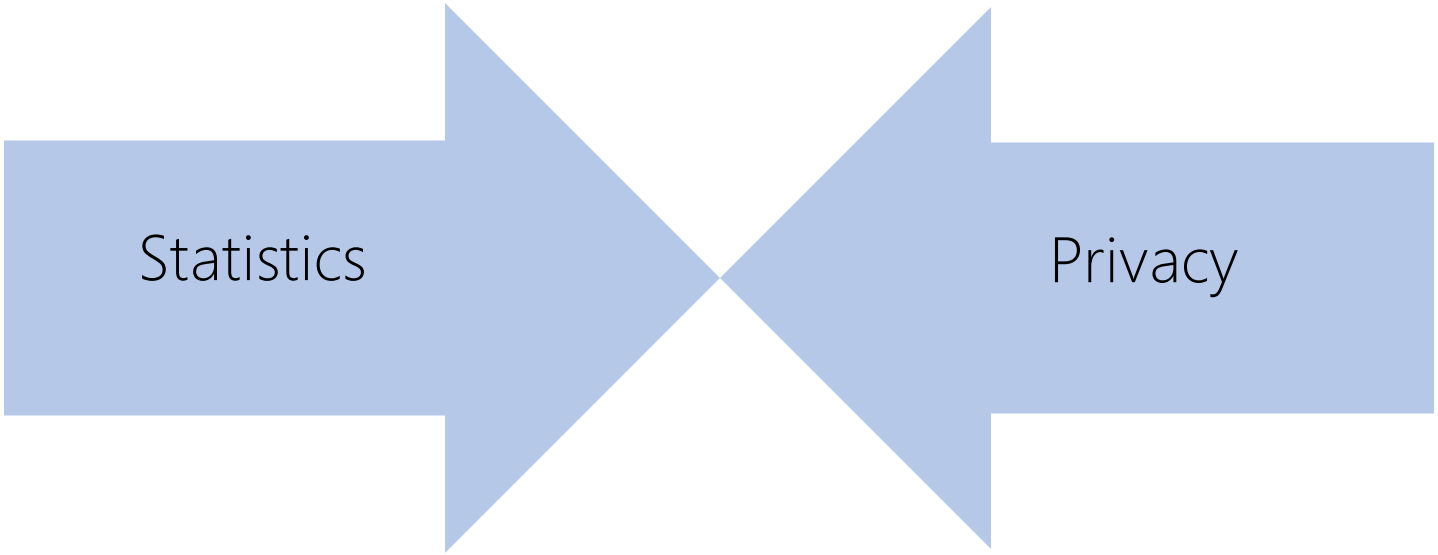
Learning Using Private Data: Naïve View



Statistics and Privacy seems conflicting!

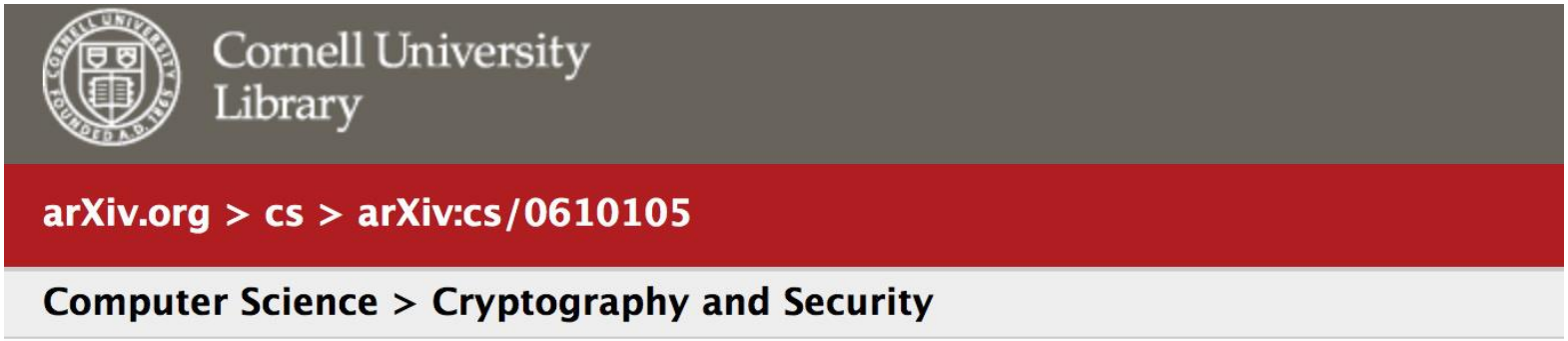
Think about computing mean of numbers

Statistics Using Private Data: DP View

Data analysis on collected data

- Privacy issues
- Too big to store
- Distributed
- Cryptographic solution are too expensive

Privacy Attacks (2000-2010)



Strava's fitness tracker heat map reveals the location of military bases

Geolocation isn't a new problem for the military

Big Data: Anonymity, Privacy, Ethics — Arvind Narayanan

« Back

Papers

Semantics derived automatically from language corpora contain human-like biases
Aylin Caliskan, Joanna J. Bryson, *Arvind Narayanan*.
Science, 2017.
Open access author copy.

When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies
Steven Goldfeder, Harry Kalodner, Dillon Reisman, *Arvind Narayanan*.
Manuscript, 2017.
Blog post.

Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic
Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, *Arvind Narayanan*, and Nick Feamster.
Manuscript, 2017.

Ten simple rules for responsible big data research
Matthew Zook, Solon Barocas, danah boyd, Kate Crawford, Emily Keller, Seeta Peña Gangadharan, Alyssa Goodman, Rachelle Hollander, Barbara A. Koenig, Jacob Metcalf, *Arvind Narayanan*, Alondra Nelson, Frank Pasquale.
PLoS Computational Biology 2017.

De-anonymizing Web Browsing Data with Social Networks
Jessica Su, Ansh Shukla, Sharad Goel, *Arvind Narayanan*.
World Wide Web Conference 2017.

Blog posts

One more re-identification demonstration, and then I'm out 23 Mar 2015

We Can De-anonymize Programmers From Coding Style. What Are the Implications? (Aylin Caliskan) Feb 26, 2015

Good and bad reasons for anonymizing data 09 Jul 2014

Personalized coupons as a vehicle for perfect price discrimination 25 Jun 2013

Reidentification as Basic Science 27 May 2013

Price Discrimination and the Illusion of Fairness 22 Jan 2013

New Developments in Deanonymization 17 Dec 2012

Data-mining Contests and the Deanonymization Dilemma: a Two-stage Process Could Be the Way Out 15 Jun 2011

Price Discrimination is All Around You 02 Jun 2011

The Linkability of Usernames: a Step Towards "Uber-Profiles" 17 Feb 2011

Press

Exercise App Shows Why Anonymous Data Can Still Be Dangerous
CBC Radio, Feb 02, 2018

In 2017, Society Started Taking AI Bias Seriously
Engadget, Dec 21, 2017

Battling AI Biases
Communications of the ACM, Nov 28, 2017

A Proposed Anti-Doxxing Law in the U.K. Could Make Personal Data Less Secure
Slate, Aug 15, 2017

What Would Make a Computer Biased? Learning a Language Spoken by Humans
Los Angeles Times, Apr 14, 2017

Even Artificial Intelligence Can Acquire Biases Against Race and Gender
Science Magazine, Apr 13, 2017

AI Programs Exhibit Racial and Gender Biases, Research Reveals
The Guardian, Apr 13, 2017

http://randomwalker.info/data-privacy/

Use Cryptography?

- SMPC
- Homomorphic encyrption
- Functional encryption
- Arithmetic on finite fields

3 Impossibility of Absolute Disclosure Prevention

Why strong privacy guarantee?

- Richer the data, more useful it is
- Reidentification is not the only risk
- Query auditing can be problematic
- Summary statistics is not safe!!!
- Ordinary facts are not okay!

Differential privacy addresses the paradox of learning nothing about individual while learning (statistics) about the population

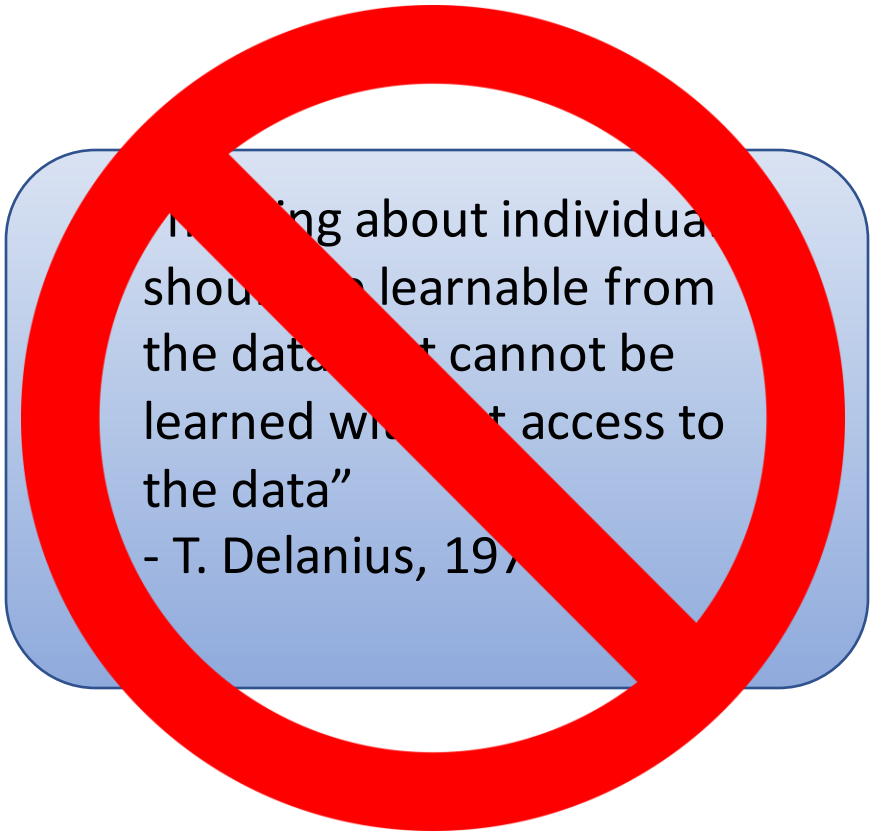
Defining Privacy: Attempt 1 (statistician view)

You cannot do that; my friends knows that I lost my job recently!

I am releasing research findings that people who lost their jobs are very likely to vote for X

Statistician's nightmare!

Defining Privacy: Attempt 1 (statistician view)



Defining Privacy: Attempt 2 (k-anonymity)

I know Jalaj is on food stamp and social care

K people are on food stamps and social care, and all of them also voted for X

Defining Privacy: Differential Privacy

I am releasing findings that people who lost their jobs are likely to vote for X

Do not blame if your friends know that you lost your job

Please participate in the survey truthfully as you have nothing to lose

The outcome would not tell that you participated or not => whom you voted

Statistician ☺ and participant ☺

Defining Privacy: Other definitions

- k anonymity [Samarati and Sweeney (1998)]
- m-invariance [Xiao and Tao (2007)]
- t closeness [Li et al. (2007)]
- ℓ diversity [Machanavajjhala et. al. (2007)]
- δ-presence [Nergiz and Clifton (2008)]

and so on ...

Attacks based on Homogeneity

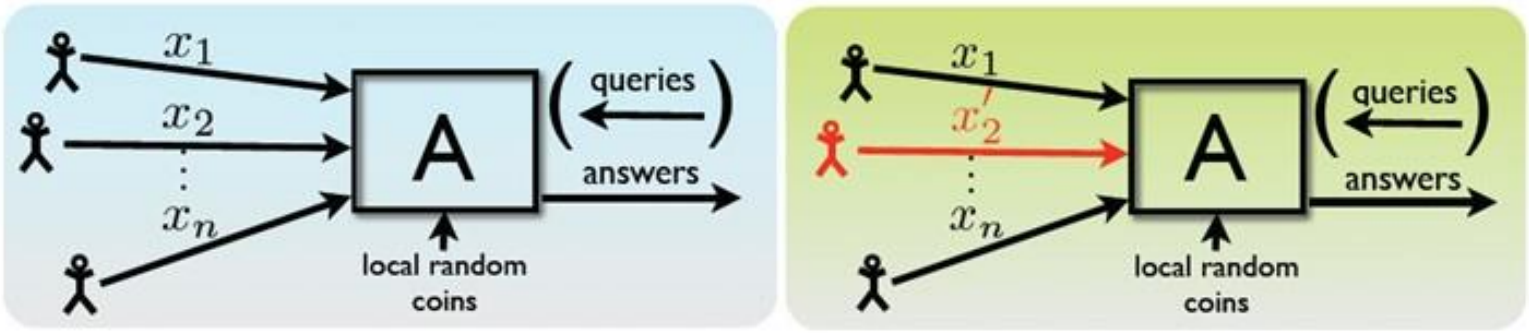
Value equivalence attack

Not every value has equal sensitivity

May be difficult and to achieve

Difficult to implement

Defining Privacy: Differential Privacy



Captures what is private

x′ is a neighbor of x
If they differ in one row

The outcome would not tell that you participated or not

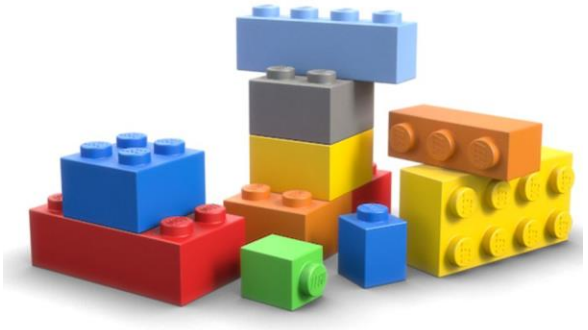
Differential Privacy [DMNS06]

- for all neighboring databases $\boldsymbol{x}$ and $\boldsymbol{x'}$
- for all possible outputs S,

$$\Pr[A(\boldsymbol{x}) \in S] \leq e^{\varepsilon} \cdot \Pr[A(\boldsymbol{x'}) \in S] + \delta$$

Captures all possible outcome

Properties of Differential Privacy



Preserved under post-processing

+

Preserved under composition

Can use simple algorithms to build complex systems

DP in other fields

- Learning with DP gives better generalization
- DP algorithms and amazing mechanism design
- Robust statistics
- Robust sublinear space algorithms

An early example: From 1965

Wagner's randomized response

- Flip an unbiased coin
- If tails, respond truthfully
- If head, flip another coin
  - If head, respond “YES”
  - If tail, respond “NO”

Differential privacy comes from plausible deniability

Fast forward 2006: Laplace mechanism

Given a query function f such that

$$\Delta_f := \max_{\delta(x,y)=1} \|f(x) - f(y)\|_1$$

Compute

$$M_L(f, x) := f(x) + Y, \quad Y \sim \mathsf{Lap}\left(\frac{\Delta_f}{\epsilon}\right)$$

Recall the pdf of Laplace distribution with scale b is

$$\frac{1}{2b} \exp\left(-\frac{|x|}{b}\right)$$

Privacy proof of Laplace mechanism

Fast forward 2006: Gaussian mechanism

Given a query function f such that

$$\Delta_f := \max_{\delta(x,y)=1} \|f(x) - f(y)\|_2$$

Compute

$$M_G(f, x) := f(x) + Y, \quad Y \sim \mathcal{N}\left(0, \frac{2\Delta_f^2 \ln(1/\delta)}{\epsilon^2}\right)$$

Recall the pdf of Gaussian distribution is

$$\frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right)$$

Fast forward: 2007

- Exponential mechanism (generally impractical; used as a benchmark)
  - Need to chose best response
  - Noise destroys its value (think AUCTION)
  - Define utility function for each response

Fast forward: 2009

- Sparse vector technique (think counting queries)
  - Only care about identity of elements above threshold
  - Add noise and report only if the noisy answer is above threshold

Fast forward: 2010

- Private Multiplicative Weight Update Mechanism (think counting queries)
  - Answer exponential number of counting queries
  - Add correlated noise

Private multiplicative weight

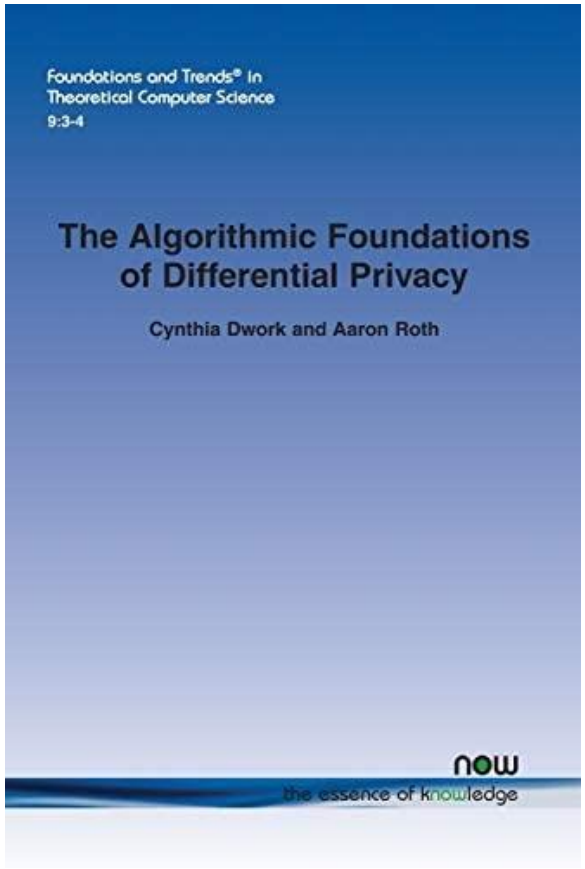
Some other model of privacy

- Local model of privacy [2006]
  - RAPPOR
  - Apple 2016 annoucement
  - Microsoft telemetry data
  - LinkedIn, Amazon, Twitter, …..
- Shuffle model of privacy [2015]
  - Based on "Cryptography through Anonymity"

Some other model of computation

- Continual release model [2010]
  - A lot of recent activities...
- Pan privacy [2010]
  - Related to "Shuffle model of privacy"

Resources



The Complexity of
Differential Privacy

Salil Vadhan

Harvard University

An upcoming book