CS295B: Data Privacy, Lecture 1

Joe Near (jnear@uvm.edu)

8/27/2018

Outline

1. Administrative
2. What is data privacy, and how is it violated?
3. How do data privacy violations affect us?

Course Information

- **Course website**: `https://jnear.github.io/cs295-data-privacy/`
- **Instructor**: Joe Near, `jnear@uvm.edu`
- **Lecture**: Monday & Wednesday, 5:05pm - 6:20pm, Votey 209
- **Office hours**: Thursdays, 2:00pm - 4:00pm, Votey 317

Resources

- **Announcements**: Course website & Piazza
- **Grading & assignments**: Blackboard
- **Discussion & Questions**: Piazza & office hours
- **Textbooks**: None (see PDFs on course website)

Structure of the Semester

(8/27 - 9/12)	Introduction to privacy, history of privacy mechanism
(9/17 - 10/3)	Theory of differential privacy & basic mechanisms
(10/10 - 10/29)	Advanced mechanisms & extensions
(10/31 - 11/14)	Differential privacy for machine learning
(11/26 - 12/5)	Applications & project presentations

Grading

- 8 homework assignments (5% each; 40% total)
- 2 in-class quizzes (10% each; 20% total)
- Midterm exam (20%)
- Final project (20%)

Final Projects

- Groups of 1-3
  Expectations scale with group size
- Deliverables:
  - Project proposal (around 11/1)
  - Project results writeup (around 12/5)
  - Project presentation (12/3 or 12/5)
  - Code (with project writeup)
- Goal: implement something substantial
  - Empirical result on realistic data
  - Realistic system for privacy-preserving analysis
  - New twist on existing privacy mechanism
  - New research contribution
- Lots more as we get closer to November 1

Questions?

Outline

1. Administrative
2. What is data privacy, and how is it violated?
3. How do data privacy violations affect us?

A Non-Definition

Information privacy

From Wikipedia, the free encyclopedia

Information privacy, or **data privacy** (or **data protection**), is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them.[1]

My Definition

Analysis of data preserves **data privacy** if:

- You learn something useful from the analysis
- The analysis does not violate the privacy of any individual

An individual's **privacy is violated** if:

- The analyst learns something about the individual that they did not know before the analysis took place

My Definition

Analysis of data preserves **data privacy** if:

- You learn something useful from the analysis
- The analysis does not violate the privacy of any individual

An individual's **privacy is violated** if:

- The analyst learns something about the individual that they did not know before the analysis took place

Danger: this is a very strong statement

Aside: Privacy is not Security

Data **privacy** **is distinct from** data **security**.

Aside: Privacy is not Security

Data **privacy** **is distinct from** data **security**.

Data security is concerned with **who** can touch the data:

- **Confidentiality**: ensuring that only the appropriate people can view the data
- **Integrity**: ensuring that only the appropriate people can modify the data

Aside: Privacy is not Security

Data **privacy is distinct from** data **security**.

Data security is concerned with **who** can touch the data:

- **Confidentiality**: ensuring that only the appropriate people can view the data
- **Integrity**: ensuring that only the appropriate people can modify the data

Data privacy is concerned with **what can be learned** from the data (i.e. its **information content**)

Example: Census Data

Census protects data privacy via **aggregation**

Population	
Population estimates, July 1, 2017, (V2017)	**623,657**
Population estimates base, April 1, 2010, (V2017)	625,741
Population, percent change - April 1, 2010 (estimates base) to July 1, 2017, (V2017)	-0.3%
Population, Census, April 1, 2010	625,741
Age and Sex	
Persons under 5 years, percent	⚠ 4.8%
Persons under 18 years, percent	⚠ 18.7%
Persons 65 years and over, percent	⚠ 18.7%
Female persons, percent	⚠ 50.6%

Grouping participants makes it difficult to learn something specific to any individual

Example: Violating Privacy under Aggregation

A company releases the average salary of its employees each year:

Year	Average Salary
2017	$73,568
2018	$74,872

Example: Violating Privacy under Aggregation

A company releases the average salary of its employees each year:

Year	**Average Salary**
2017	$73,568
2018	$74,872

Auxiliary information:

- 58 employees in 2017
- Your friend Bob was hired between the two releases

Example: Violating Privacy under Aggregation

A company releases the average salary of its employees each year:

Year	Average Salary
2017	\$73,568
2018	\$74,872

Auxiliary information:

- 58 employees in 2017
- Your friend Bob was hired between the two releases

$$\frac{\sum e_i}{58} = 73,568 \quad \frac{\sum e_i + B}{59} = 74,872$$

Bob's salary: \$150,504

Census Will Use Differential Privacy!

The modernization of statistical disclosure limitation at the U.S. Census Bureau

Aref N. Dajani[1], Amy D. Lauger[1], Phyllis E. Singer[1], Daniel Kifer[2], Jerome P. Reiter[3], Ashwin Machanavajjhala[4], Simson L. Garfinkel[1], Scot A. Dahl[6], Matthew Graham[7], Vishesh Karwa[8], Hang Kim[9], Philip Leclerc[1], Ian M. Schmutte[10], William N. Sexton[11], Lars Vilhuber[7, 11], and John M. Abowd[5]

Privacy Violations that Aren't

An individual's **privacy is violated** if:

- The analyst learns something about the individual that they did not know before the analysis took place

Privacy Violations that Aren't

An individual's **privacy is violated** if:

- The analyst learns something about the individual that they did not know before the analysis took place

Example:

- A study concludes that coffee drinkers have 100% chance of being mean to pets
- **Auxiliary information**: Joe drinks coffee
- **Conclusion**: Joe is probably mean to his pets

Privacy Violations that Aren't

An individual's **privacy is violated** if:

- The analyst learns something about the individual that they did not know before the analysis took place

Example:

- A study concludes that coffee drinkers have 100% chance of being mean to pets
- **Auxiliary information**: Joe drinks coffee
- **Conclusion**: Joe is probably mean to his pets

Is this a privacy violation?

Privacy Violations that Aren't

An individual's **privacy is violated** if:

- The analyst learns something about the individual that they did not know before the analysis took place

Example:

- A study concludes that coffee drinkers have 100% chance of being mean to pets
- **Auxiliary information**: Joe drinks coffee
- **Conclusion**: Joe is probably mean to his pets

Is this a privacy violation?

Consider: the "violation" happens **whether or not Joe participates in the study!**

A Revised Definition

A data analysis violates an **individual's privacy** if:

- The analyst learns something about the individual that they would not have learned if the individual **had not participated in the analysis**

A Revised Definition

A data analysis violates an **individual's privacy** if:

- The analyst learns something about the individual that they would not have learned if the individual **had not participated in the analysis**

In other words:

- A privacy-preserving analysis should have the same outcome, **regardless of the participation** of any particular individual

Outline

1. Administrative
2. What is data privacy, and how is it violated?
3. How do data privacy violations affect us?

AOL Web Search Dataset

A Face Is Exposed for AOL Searcher No. 4417749

By MICHAEL BARBARO and TOM ZELLER Jr. AUG. 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from "numb fingers" to "60 single men" to "dog that urinates on everything."

Auxiliary data: biographical information (dog ownership, location)

Netflix Prize Dataset

Robust De-anonymization of Large Sparse Datasets

Arvind Narayanan and Vitaly Shmatikov
The University of Texas at Austin

Abstract

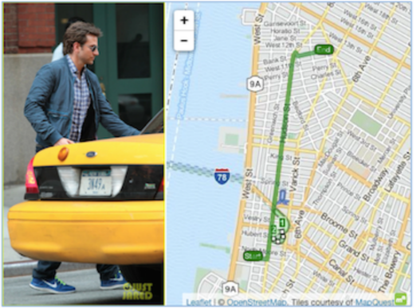
We present a new class of statistical de-anonymization attacks against high-dimensional micro-data, such as individual preferences, recommendations, transaction records and so on. Our techniques are robust to perturbation in the data and tolerate some mistakes in the adversary's background knowledge.

We apply our de-anonymization methodology to the

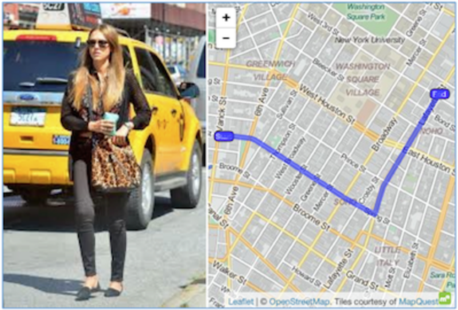
and sparsity. Each record contains many attributes (*i.e.*, columns in a database schema), which can be viewed as dimensions. Sparsity means that for the average record, there are no "similar" records in the multi-dimensional space defined by the attributes. This sparsity is empirically well-established [7, 4, 19] and related to the "fat tail" phenomenon: individual transaction and preference records tend to include statistically rare attributes.

Auxiliary data: Internet Movie Database ratings

NYC Taxi Data



Bradley Cooper (Click to Explore)



Jessica Alba (Click to Explore)

Auxiliary data: geotagged celebrity gossip photos

James Comey's Twitter Account

James Comey confirms he is Reinhold Niebuhr on Twitter

Jordan Crook @jordanrcrook / Oct 24, 2017 Comment

James Comey, the former FBI director who was abruptly fired in May, has seemingly revealed himself as **Twitter** user Reinhold Niebuhr.

Auxiliary data: social graph (Comey's son)

Latanya Sweeney & Medical Records

BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION

Paul Ohm*

At the time that GIC released the data, William Weld, then–Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers.[86] In response, then–graduate student Sweeney started hunting for the Governor's hospital records in the GIC data.[87] She knew that

Auxiliary data: voter rolls (date of bith, gender, zip code)

Latanya Sweeney & Medical Records

BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION

Paul Ohm[*]

At the time that GIC released the data, William Weld, then–Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers.[86] In response, then–graduate student Sweeney started hunting for the Governor's hospital records in the GIC data.[87] She knew that

Auxiliary data: voter rolls (date of bith, gender, zip code)

DOB, gender, zip code uniquely identify 87% of people in US

Latanya Sweeney & Genetic Data

Harvard Professor Re-Identifies Anonymous Volunteers In DNA Study

Adam Tanner Contributor
I write about the business of personal data.

A Harvard professor has re-identified the names of more than 40% of a sample of anonymous participants in a high-profile DNA study, highlighting the dangers that ever greater amounts of personal data available in the Internet era could unravel personal secrets.

Auxiliary data: zip code, date of birth and gender

Strava's Heatmap

Nathan Ruser
@Nrg8000

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee… … It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

2:24 PM - Jan 27, 2018

2,647 2,404 people are talking about this

Strava's Heatmap

Nathan Ruser
@Nrg8000

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee… … It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

2:24 PM - Jan 27, 2018

2,647 2,404 people are talking about this

Question: were any individuals harmed?
Is this a privacy violation at all?

Lessons Learned

- **Aggregation** doesn't necessarily protect individual privacy
- **Anonymization** doesn't necessarily protect individual privacy
- **Large datasets** (i.e. large populations) don't necessarily protect individual privacy

Lessons Learned

- **Aggregation** doesn't necessarily protect individual privacy
- **Anonymization** doesn't necessarily protect individual privacy
- **Large datasets** (i.e. large populations) don't necessarily protect individual privacy
- **Machine learning** doesn't necessarily protect individual privacy

Lessons Learned

- **Aggregation** doesn't necessarily protect individual privacy
- **Anonymization** doesn't necessarily protect individual privacy
- **Large datasets** (i.e. large populations) don't necessarily protect individual privacy
- **Machine learning** doesn't necessarily protect individual privacy
- Defining privacy is hard

Lessons Learned

- **Aggregation** doesn't necessarily protect individual privacy
- **Anonymization** doesn't necessarily protect individual privacy
- **Large datasets** (i.e. large populations) don't necessarily protect individual privacy
- **Machine learning** doesn't necessarily protect individual privacy
- Defining privacy is hard

Principles for protecting privacy:

- Privacy threats are **counterintuitive**
- We **must** do something "extra" to ensure privacy
- We should **define privacy** carefully and precisely
- **Challenge**: tension between **accuracy** and **privacy**