CS2080: Applied Privacy for Data Science

Course Overview

Salil Vadhan, James Honaker, Priyanka Nanayakkara

School of Engineering & Applied Sciences
Harvard University

January 27, 2025

Announcements

- Fill out first-class survey today: yellkey.com/ago (good only for <24hrs)
  - If the yellkey link does not work for you, try this: https://shorturl.at/jSosl
- TF introductions: Zach Ratliff (head TF), Christian Aagnes, Sahil Kuchlous, Jason Tang, Yanis Vandecasteele
- Course website (https://opendp.github.io/cs208/) has 2025 syllabus.
- Office hours this week:
  - Salil Tue 1pm-2:30pm (Zoom), Fri 10:30am-12pm (SEC 3.327)
  - James Weds 9:30-10:30am (SEC 4.442)
  - Priyanka Wed 2:30pm-4:30pm (SEC 2.101)
  - Zach Thu 3pm-4pm (SEC 3.314)
- Background review sessions this week (recorded):
  - Theory/math/stats/algorithms: Thu 9:45-11:00am (SEC 4.308)
  - Programming/experiments: TBD

Plan for today: whirlwind course overview

- Salil: motivation for & overview of differential privacy theory
- James: from theory to practice
- Priyanka: human-centered DP (i.e., “usable” DP)
- Salil: class structure
- Q&A

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
and more …

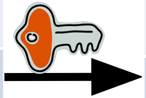
How can we:

- 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

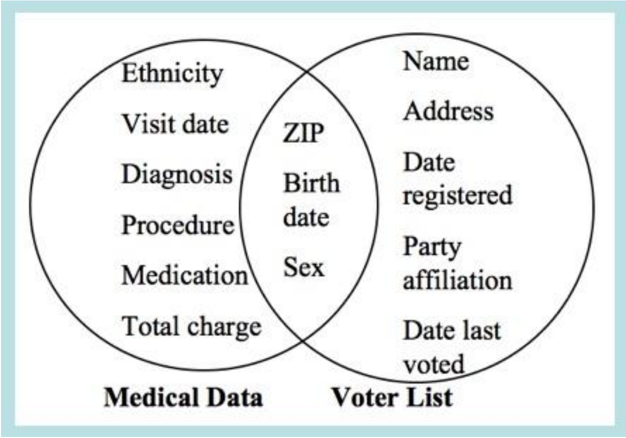


Name	Sex	Blood		HIV?
100101	001001	110101		110111
101010	111010	111111		001001
001010	100100	011001		110101
001110	010010	110101		100001
110101	000000	111001		010010
111110	110010	000101		110101

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



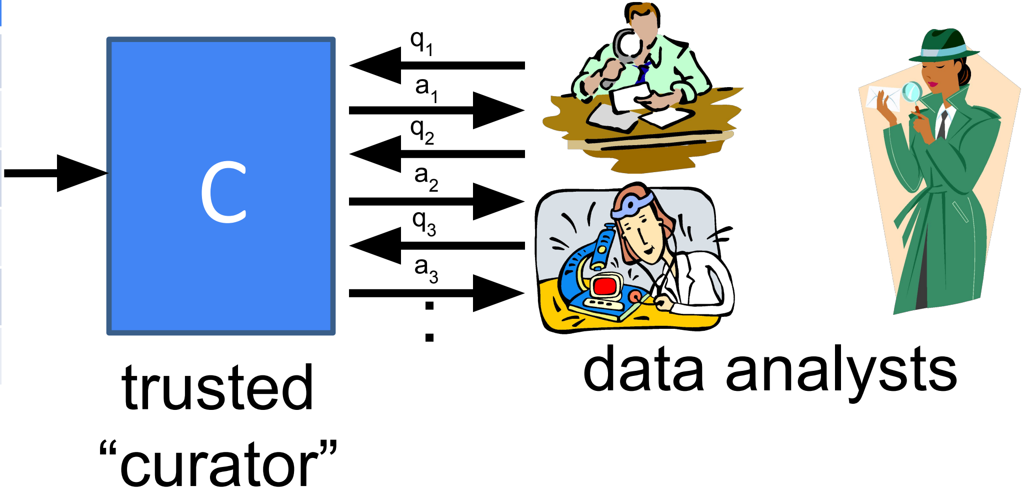
[Sweeney `97]

"re-identification" often easy

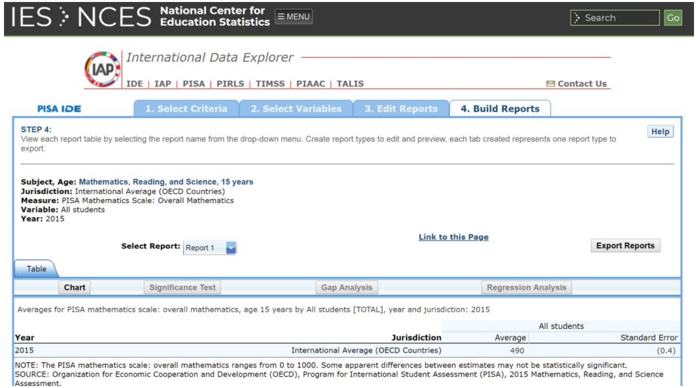
Problems?

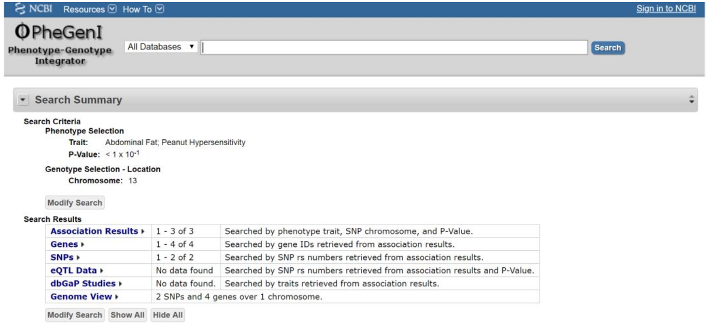
Approach 3: Mediate Access

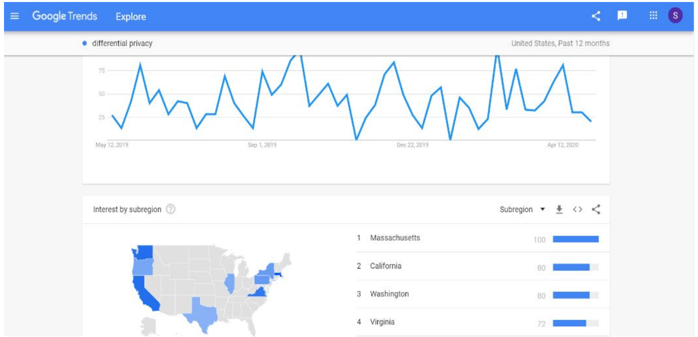
Name	Sex	Blood		HIV?
Chen	F	B		Y
Jones	M	A		N
Smith	M	O		N
Ross	M	O		Y
Lu	F	A		N
Shah	M	B		Y



Existing Query Interfaces

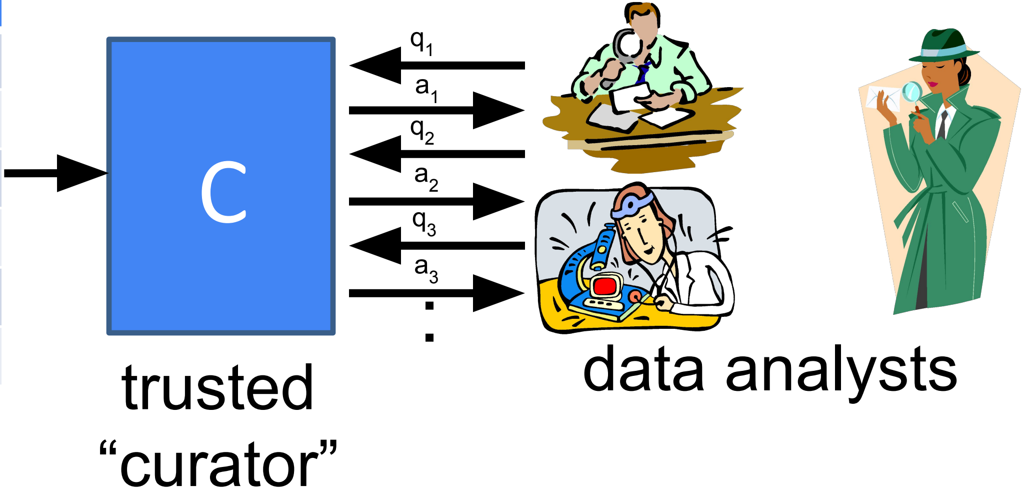






Approach 3: Mediate Access

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 Enhancing Technologies (PETs)

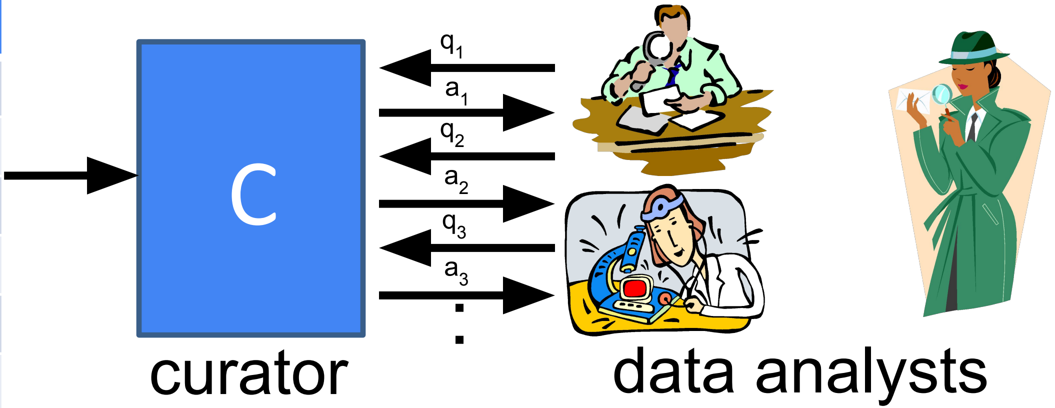
Model	Utility	Privacy	Who Holds Data?
Differential Privacy	statistical analysis of dataset	individual-specific info	trusted curator
Secure Multiparty Computation	any query desired	everything other than result of query	original users (or semi-trusted delegates)
Fully Homomorphic (or Functional) Encryption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

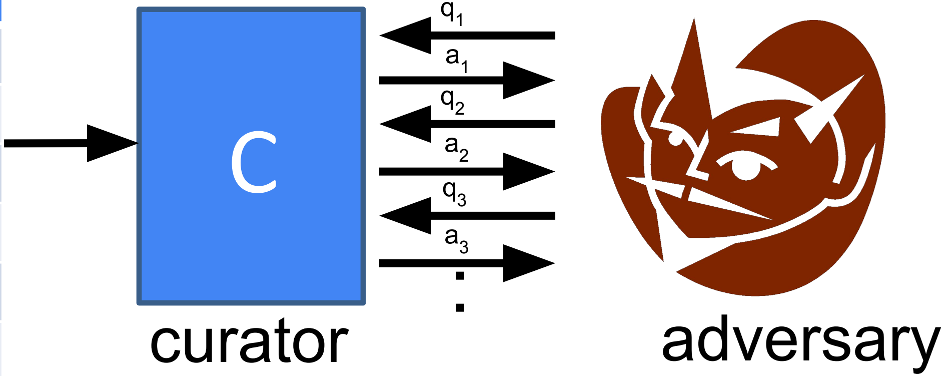


Requirement: effect of each individual should be “hidden”

Differential privacy

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

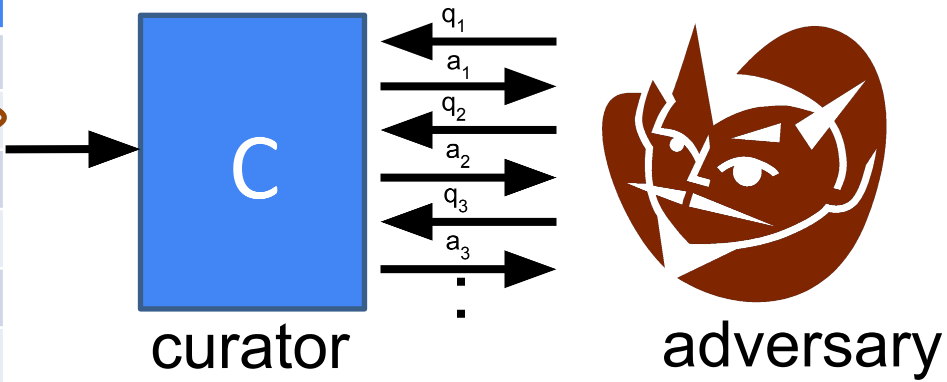
Sex	Blood		HIV?
F	B		Y
M	A		N
M	O		N
M	O		Y
F	A		N
M	B		Y



Differential privacy

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

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

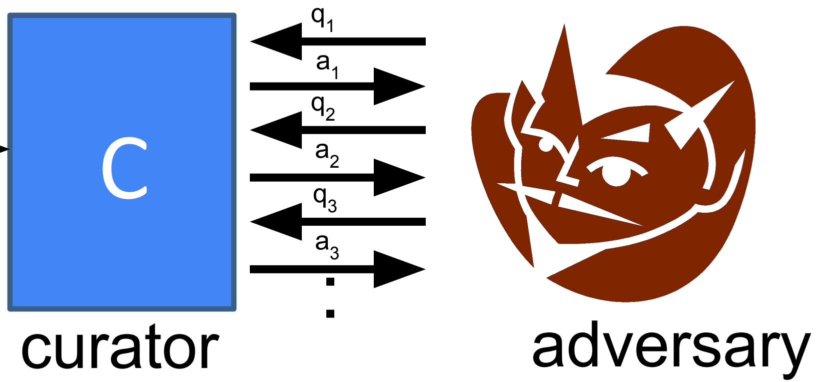


Requirement: an adversary shouldn’t be able to tell if any one person’s data were changed arbitrarily

Differential privacy

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

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

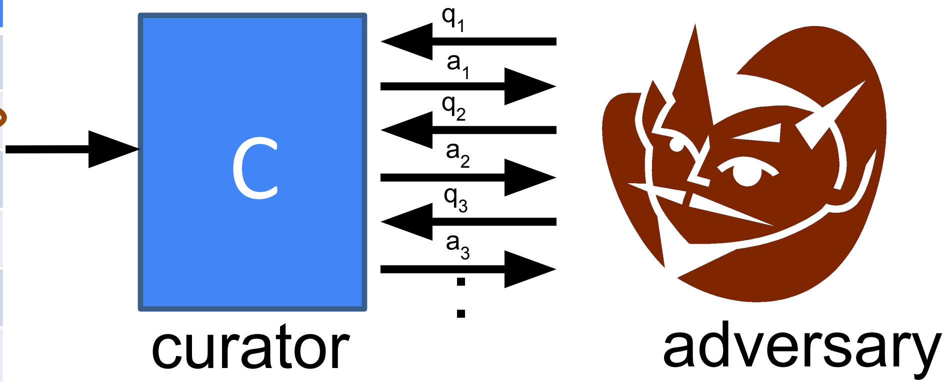


Requirement: an adversary shouldn’t be able to tell if any one person’s data were changed arbitrarily

Differential privacy

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

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

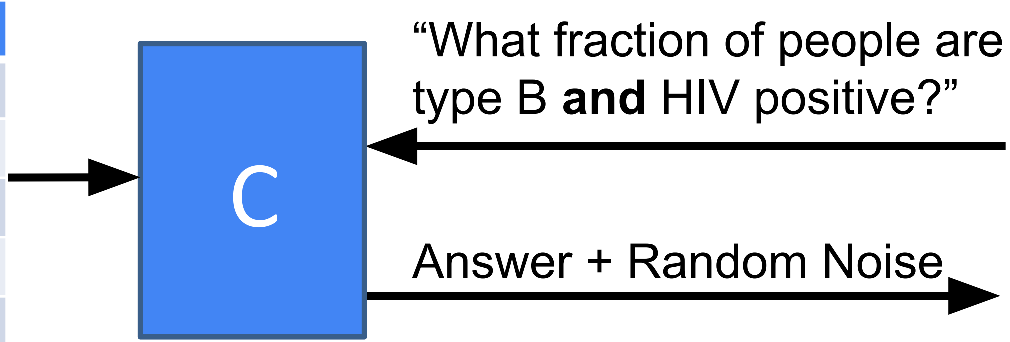


Requirement: an adversary shouldn’t be able to tell if any one person’s data were changed arbitrarily

Simple approach: random noise

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

n



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

The (Inherent) Privacy-Utility Tradeoff

Every statistical release incurs some privacy loss ε_i.

- More noise $\Rightarrow$ more privacy (smaller ε_i), less accuracy
- Less noise $\Rightarrow$ less privacy (larger ε_i), more accuracy
- Tradeoff is less stark on larger populations ($n \to \infty$)

With multiple queries, the privacy loss accumulates.

- Overall privacy loss $\leq \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_k$
- There are better composition theorems for differential privacy.
  [Dwork-Rothblum-V. 09, Kairouz-Oh-Viswanath `15, Murtagh-V. `16, …]

Recommended use: set an overall budget ε (e.g. $\varepsilon = .1$)

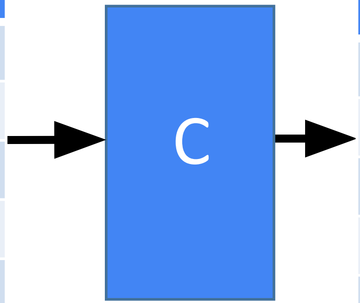
- Stop answering queries when budget reached.

Amazing possibility I: synthetic data

n

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

$d \ll n^{2/3}$



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

“fake” people

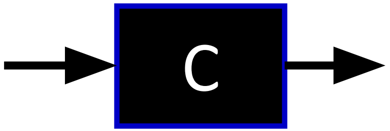
Utility: preserves fraction of people with *every* combination of attributes!

Problem: uses computation time exponential in d

Amazing Possibility II: Statistical Inference & Machine Learning

n

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



Hypothesis h or model θ about world, e.g. rule for predicting disease from attributes

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

The Differential Privacy Goldmine

- DP raised fascinating questions and connections for theorists in many areas

  cryptography, computational complexity, machine learning, statistics, information theory, convex geometry, mechanism design, quantum computing, programming languages, databases, data structures, streaming algorithms, …

  While addressing a problem of urgent societal need!

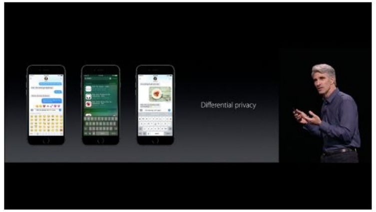
- Many fundamental theoretical questions remain, and efforts to bring DP to practice raise even more.

http://clipart-library.com/clipart/5TRrorGLc.htm

These were James’s Slides

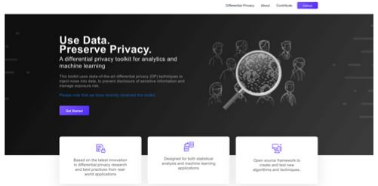

Apple will not
see your data

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)
- All public-use products from 2020 decennial census

Google

- “RAPPOR” for Chrome Statistics (2014)
- Privacy Sandbox for AdTech (2019)

Apple

- iOS10 and Safari(2016)
- Private Click Measurement (2022)

Microsoft

- SmartNoise (2020)
- AI for Good: Broadband Coverage (2021) DIgital Divide (2024)

Wikimedia

- Usage Metrics (2024)

Mozilla

- Firefox Privacy Preserving Attribution (2024)
- Anonym Private Lift and Attribution (2024)

Harvard Privacy Tools Project

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

NSF

U.S. DEPARTMENT OF COMMERCE BUREAU OF THE CENSUS

Alfred P. Sloan FOUNDATION

Google

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.

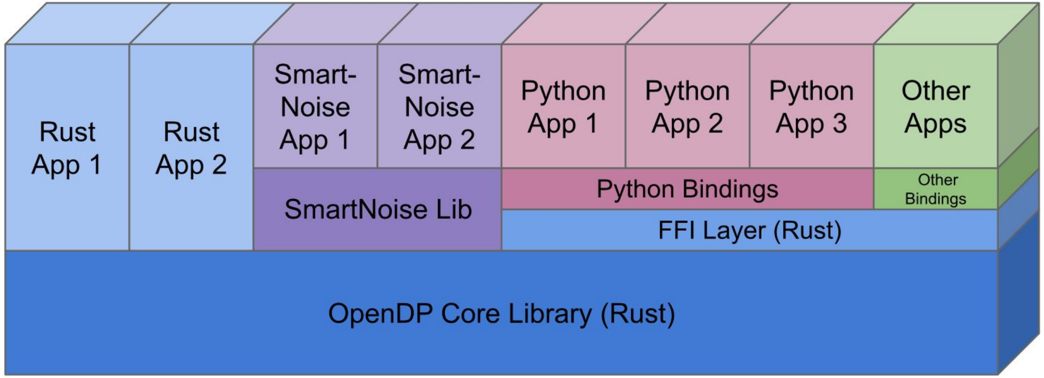
Why?

- 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.org`

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)
```



OpenDP

https://opendp.org/opendp-summer-interns

February 1 Deadline

2025 projects include:

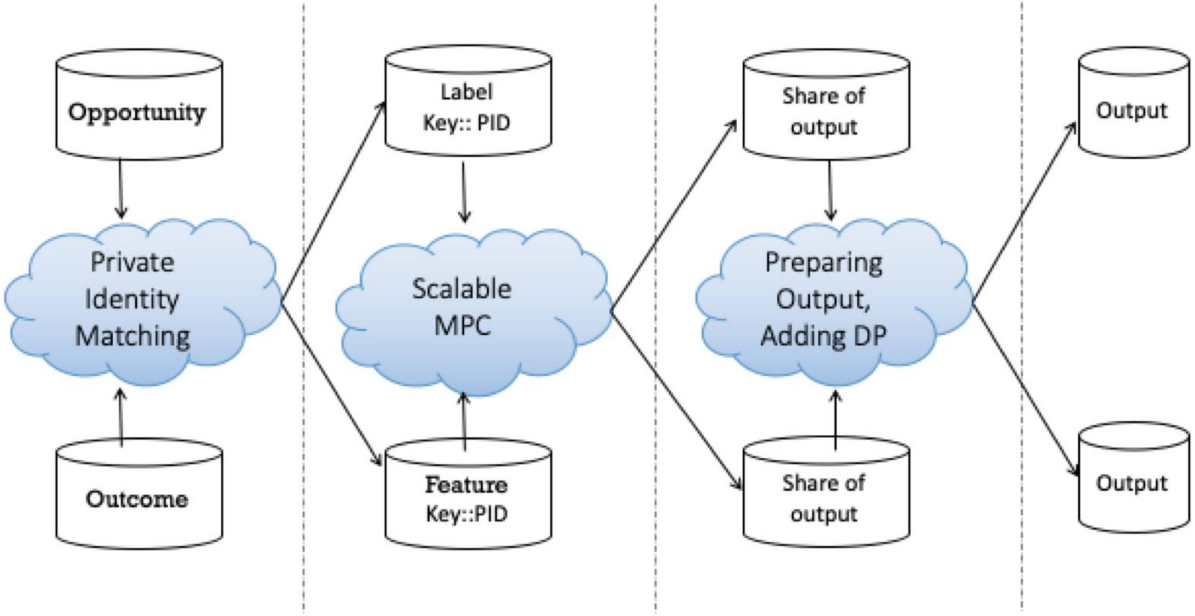
- **Building and integrating software**
- **Community building and outreach**
- **Usability and UX**
- **Writing math proofs**
- **DP research**
- **Privacy, ethics, policy and responsible use**

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?



Goal of DP:
protect people’s privacy

The privacy piece: How does DP interact with other understandings of privacy?

Several frameworks for privacy, including:

- Privacy as control / information disclosure
- Privacy as interpersonal boundary regulation
- Privacy as social context

See Wisniewski and Page 2022 for a summary

The privacy piece: How does DP interact with other understandings of privacy?

Several frameworks for privacy, including:

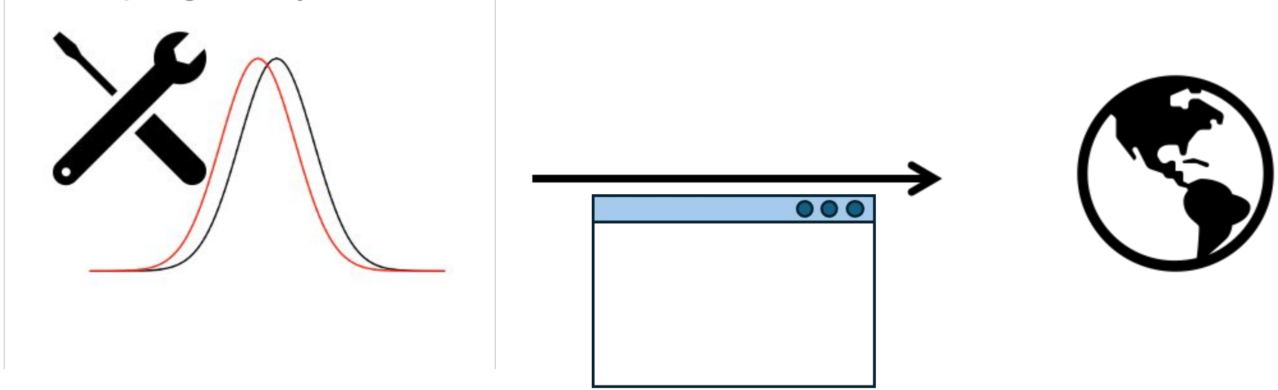
- Privacy as control / information disclosure
- Privacy as interpersonal boundary regulation
- **Privacy as social context (Contextual Integrity, Nissenbaum 2009)**

Contextual Integrity

DP

The people piece: How can we make DP “usable”?

- Several previous implementations have required expert teams, but it’s unrealistic to expect most organizations to have DP experts in-house.
- How can we make DP usable for data analysts *without* DP expertise? How might we support them in setting privacy budgets?
- Once we’ve designed usable tools, how do we evaluate them? How do we know they’re helping analysts make “better” decisions?



Programming frameworks & interfaces

The people piece: How can we communicate DP's guarantees to diverse audiences?

- Several parties have an interest in how data are protected:
  - Data subjects (i.e., people contributing their information)
  - Data users (data analysts at companies, researchers, etc.)
  - Policymakers
  - …and more
- How might we communicate DP's guarantees to these audiences?

Beyond privacy: Evaluating downstream data utility

- What are the implications of adding noise to computations, especially for high-stakes data releases?
- How should we define “utility”?
- How might we systematically and rigorously assess the downstream utility of data protected under DP?

Notes (this slide is just PN's thinking. Will edit into slides later)

- Goal of DP is to protect people's privacy
- In the course we'll learn the mathematical foundations of DP, but we'll also center societal questions around the use of DP.
- The privacy piece: Privacy is a complex and contested concept. Scholars outside computer science have long thought about what privacy is and how it should be upheld (philsophers, legal scholars, etc). We'll relate DP to other theories of privacy, namely contextual integrity. We'll see how CI can help inform decisions about when DP is appropriate, and how considering the underlying philosophy of DP can in turn inform CI.
- The "people" piece:
    - Decision-makers often do not have CS backgrounds, let alone DP background. How do we make sure DATA ANALYSTS can actually use DP? Make decisions about setting and splitting privacy budgets? We'll see how PROGRAMMING FRAMEWORKS AND INTERFACES can make DP usable for these audiences, who have required domain knowledge. When we design an interface, how do we EVALUATE it? How do we know it's

Course Structure

Looks like last year we didn't get to this until Lecture 2, but may want to bump to day 1.

Class Goals

By the end of the course, we hope that you will all be able to:

- Identify and demonstrate risks to privacy in data science settings,
- Correctly match differential privacy technology with an application,
- Safely implement privacy solutions, and experimentally validate the performance and utility of algorithms,
- Understand differential privacy at a level sufficient to engage in research about best practices in implementation, apply the material in practice, and/or connect it to other areas,
- Analyze the ethical and policy implications of differential privacy deployments,
- Formulate and carry out an interesting, short-term independent research project, and present the work in both written and oral form.

Course Elements

- Pre-class readings to comment on via Perusall
- In-class small group discussions. Attendance expected.
- Lecture on both theory & implementation (bring your laptop for live-coding) (live-streamed & recorded in case you have an excused absence)
- Problem sets, approx. weekly. Mix of analytical and experimental problems.
- Weekly section and office hours
- Final project

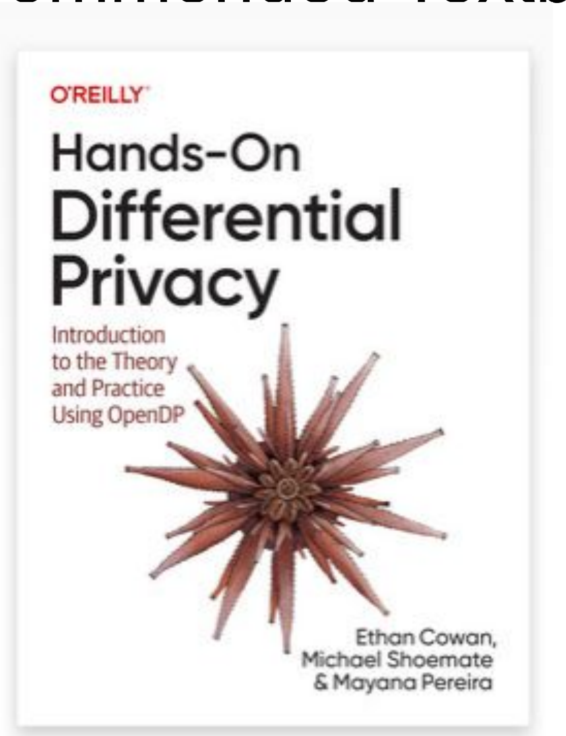
Grading: approx. 20% participation, 40% problem sets, 40% project

Prerequisites

Basic probability at the level of STAT 110, and algorithms and Python/R programming at the level of CS109/AC209 or CS1200.

If you are unsure, ask us and use first 1-2 weeks to gauge.

Recommended Textbook



Lots of other resources in annotated course bibliography and in readings assigned on Perusall.

Class Culture

Desiderata:

- Inclusive & supportive environment
- Shared learning mission
- Diverse experiences & viewpoints valued
- Learn from inquiry & disagreement

To this end:

- Be kind and open-minded
- Let us know if anything is said or done (including by us!) that feels inappropriate
- Let us know if experiences outside class or physical/mental health issues are impacting your performance in class

Other Courses that Cover DP

- CS 1260 “Fairness & Privacy: Perspectives of Law & Probability” (Fall 2024, Spring 2026)
- Stat 188 “Variations, Information and Privacy” (Fall 2024, Fall 2025?)
- AC 221 “Critical Thinking in Data Science (Spring 2025)
- CS 2260 “Topics in Theory for Society: Differential Privacy” (Fall 2025)
- Boston U. “Privacy in Statistic and Machine Learning” (Spring 2025, TuTh 2pm-3:15pm)

Course Topics I

- Privacy Attacks on “De-Identified” Data and Statistical Data Releases
  - Reidentification attacks
  - Reconstruction attacks
  - Membership attacks
- Foundations of Differential Privacy
  - Definition and interpretation
  - Basic mechanisms (Laplace, Gaussian, randomized response, histograms, exponential)
  - Composition of differential privacy & other measures of privacy
  - Survey of known algorithms and experimental validation

Course Topics II

- Implementing (centralized) differential privacy
  - Deployments by US Census Bureau and other organizations (Microsoft, Wikimedia Foundation, …)
  - Synthetic data releases and statistical releases
  - Differentially private machine learning and deployments by Google and Meta
  - Programming platforms such as OpenDP
  - Interfaces & usability
  - Evaluating downstream utility
- Distributed Models differential privacy
  - Local vs. federated vs. centralized DP
  - Basic theory and mechanisms (randomized response, histograms, SGD)
  - Combining DP with other PETs (e.g. secure multiparty computation)
  - Deployments by Google, Apple, Meta, Mozilla

Course Topics III

- Social perspectives on DP
  - Differential privacy in relation to other (non-CS) privacy philosophies
  - Communicating differential privacy guarantees to various stakeholders
  - Privacy law and policy
  - Power dynamics in sociotechnical systems
- Government & industry panel discussion
- Other possible topics (depending on time and interest)
  - Differential privacy for graph and social network data
  - Statistical inference under differential privacy
  - Side-channel & randomness attacks on implementations

Announcements

- Fill out first-class survey today: yellkey.com/ago (good only for <24hrs)
  - If the yellkey link does not work for you, try this: https://shorturl.at/jSosl
- TF introductions: Zach Ratliff (head TF), Christian Aagnes, Sahil Kuchlous, Jason Tang, Yanis Vandecasteele
- Course website (https://opendp.github.io/cs208/) has 2025 syllabus.
- Office hours this week:
  - Salil Tue 1pm-2:30pm (Zoom), Fri 10:30am-12pm (SEC 3.327)
  - James Weds 9:30-10:30am (SEC 4.442)
  - Priyanka Wed 2:30pm-4:30pm (SEC 2.101)
  - Zach Thu 10am-11:30am (SEC 3.314)
- Background review sessions this week (recorded):
  - Theory/math/stats/algorithms: Thu 9:45-11:00am (SEC 4.308)
  - Programming/experiments: TBD