Privacy and Its Impacts

Never Stand Still | Faculty of Engineering | Computer Science and Engineering

Dr. Wanli Xue
Senior Research Associate

Outline

- Privacy and its ‘definition’
- Security to privacy
- Privacy related cases (wireless apps)
- Privacy preserving techniques

Question: Privacy for Money?

- Willing to sell privacy for money?

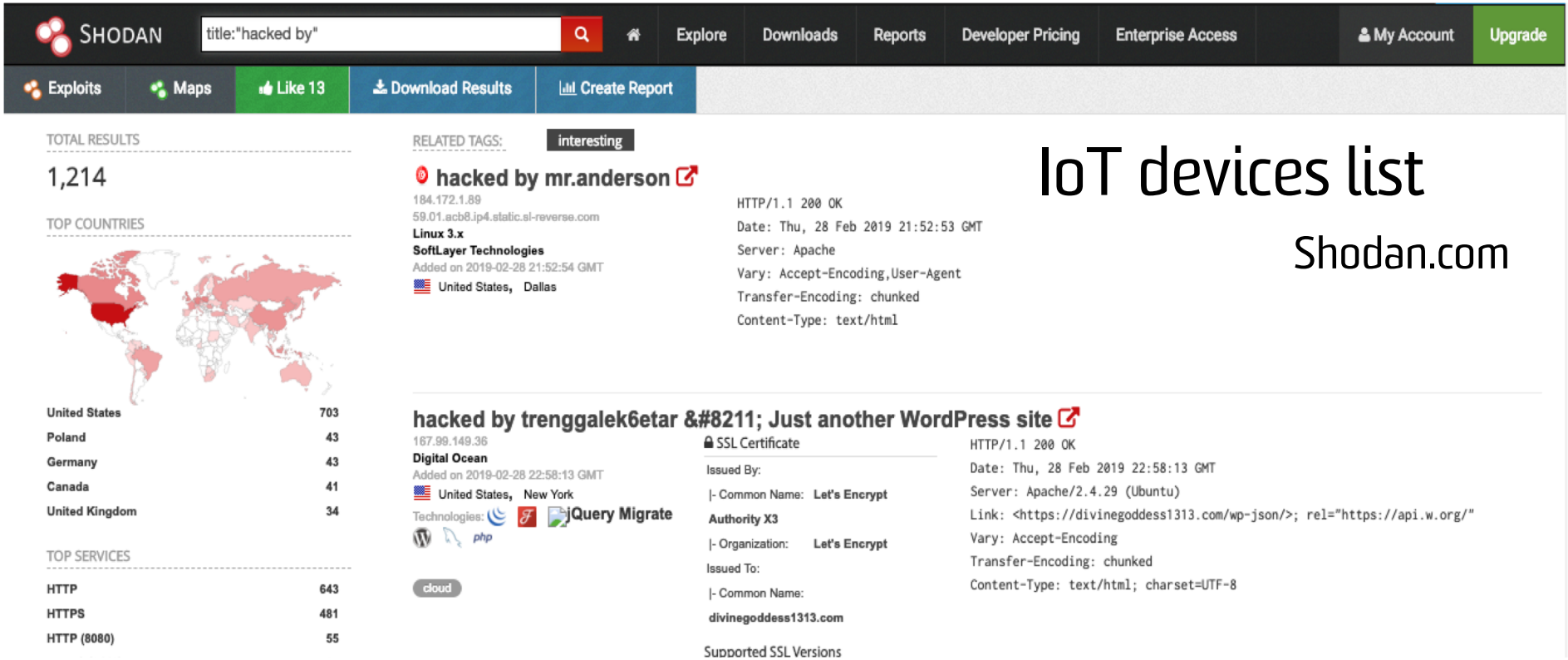
- To What extent
  - 1. I ate an apple at 10:00 am
  - 2. I ate apples this morning
  - 3. I ate something sometime
  - 4. I had bla bla

- At what price?

Privacy is a Relative Definition

- No clear boundary
- Ambiguous
  - Some website or activity is legal in one country but illegal in another
- Difficult to reach an agreement
  - People wear cloth to cover the private part of body
  - Which part of body is supposed to be covered when fire alarm triggers in public bathhouse

Keyword: Hacked by, Camera, etc.



A hacked camera?

A hacked camera?

- Happening in Ukraine
- More than 24 hours
- So many flows even make service unavailable

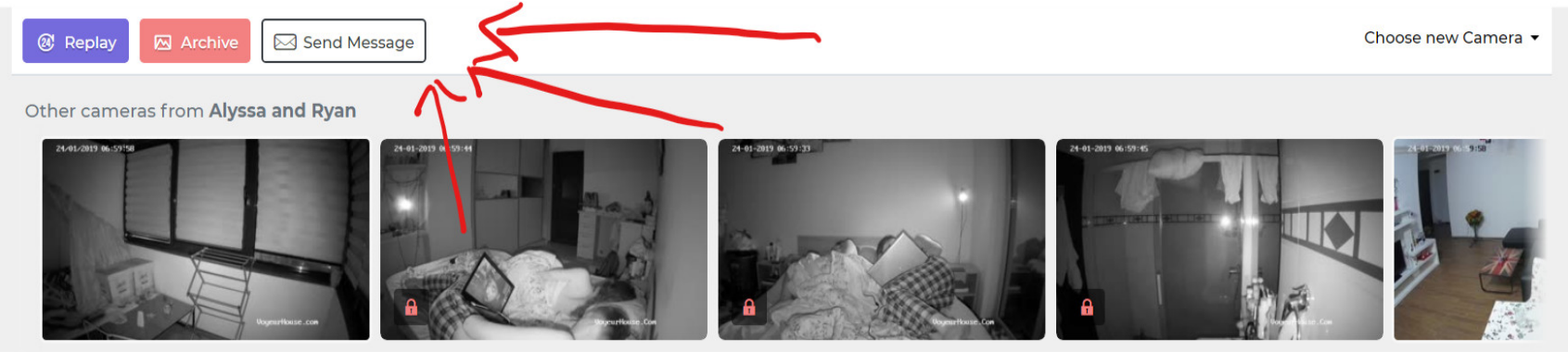
- What is that actually?

503 Service Unavailable

No server is available to handle this request.
ded6144

Not Security Issue, only Privacy

- No one get hacked, they are willing to do
- Live broadcast website
- Legal in Ukraine
- People are willing to do that



Are these also privacy issues?

- What is the difference between this and
  - Facebook (Wechat, *Google+)* social circle
  - Instagram pictures (selfies)
  - Vlog, youtuber
  - Short video (e.g., Tik Tok)

Google+ has been announced to be shut down because of privacy leakage

Security vs. Privacy

- Bypass the protection
- Without authorization
- Illegal
- Gain information directly
- Will cause loss directly

- Don’t have to hack a system
- All the data is there (usually)
- Gain information via sophisticated methods (e.g., AI)
- Illegal or legal?

Privacy from Industry

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

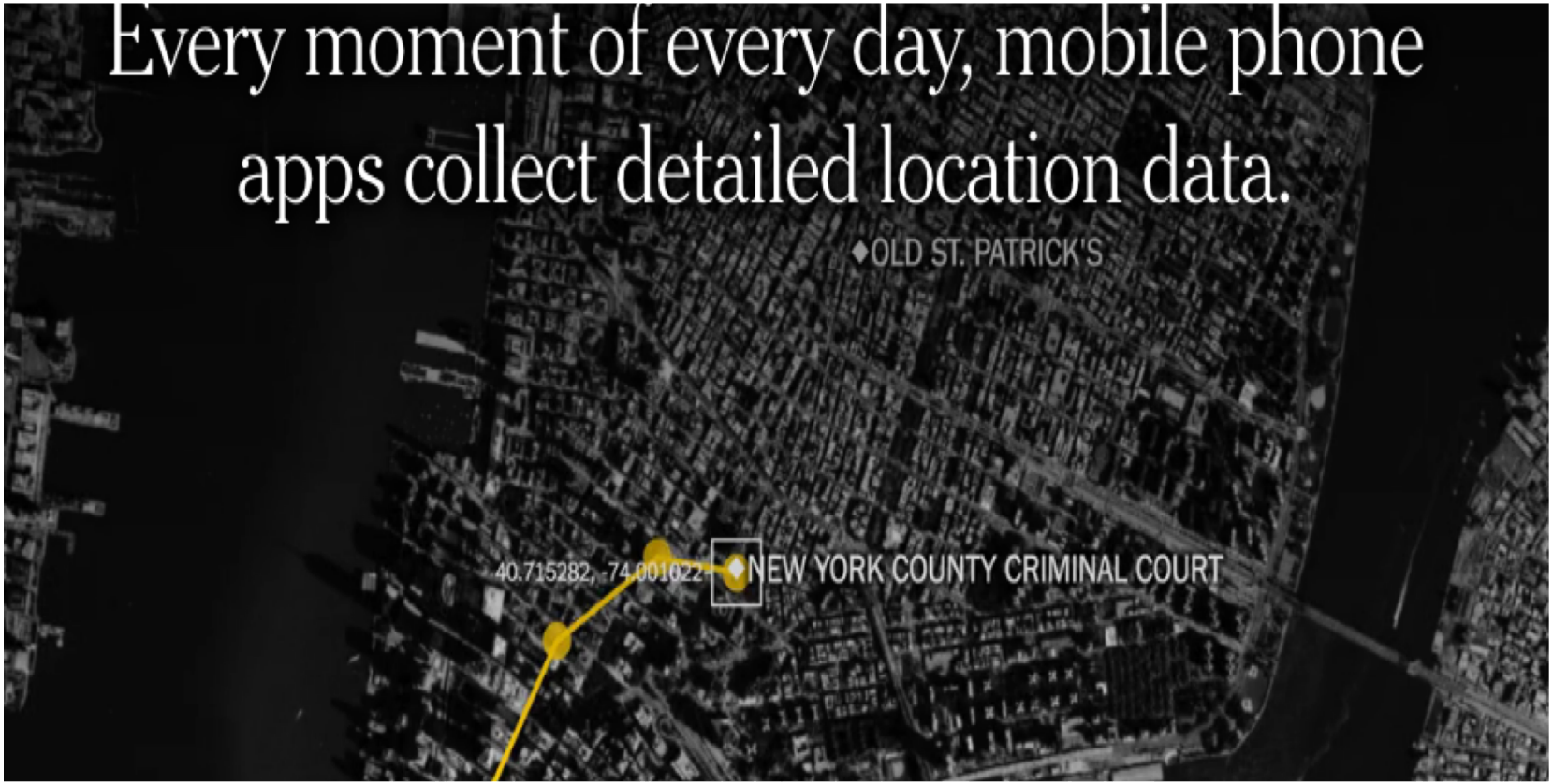
- **Latest: Strava suggests military users 'opt out' of heatmap as row deepens**

GPS information

- Privacy of location
- Privacy of identity
- …

https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Apps know you well/better



https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

What can Privacy Leakage Cause?

- Give away secret army base location (attack?)
- What did you do last night (ex-boyfriends address?)
- Which path for jogging (encounter coincidently?)
- Smart home IoT devices list (IP address? Protocols?)

Another real case

- A Seizure?

A Tweet to Kurt Eichenwald, a Strobe and a Seizure. Now, an Arrest.

The journalist Kurt Eichenwald at his home in Dallas, Tex., on Friday.
Brandon Thibodeaux for The New York Times

By Cecilia Kang

March 17, 2017

WASHINGTON — When the journalist Kurt Eichenwald opened an animated image sent to him on Twitter in December, the message "You deserve a seizure for your posts" appeared in capital letters along with a blinding strobe light. Mr. Eichenwald, who has epilepsy, immediately suffered a seizure.

"a Twitter post with a GIF. When Mr. Eichenwald clicked on the file, the strobe light triggered the seizure, his lawyer said. Mr. Eichenwald fell to the ground."

- Know he has epilepsy
- Send a Twitter message
- Triger the epilepsy
- Get caught..

https://www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html

Protect the Privacy

-- EU GDPR

- EU General Data Protection Regulation (GDPR)
  - the most important change in data privacy regulation in 20 years.
- What should be protected?
  - Identity
  - Location
  - Health

…

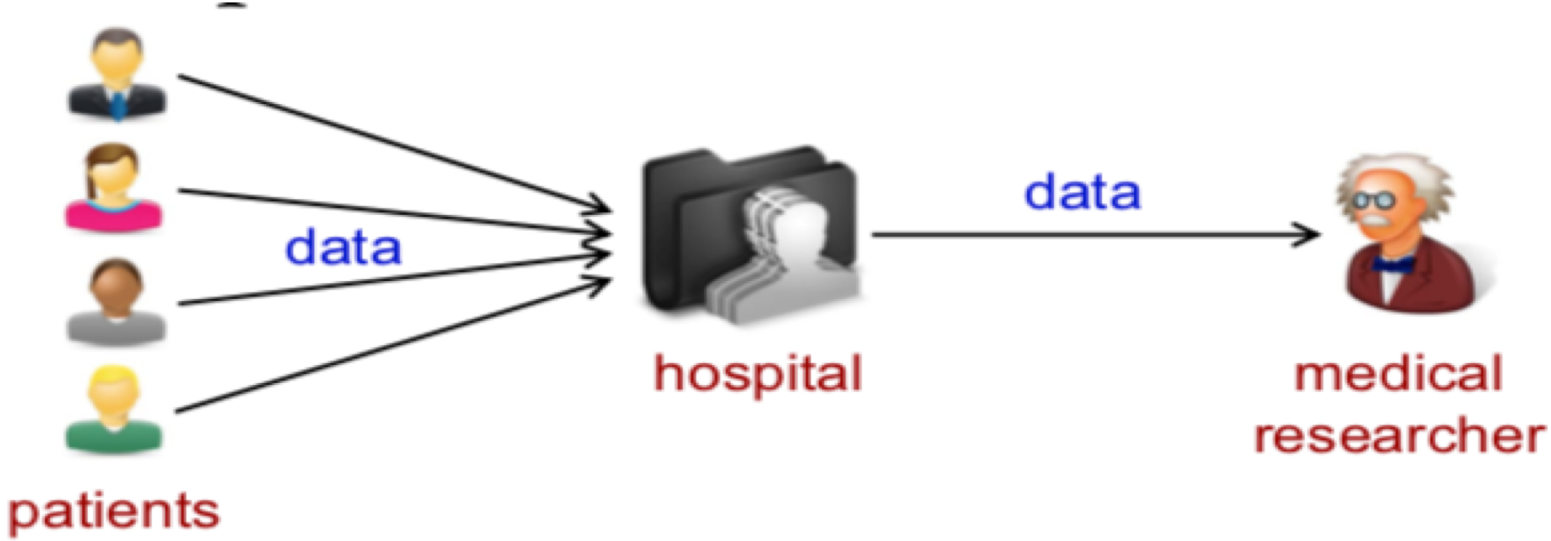
- Utility? ------ Privacy preservation techniques

Privacy Preserving Techniques

- Privacy preserving data publishing: What and Why
- Examples of privacy attacks
- Existing solutions
- Conclusion and open problems

All material from now on adapted from Xiaokui Xiao, Nanyang Technological University

Example: Medical Data Release



- Each contributor: provides data about herself
- Hospital: collects data and releases them in a certain form
- Recipient: uses the released data for analysis

Privacy Preserving Data Publishing

- Objectives:
  - The privacy of the contributors are protected
    - Location, identities, age, postcode…
  - The recipient gets useful data
    - To provide service for public, recommendation, research

Why is this important?

- Many types of research rely on the availability of private data
  - Demographic research
  - Medical research
  - Social network studies
  - Web search studies
  - …

Why is this difficult?

- Intuition
  - There are only 7 billion people on earth
  - 7 billion ≈ 33 bits
  - Theoretically speaking, we need only 33 bits of information to pinpoint an individual

Privacy Breach: The MGIC Case

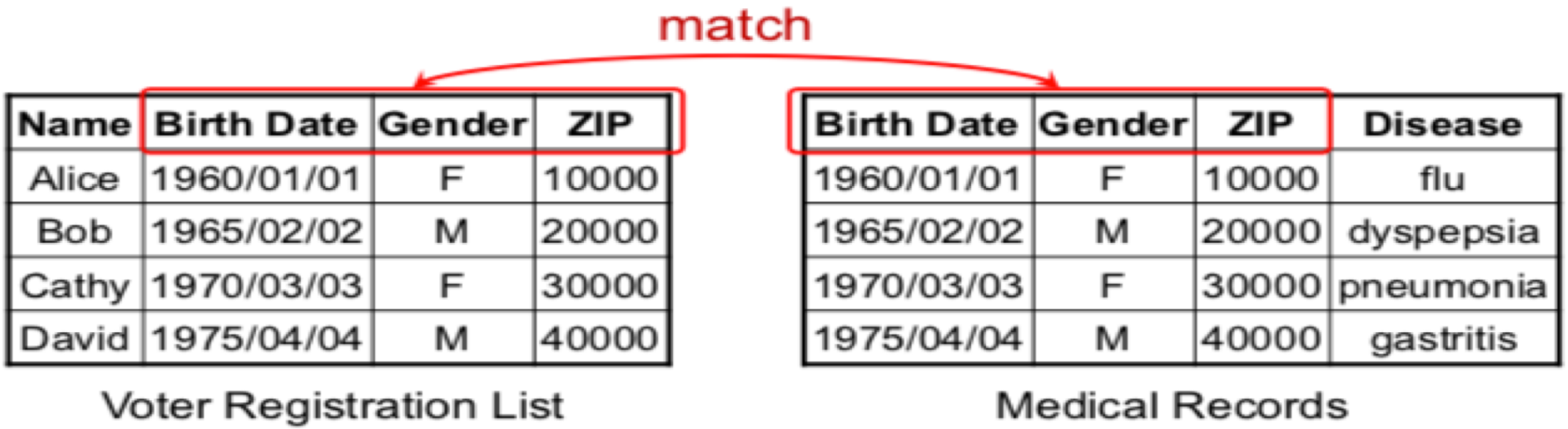
- Time: mid-1990s
- Curator: Massachusetts Group Insurance Commission (MGIC)
- Data released: “anonymized” medical records
- Intention: facilitate medical research

Name	Birth Date	Gender	ZIP	Disease
Alice	1960/01/01	F	10000	flu
Bob	1965/02/02	M	20000	dyspepsia
Cathy	1970/03/03	F	30000	pneumonia
David	1975/04/04	M	40000	gastritis

Medical Records

Privacy Breach: The MGIC Case

- Time: mid-1990s
- Curator: Massachusetts Group Insurance Commission
- (MGIC)
- Data released: “anonymized” medical records
- Intention: facilitate medical research

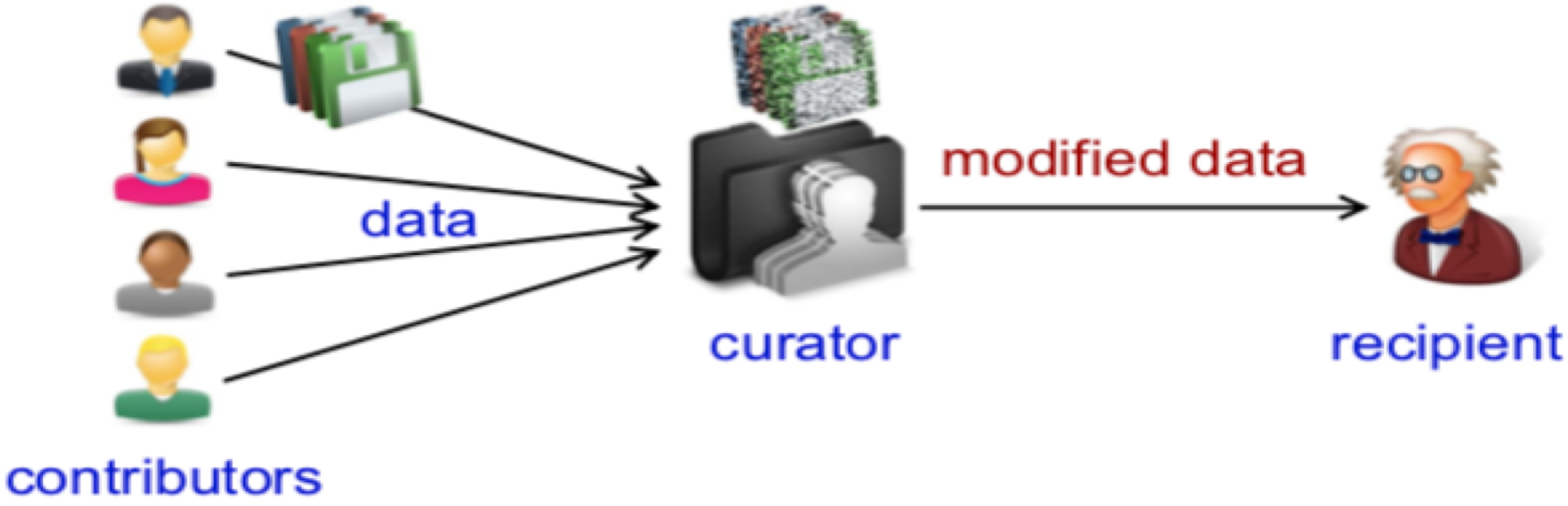


Other Privacy Breach

- The American Online 2006 : keywords in search queries
- The DNA case 2005: dob, birthplace
- IMDb and Netflix

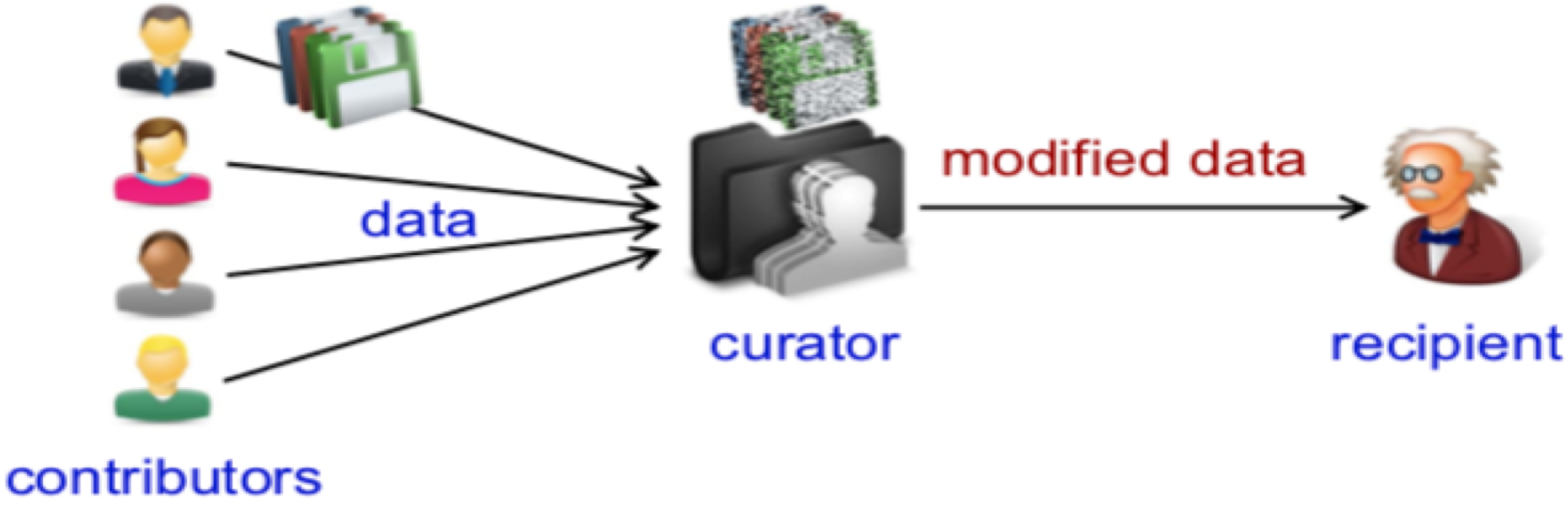
- Hotels, credit cards, Google+, **FB**,…

Aim of Privacy Preserving Data Publishing



- Publish a modified version of the data, such that
  - the contributors' privacy is "adequately" protected
  - the published data is useful for its intended purpose (at least to some degree)

Privacy Preserving Data Publishing



- Two issues
  - privacy principle: what do we mean by “adequately” protected privacy?
  - modification method: how should we modify the data to ensure privacy while maximizing utility?

Existing Solutions

- This talk will focus on solutions with formal privacy models (developed after 2000)
  - *k*-anonymity
  - *l*-diversity
  - (t-closeness)
  - differential privacy

- Before 2000
  - Previous solutions without a formal privacy model
  - Evaluates privacy based on empirical studies only

k-Anonymity: Example

- Suppose that we want to publish the medical records below
- We know that
  - eliminating names is not enough
  - because an adversary may identify patients by Age and ZIP

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

Age	ZIP	Disease
20	10000	flu
30	20000	dyspepsia
40	30000	pneumonia
50	40000	gastritis

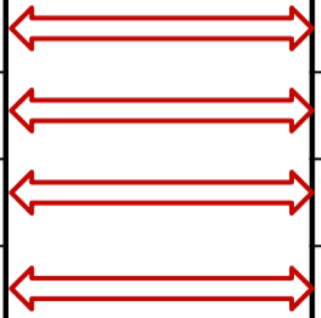
medical records

k-Anonymity: Example

- *k*-anonymity [Sweeney 2002]
  - requires that each (Age, ZIP) combination can be matched to at least *k* patients
- How?
- Make Age and ZIP less specific in the medical records

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge



Age	ZIP	Disease
20	10000	flu
30	20000	dyspepsia
40	30000	pneumonia
50	40000	gastritis

medical records

k-Anonymity: Example

- *k*-anonymity [Sweeney 2002]
  - requires that each (Age, ZIP) combination can be matched to at least *k* patients

2-anonymous table

"generalization"

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

Age	ZIP	Disease
[20,30]	[10000,20000]	flu
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

medical records

k-Anonymity: General Approach

- Identify the attributes that the adversary may know
  - Referred to as Quasi-Identifiers (QI)
- Divide tuples in the table into groups of sizes at least *k*
- Generalize the QI values of each group to make them identical

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

QI

Age	ZIP	Disease
[20,30]	[10000,20000]	flu
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-anonymous table

k-Anonymity: Vulnerability

- *k*-anonymity requires that each combination of quasi-identifiers (QI) is hidden in a group of size at least *k*
- But it says nothing about the remaining attributes
- Result: Disclosure of sensitive attributes is possible

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

QI sensitive

Age	ZIP	Disease
[20,30]	[10000,20000]	flu
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-anonymous table

k-Anonymity: Vulnerability

- Intuition:
  - Hiding in a group of *k* is not sufficient
  - The group should have a diverse set of sensitive value

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

QI sensitive

Age	ZIP	Disease
[20,30]	[10000,20000]	dyspepsia
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-anonymous table

l-Diversity [Machanavajjhala et al. 2006]

- Approach: (similar to *k*-anonymity)
  - Divide tuples into groups, and make the QI of each group identical
- Requirement: (different from *k*-anonymity)
  - Each group has at least *l* "well-represented" sensitive values
- Several definitions of "well-represented" exist
  - Simplest one: in each group, no sensitive value is associated with more than 1/*l* of the tuples

Age	ZIP	Disease
[20,30]	[10000,20000]	flu
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-diverse table

l-Diversity [Machanavajjhala et al. 2006]

- Rationale: The 1/*l* association in the generalized table leads to 1/*l* confidence for the adversary

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

Age	ZIP	Disease
[20,30]	[10000,20000]	flu
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-diverse table

l-Diversity: Vulnerability

- Suppose that the adversary wants to find out the disease of Bob
- The adversary knows that Bob is unlikely to have breast cancer
- So he knows that Bob is likely to have dyspepsia

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

Age	ZIP	Disease
[20,30]	[10000,20000]	breast cancer
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-diverse table

l-Diversity: Vulnerability

- Intuition:
  - It is not sufficient to impose constraints of the diversity of sensitive values in each group
  - Need to take into account the adversary's background knowledge (e.g., males are unlikely to have breast cancer)

Name	Age	ZIP
Andy	20	10000
Bob	30	20000
Cathy	40	30000
Diane	50	40000

adversary's knowledge

Age	ZIP	Disease
[20,30]	[10000,20000]	breast cancer
[20,30]	[10000,20000]	dyspepsia
[40,50]	[30000,40000]	pneumonia
[40,50]	[30000,40000]	gastritis

2-diverse table

Algorithm-Based Attacks

- Algorithms designed for *l*-diversity (and its improvements) are often vulnerable to *algorithm-based attacks*
- Intuition:
  - Those algorithms always try to use the least amount of generalization to achieve *l*-diversity
  - An adversary can utilize the characteristics of the algorithms to do some “reverse engineering” on the generalized tables

Brief Summary

- Assumption about adversary's knowledge
- Adapted for each dataset
- Most proposed methods are vulnerable for algorithm-based attacks
- It does not converge to a "final" adversary model

Differential Privacy [Dwork 2006]

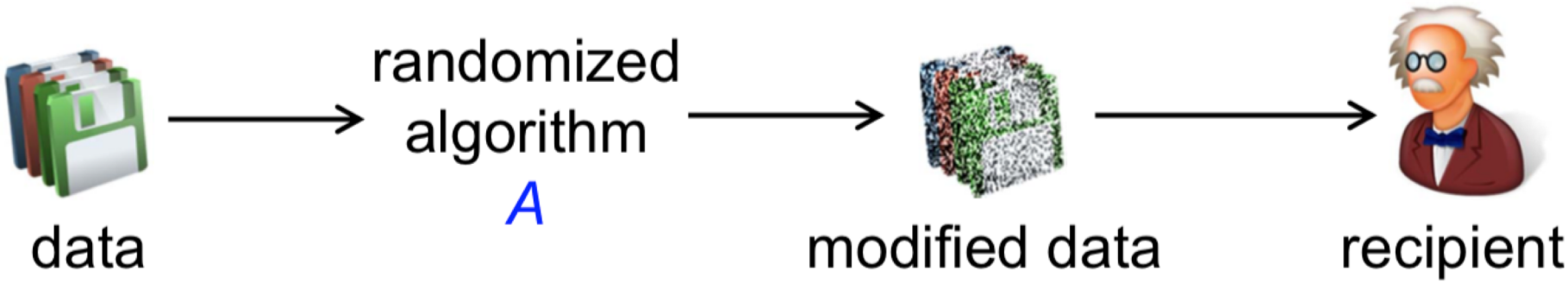
- A privacy principle proposed by theoreticians
- More difficult to understand *k*-anonymity and *l*-anonymity
- Becomes well-adopted because
  - Its privacy model is generally considered strong “enough”
  - Its definition naturally takes into account algorithm-based attacks

Differential Privacy: Intuition

- Suppose that we have a dataset *D* that contains the medical record of every individual in Australia
- Suppose that Alice is in the dataset
- Intuitively, is it OK to publish the following information?
  - Whether Alice has diabetes
  - The total number of diabetes patients in *D*
- Why is it OK to publish the latter but not the former?
- Intuition:
  - The former completely depends on Alice
  - The latter does not depend much on Alice

Differential Privacy: Intuition

- In general, we should only publish information that does not highly depend on any particular individual
- This motivates the definition of differential privacy

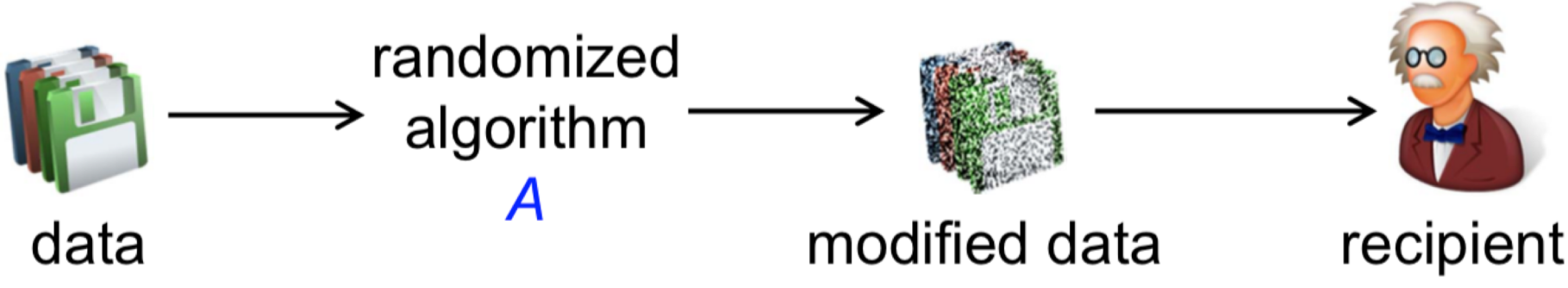


Differential Privacy: Definition

- Neighbouring datasets:
  - Two datasets *D* and *D'*, such that *D'* can be obtained by changing one single tuple in *D*
- A randomized algorithm *A* satisfies ε-differential privacy, iff for any two neighbouring datasets *D* and *D'* and for any output *O* of *A*,

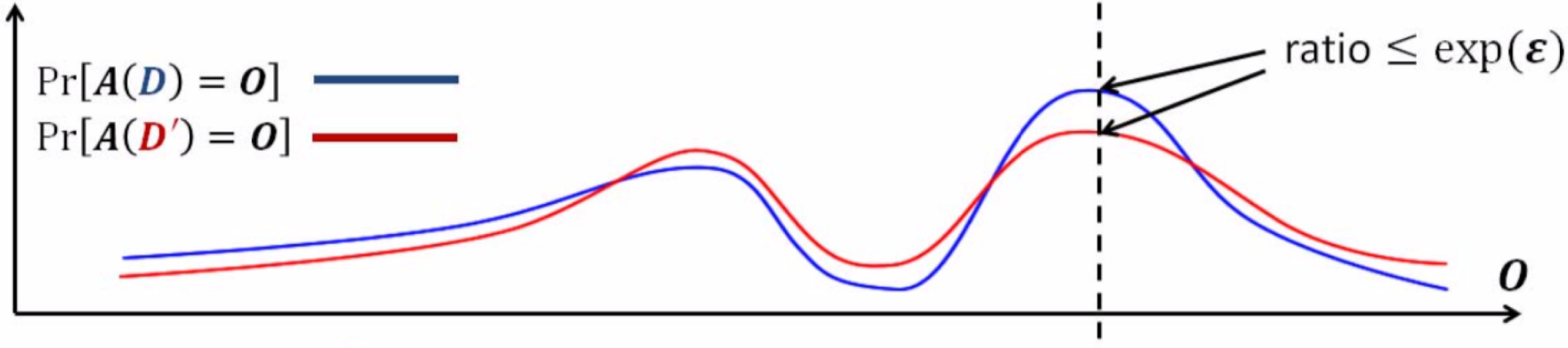
$$\Pr[\boldsymbol{A}(\boldsymbol{D}) = \boldsymbol{O}] \leq \exp(\boldsymbol{\varepsilon}) \cdot \Pr[\boldsymbol{A}(\boldsymbol{D'}) = \boldsymbol{O}]$$

- Rationale: The output of the algorithm does not highly depend on any particular tuple in the input



Differential Privacy: Definition

- Illustration of ε-differential privacy



where D and D' are neighboring databases that differ by **at most one** tuple

$$\exp(-\varepsilon) \leq \frac{\Pr[A(D) = O]}{\Pr[A(D') = O]} \leq \exp(\varepsilon)$$

Achieving Differential Privacy: Example

- Suppose that we have a set *D* of medical records
  - the number of diabetes patients in *D* (e.g., 1000)

- Naïve solution: Release 1000 directly
  - Easy to be accessed by adversary, and it violates dp, since

$$\Pr[\boldsymbol{A}(\boldsymbol{D}) = \mathbf{1000}] \leq \exp(\boldsymbol{\varepsilon}) \cdot \Pr[\boldsymbol{A}(\boldsymbol{D'}) = \mathbf{1000}]$$

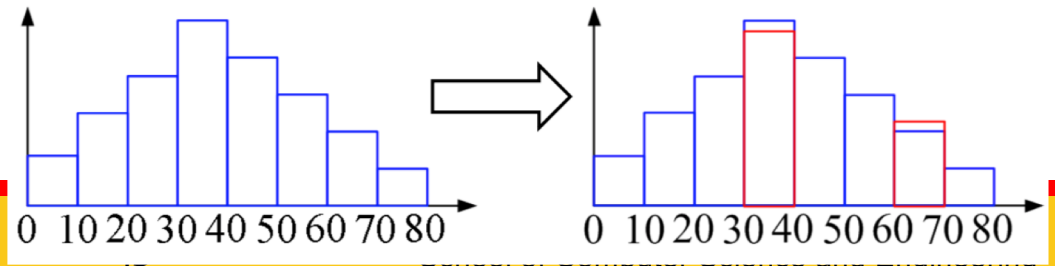
    dose not hold
- Better solution: add noise into 1000 before releasing it
  - What kind of noise should add
  - How to make it satisfy dp

The Laplace Mechanism

- In general, if we want to release a set of values (e.g., counts) from a dataset,
  - We add i.i.d. Laplace noise to each value to achieve differential privacy
- This general approach is called *the Laplace mechanism*
- Figuring out the correct amount of noise to use could be a research issue
  - λ noise leads to (1/ λ)-differential privacy
  - 1/ λ = ϵ

----------Another example----------

  - 2 λ noise leads to (1/ λ)-differential privacy



Other Research Issues

- In general, choosing a good strategy requires exploiting the characteristics of
  - the input data
  - the output results
  - the way that users may use the output results

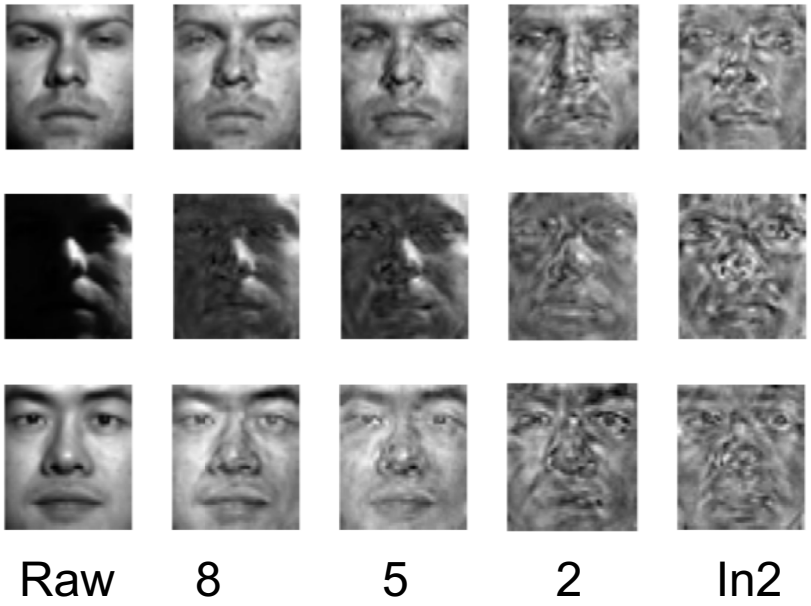
- Other approaches:
  - Exponential mechanism for non-numerical value
  - Random response, RAPPOR of Google

Open Problems

- Differential privacy might be too strong
  - It requires that changing one tuple should not bring much change to the published result
- Alternative interpretation:
  - Even if an adversary knows n – 1 tuples in the input data, he won't be able to infer information about the remaining tuple
- Knowing n – 1 individuals is often impossible
- How should we relax differential privacy?

Open Problems

- How to choose an appropriate ϵ for ϵ - differential privacy?
- Need a way to quantify the cost of privacy and the gain of utility in releasing data



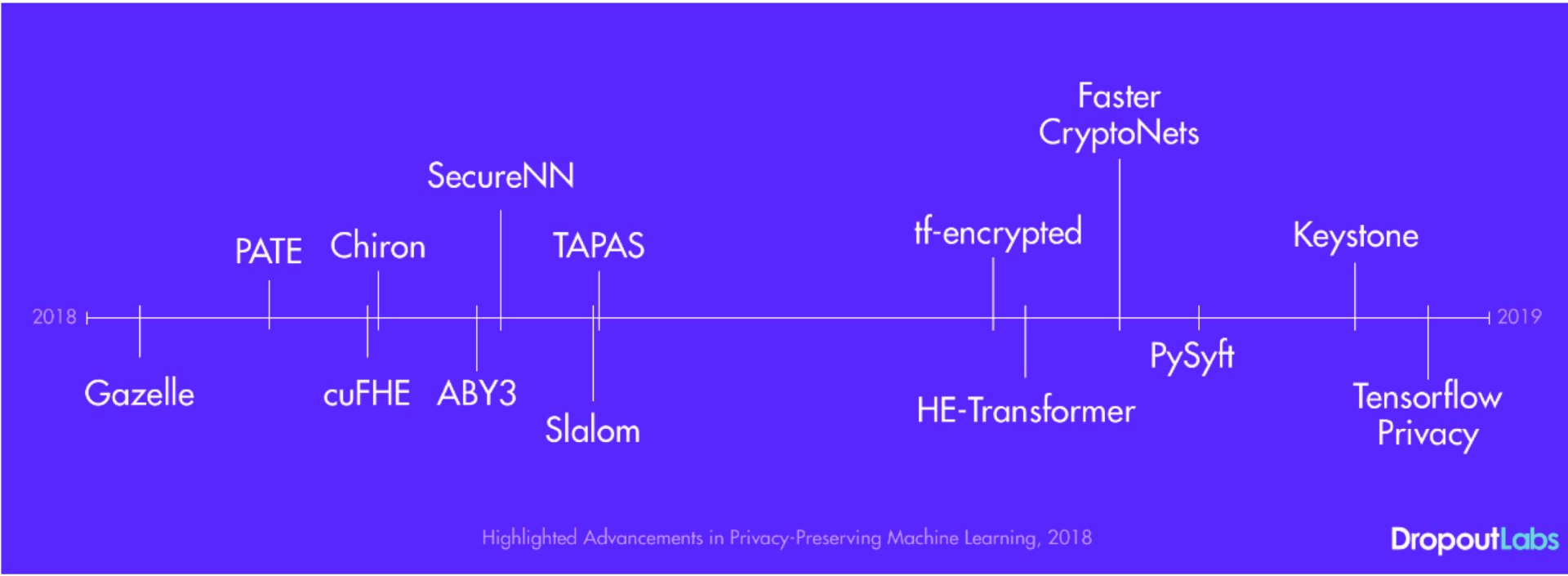
Xue, W., Shen, Y., Luo, C., Hu, W. and Seneviratne, A., 2018, August. Acies: A Privacy-Preserving System for Edge-Based Classification. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 914-919). IEEE.

Where is Differential Privacy in Real?

- Using in your apps/web …
  - Apple

    https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf
  - Google
    - e.g., Chrome, RAPPOR, differential privacy with deep learning, TensorFlow/privacy
  - Microsoft?
    - Only vulnerabilities? IE? Excel?
    - Cynthia Dwork, who propose the differential privacy, is a research in MS...

More Interesting



https://medium.com/dropoutlabs/privacy-preserving-machine-learning-2018-a-year-in-review-b6345a95ae0f

Reference and Acknowledgement:

- Each of them is labelled when they appeared
  - Shodan.com
  - Wechat blog: 浅黑科技 https://mp.weixin.qq.com/s/8SRxYHg6rJmh-ITRTqYMGw (Chinese)
  - App example1https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
  - App example2https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html
  - Epilepsy case https://www.nytimes.com/2017/03/17/technology/social-media-attack-that-set-off-a-seizure-leads-to-an-arrest.html
  - **All material about privacy preservation techniques adapted from Xiaokui Xiao, Nanyang Technological University https://people.cs.pitt.edu/~bill/1699/read/374aa6a.pdf**
  - state-of-the-art PPML https://medium.com/dropoutlabs/privacy-preserving-machine-learning-2018-a-year-in-review-b6345a95ae0f
  - Xue, W., Shen, Y., Luo, C., Hu, W. and Seneviratne, A., 2018, August. Acies: A Privacy-Preserving System for Edge-Based Classification. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 914-919). IEEE.


SCIENTIA
MANU ET MENTE
UNSW
THE UNIVERSITY OF NEW SOUTH WALES

Thanks!

Q&A

Appendix about Differential Privacy

Comparison with *k*-anonymity and *l*-diversity

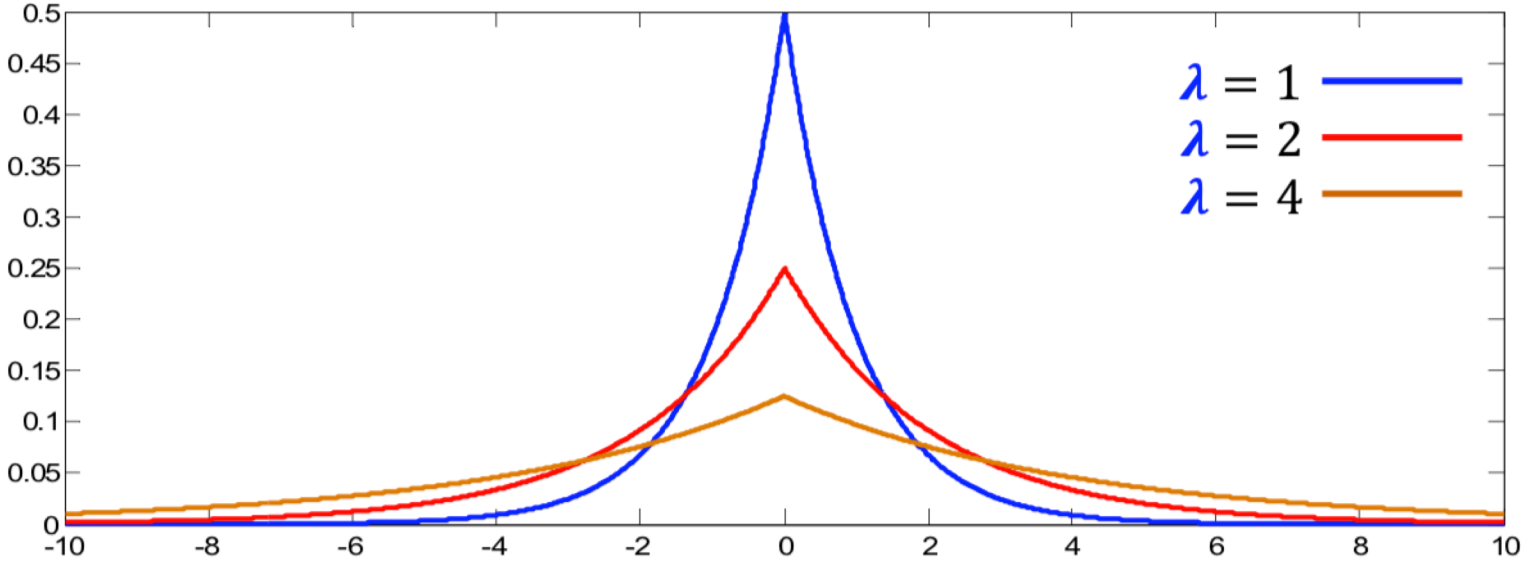
- Differential privacy does not directly model the adversary's knowledge

$$\exp(-\boldsymbol{\varepsilon}) \leq \frac{\Pr[\boldsymbol{A}(\boldsymbol{D}) = \boldsymbol{O}]}{\Pr[\boldsymbol{A}(\boldsymbol{D'}) = \boldsymbol{O}]} \leq \exp(\boldsymbol{\varepsilon})$$

- But its privacy protection is generally considered "strong enough"
- Differential privacy is more general
  - There is no restriction on the type of *O*
  - It can be a table, a set of frequent itemsets, a regression model, etc.

Laplace Distribution Noise

- $pdf(x) = \frac{1}{2\lambda}\exp(-\frac{|x|}{\lambda})$
- Increase/decrease x by α
  - $pdf(x)$ changes by a factor of $\exp\left(-\frac{|\alpha|}{\lambda}\right)$
- Variance: $2\lambda^2$; λ is referred as the scale



Laplace Distribution Noise

- Add Laplace noise before releasing the number of diabetes patients in *D*
- Changing one tuple in *D*
  - shifting the mean of Laplace distribution by 1
- The two distributions have bounded differences
  - differential privacy is satisfied