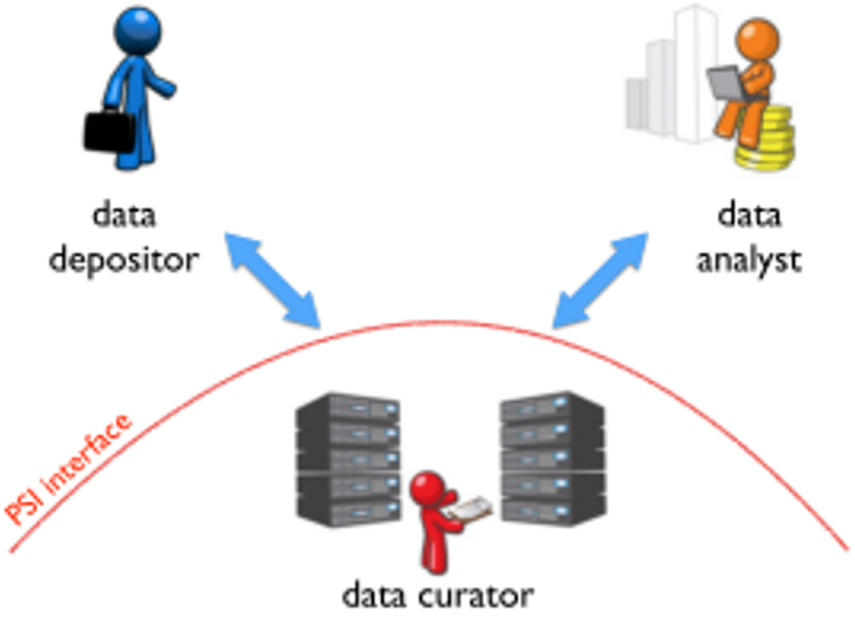
```
>>> from opendp.meas import make_base_geometric
...
>>> # call the constructor to produce a measurement
>>> base_geometric = make_base_geometric(scale=1.0)
...
>>> # investigate the privacy relation
>>> absolute_distance = 1
>>> epsilon = 1.0
>>> assert base_geometric.check(d_in=absolute_distance, d_out=epsilon)
...
>>> # feed some data/invoke the measurement as a function
>>> aggregated = 5
>>> release = base_geometric(aggregated)
```



Target: Data Repositories



Target: Data Repositories



IQSS Dataverse Network >

POWERED BY THE Dataverse Network™ PROJECT v. 3.2

Murray Research Archive Original Collection Dataverse

Create Account Log In

INTERGENERATIONAL STUDIES, 1932-1982

hdl:1902.1/00627UNF:3:jYQzhUZ5MxpaKGMvIojITA==

Version: 5– Released: Tue Jun 19 13:50:23 EDT 2012

Cataloging Information | **DATA & ANALYSIS** | Comments (0) | Versions

Use the check boxes next to the file name to download multiple files. Data files will be downloaded in their default format. You can also download all the files in a category by checking the box next to the category name. You will be prompted to save a single archive file. Study files that have restricted access will not be downloaded.

Access to some files is restricted, and those files are not available for downloading. Check the Terms of Use for more information.

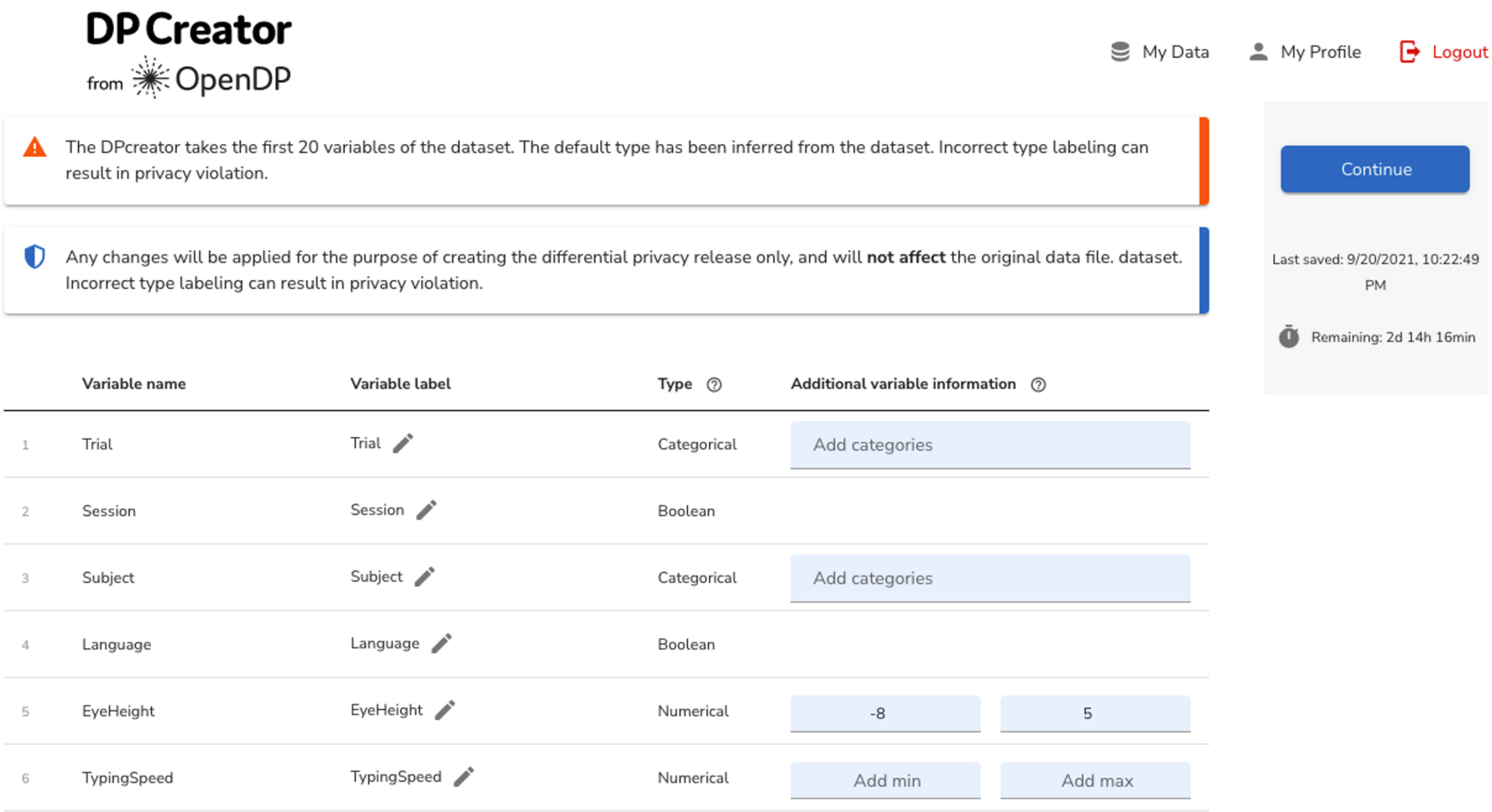
Select all files | Download All Selected Files

1. Documentation		
00627IHD-InterGenerational-Co… Adobe PDF - 41 MB - …	Download	Description of coded data variables
00627IHD-InterG… Adobe PDF - 7 M…	Download	Blank measures for study
00627IHD-InterG… Adobe PDF - 173 K…	Download	Overview: abstract, research methodology, publications, and other info.
2. Berkeley Data		
00627IHD-InterGenerational-BerkSpou-Data.por SPSS Portable - 29 KB - 0 downloads	Restricted	Data on Spouses in Berkeley Sample in SPSS Portable Format
00627IHD-InterGenerational-BerkSpou-Data.tab Tab Deli… TABUL…	Restricted	Data on Spouses of Berkeley Sample in Tab
00627IHD-InterGenerational-BerkSubj-Data.por SPSS Portable - 217 KB - 0 downloads	Restricted	Data on Subjects in Berkeley Sample in SPSS Portable Format

Many datasets are restricted due to privacy concerns

Goal: enable wider sharing while protecting privacy

Privacy Preserving Interfaces

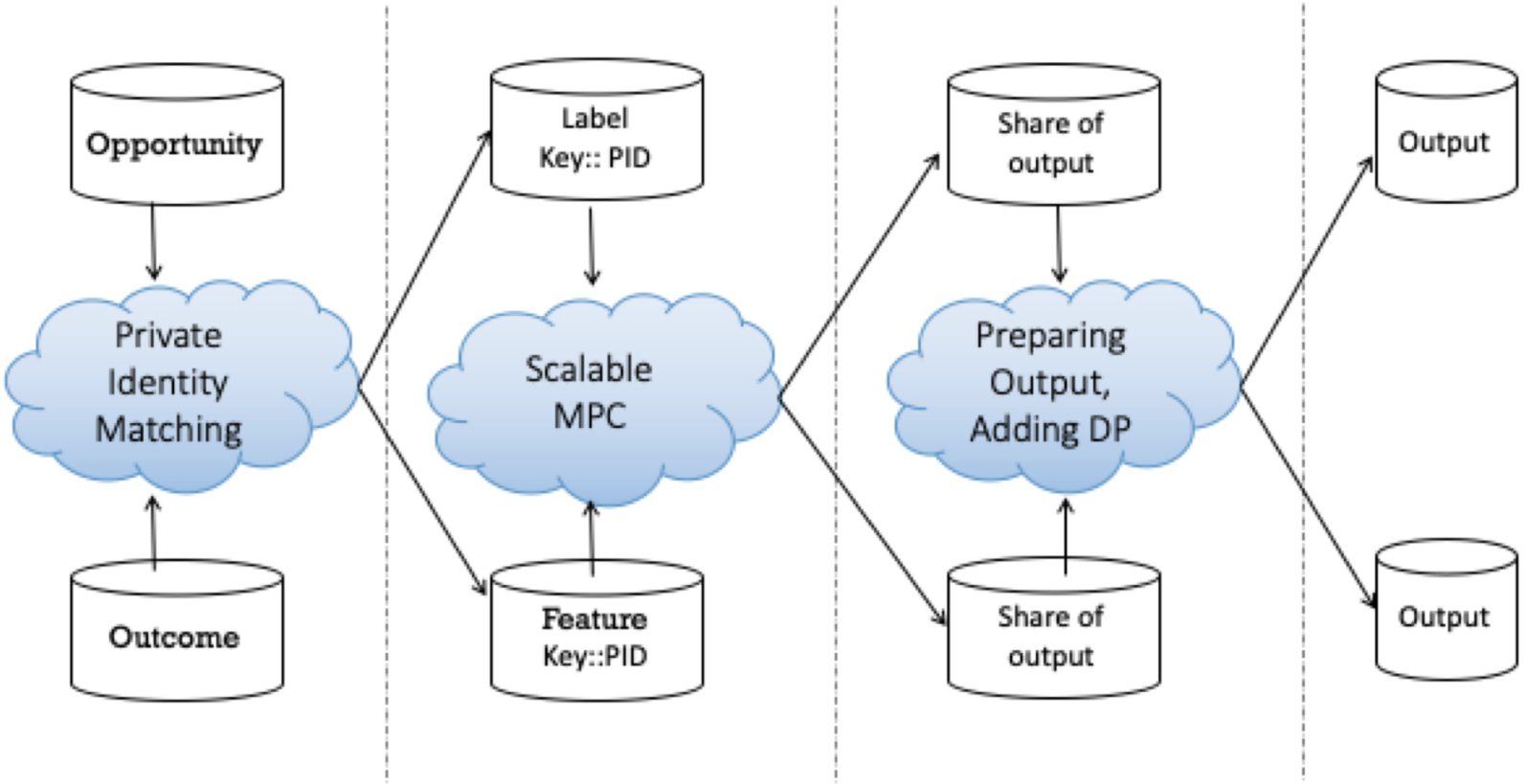


Challenges for DP in Practice

- Accuracy for "small data" (moderate values of n)
- Modelling & managing privacy loss over time
  - Especially over many different analysts & datasets
- Analysts used to working with raw data
  - One approach: "Tiered access"
  - DP for wide access, raw data only by approval with strict terms of use (cf. Census PUMS vs. RDCs)
- Cases where privacy concerns are not "local" (e.g. privacy for large groups) or utility is not "global" (e.g. targeting)
- Matching guarantees with privacy law & regulation
- …

Challenge for DP in Practice

When to rely on DP and how to combine DP with other privacy enhancing techniques?



Differential Privacy: Interpretations

Distribution of $C(D,q_1,\ldots,q_t) \approx_\varepsilon$ Distribution of $C(D',q_1,\ldots,q_t)$

- Whatever an adversary learns about me, it could have learned from everyone else's data.
- Mechanism cannot leak "individual-specific" information.
- Above interpretations hold regardless of adversary's auxiliary information.

But

- No protection for information that is not localized to a few rows.
- Differential privacy does not prevent statistical analysis and machine learning.

Nice Properties of Differential Privacy

Privacy loss measure (ϵ)

"Information structures no longer have to be the binary extremes"

Post-processing:

"No adversary can break the privacy guarantee"

Composition:

"The epsilons add up"

Basic Definitions and Techniques

- Definitions
  - Approximate DP/ local DP/ alternative definitions
- Introducing randomness (How to add noise and how much noise)
  - Randomized Response/Laplace/Exponential/Gaussian mechanisms
- Composition theory

Some Differentially Private Algorithms

Private Machine Learning

- Private ERM [RBHT12, CMS11, KST12, BST14]
- Modern ML: DPSGD [ACG+16, WBK19, MTZ19] and beyond; PATE [PAE+17, PSM+18]

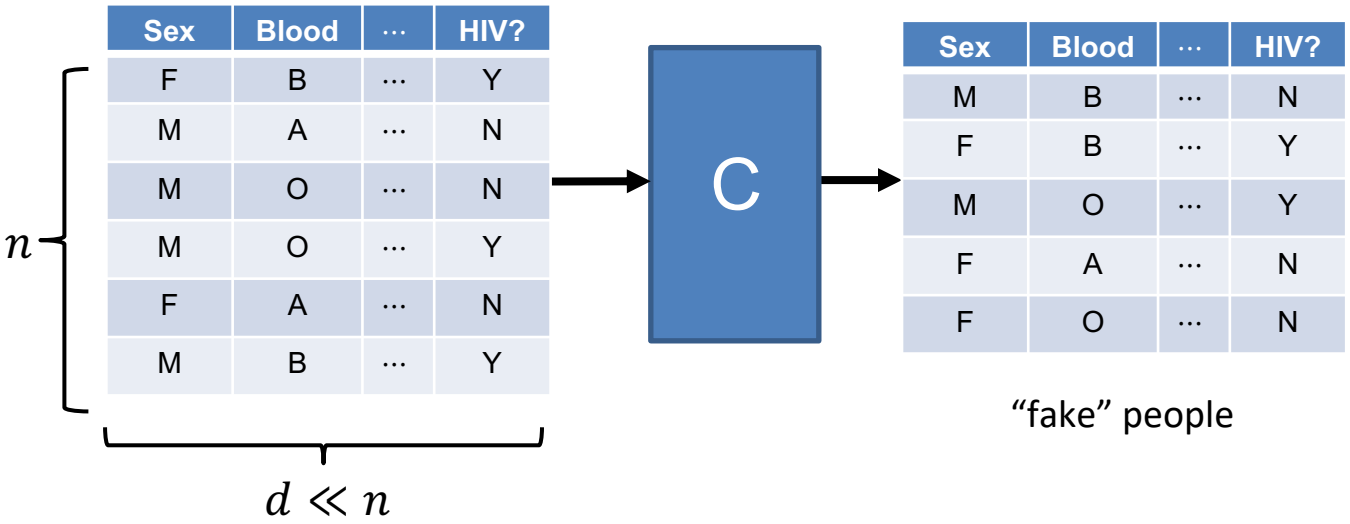
Private Stats

- Mean estimation & Confidence interval [BDK+2020, KSU20, KV18]
- Hypothesis testing [GLRV16, GR18, CKS+19, CKM+19]
- singular value decomposition [HR12, HR13, KT13, DTTZ14]

Private Synthetic Data [HLM12, GAH+14, VTB+20, NWD21, LBW21]

…

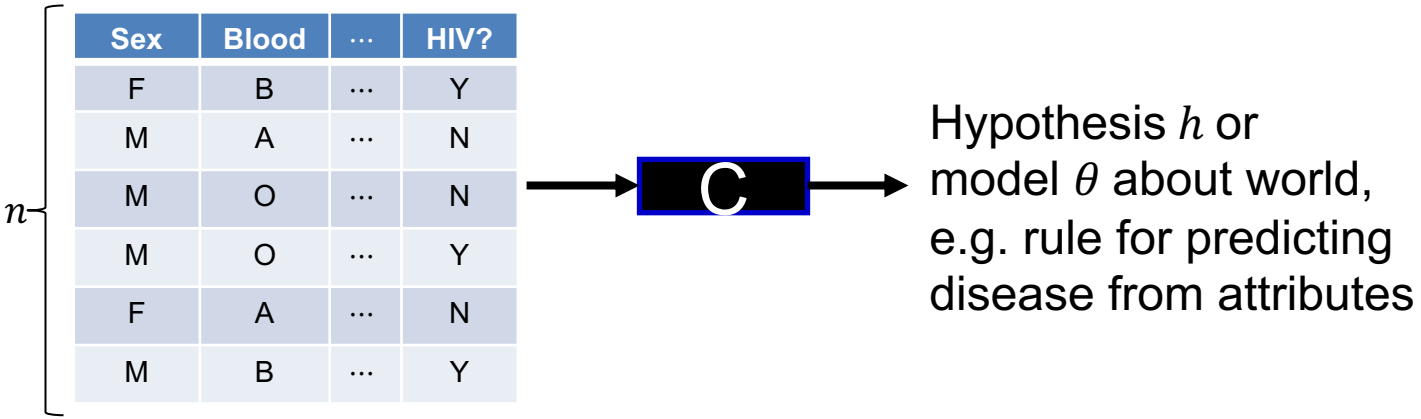
Amazing possibility: synthetic data



Utility: preserves fraction of people with *every* set of attributes!

Problem: uses computation time exponential in d.

Amazing Possibility II: Statistical Inference & Machine Learning



Theorem [KLNRS08,S11]: Differential privacy for vast array of machine learning and statistical estimation problems with little loss in convergence rate as $n \to \infty$.

DP Theory

Differential privacy research has

- many intriguing theoretical challenges
- rich connections w/other parts of CS theory & mathematics

e.g. cryptography, learning theory, game theory & mechanism design, convex geometry, pseudorandomness, optimization, approximability, communication complexity, statistics, …

Ethics, Law, and Society

- Analyze differential privacy deployments from various perspectives
  - **Ethics**: How does differential privacy alter ethical considerations around collecting sensitive data for public interest purposes?
  - **Law and policy**: What is the relationship between differential privacy and existing regulatory standards for privacy protection?
  - **Science & Technology Studies**: How does differential privacy reflect and shape power dynamics among data subjects, data holders, and researchers?

- Identify critiques, gaps, points of tension, and possible solutions