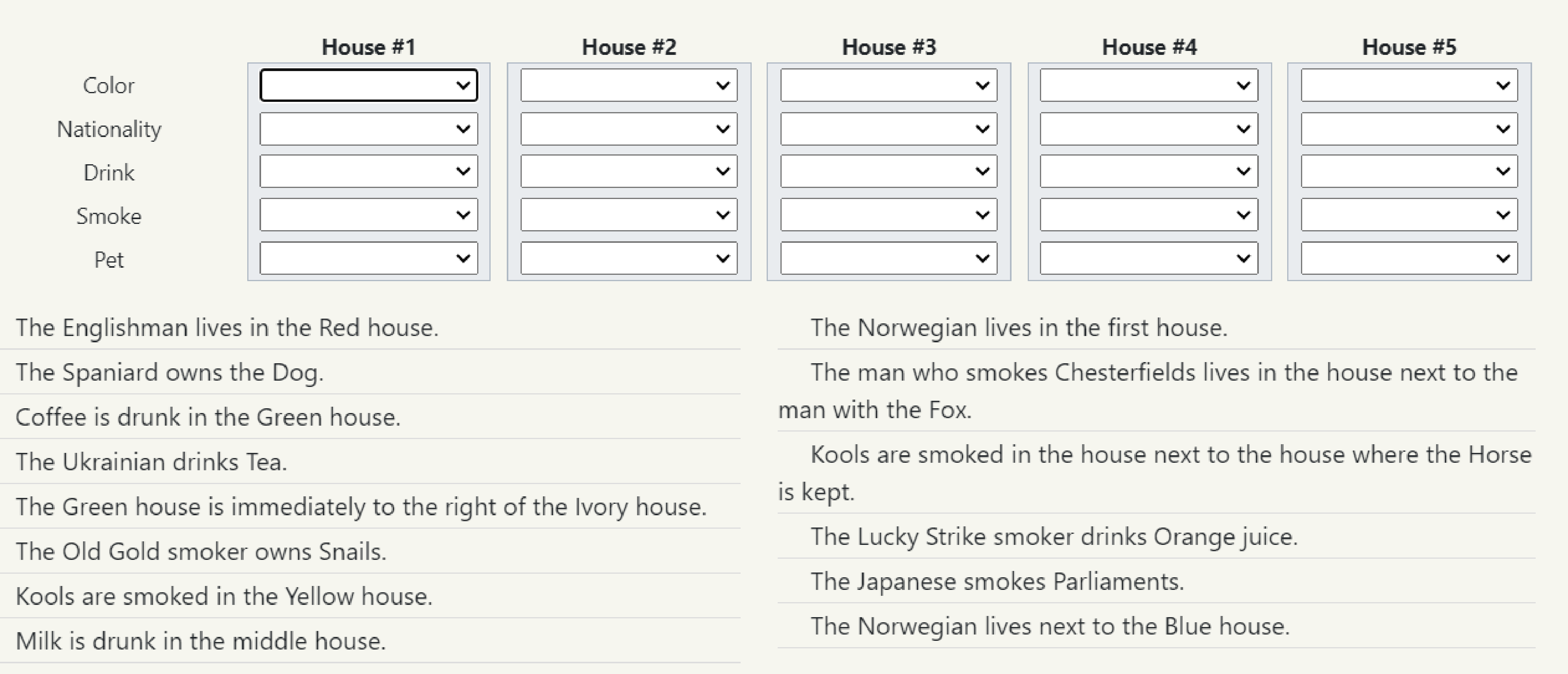
Differential Privacy for Policymakers

Clément Canonne, University of Sydney

15/02/2024

Prelude

Who owns the zebra? Who drinks water? 🦓



	House #1	House #2	House #3	House #4	House #5
Color					
Nationality					
Drink					
Smoke					
Pet					

The Englishman lives in the Red house.

The Spaniard owns the Dog.

Coffee is drunk in the Green house.

The Ukrainian drinks Tea.

The Green house is immediately to the right of the Ivory house.

The Old Gold smoker owns Snails.

Kools are smoked in the Yellow house.

Milk is drunk in the middle house.

The Norwegian lives in the first house.

The man who smokes Chesterfields lives in the house next to the man with the Fox.

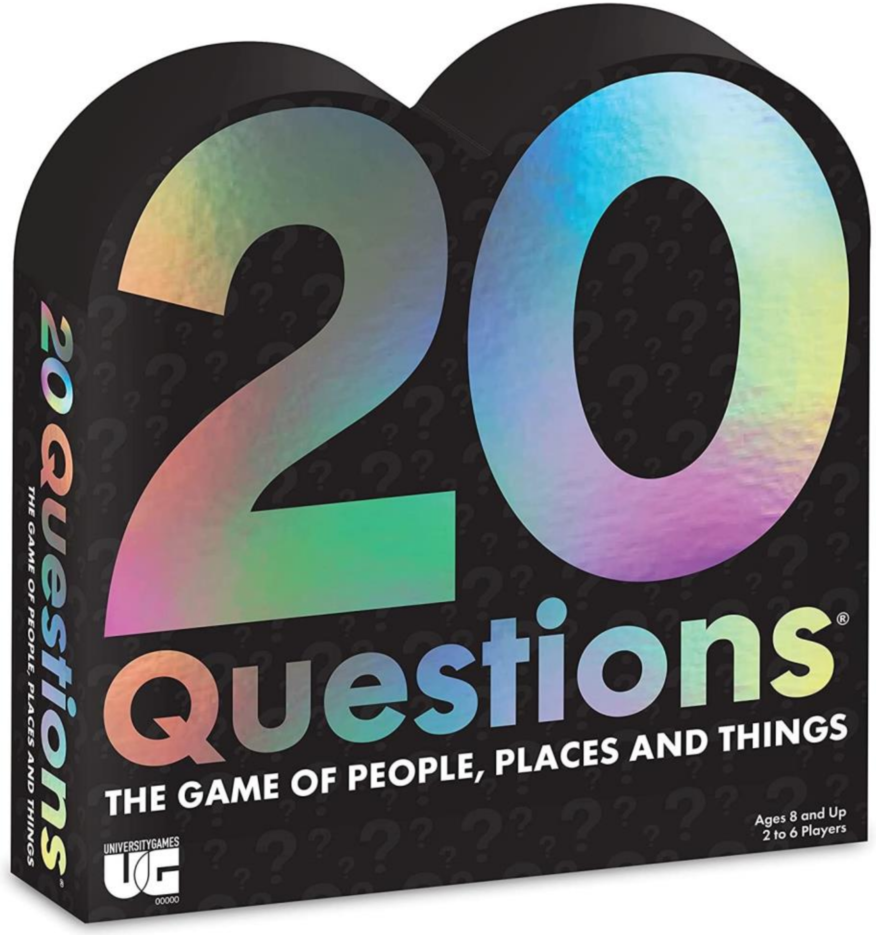
Kools are smoked in the house next to the house where the Horse is kept.

The Lucky Strike smoker drinks Orange juice.

The Japanese smokes Parliaments.

The Norwegian lives next to the Blue house.

Twenty questions


20
Questions®
THE GAME OF PEOPLE, PLACES AND THINGS
Ages 8 and Up
2 to 6 Players
UNIVERSITYGAMES
UG
20 Questions®
THE GAME OF PEOPLE, PLACES AND THINGS

“The original game of people, places and things is **back with an all-new look, and all-new content for today’s audience!**”

How is that relevant?

“Why”

What is **privacy**?

“I know it when I lost it”

- You cannot get it back

What is **privacy**?

- “I know it when I lost it”
  - You cannot get it back
- Maybe we can just deidentify data records? (remove personally identifying information)
  - Proxy information in the data itself
  - Multiple sources/ background information
  - “Attackers” may be smarter than we think

What is **privacy**?

- "I know it when I lost it"
  - You cannot get it back
- Maybe we can just deidentify data records? (remove personally identifying information)
  - Proxy information in the data itself
  - Multiple sources/ background information
  - "Attackers" may be smarter than we think

What is **privacy**?

- “I know it when I lost it”
  - You cannot get it back
- Maybe we can just deidentify data records? (remove personally identifying information)
  - Proxy information in the data itself
  - Multiple sources/ background information
  - “Attackers” may be smarter than we think
- How to even reason about what could happen?

“Oops, we did it again.”

- De-identification (Sweeney’97)
- De-identification (Netflix, Narayanan-Shmatikov ‘06)
- De-identification (NYC Taxis'14)

…

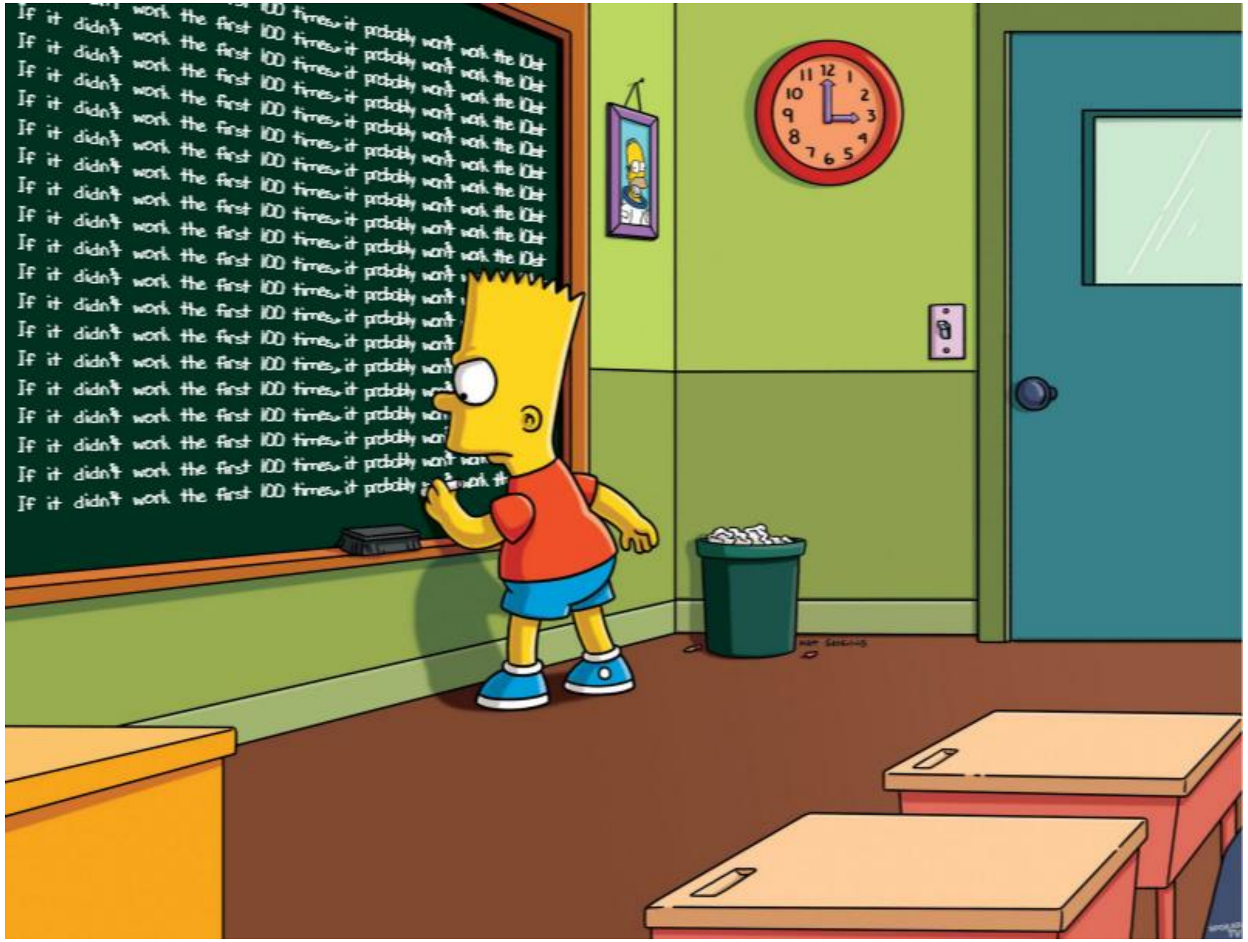
- De-identification (Medicare ‘16)
- De-identification (Victoria Myki ‘19)
- De-identification (coming soon in a place near you)

“We don’t need all that.”

- K-anonymity
- Data suppression
- Data swapping
- Synthetic data
- Legislate away
- “It looks good on my laptop”

“We don’t need all that.”

- K-anonymity
- Data suppression
- Data swapping
- Synthetic data
- Legislate away
- “It looks good on my laptop”


If it didn't work the first 100 times, it probably won't work the 101st

Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. 2017. “Exposed! A Survey of Attacks on Private Data.” Annual Review of Statistics and Its Application (2017). https://privacytools.seas.harvard.edu/publications/exposed-survey-attacks-private-data

Fundamental Law of Information Recovery

Fact. “Giving overly accurate answers to too many questions will inevitably destroy privacy.”

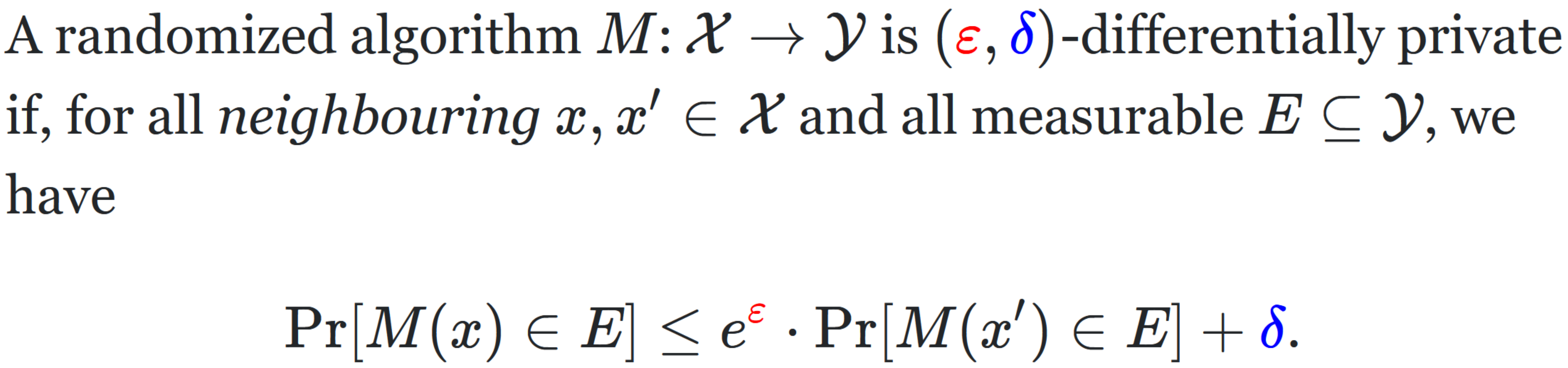
What do we want?

- Rigorous, worst-case* guarantees
  - "It looks good" is not enough
  - Cannot depend on assumptions on the data
- Future-proof guarantees
  - Whatever happens in the future, it won't leak more information
- Information-theoretic guarantees
  - A bit strange for a computer scientist, but… not computational!
- Composability
  - These are building blocks!
- Interpretability
  - What does it mean?

Differential Privacy

“What?”

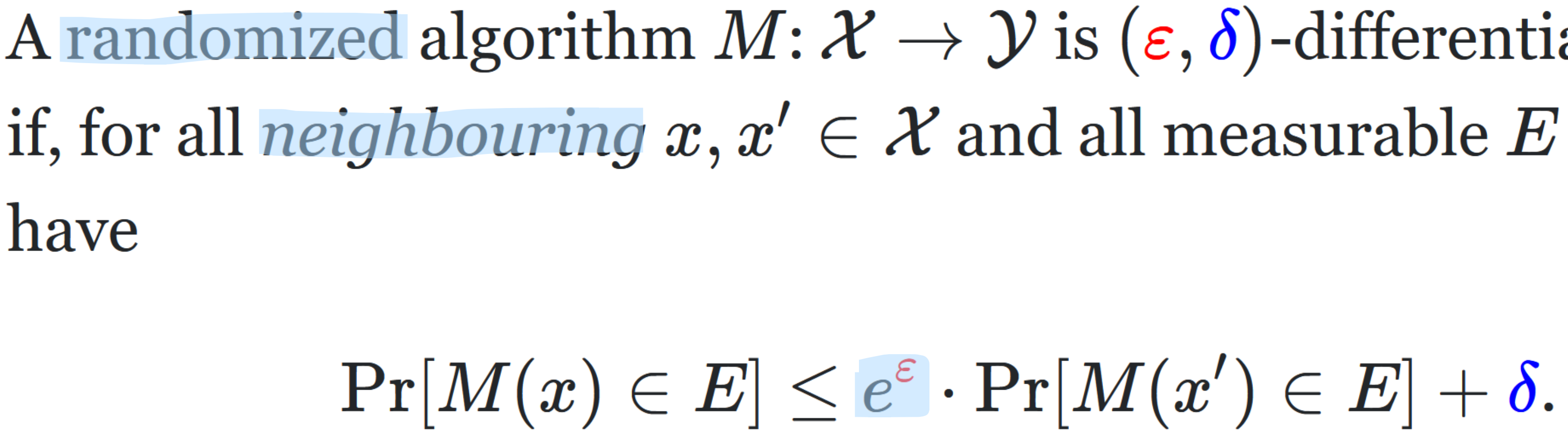
Differential Privacy (DMNS06)



A randomized algorithm $M\colon \mathcal{X} \to \mathcal{Y}$ is (ε, δ)-differentially private if, for all *neighbouring* $x, x' \in \mathcal{X}$ and all measurable $E \subseteq \mathcal{Y}$, we have

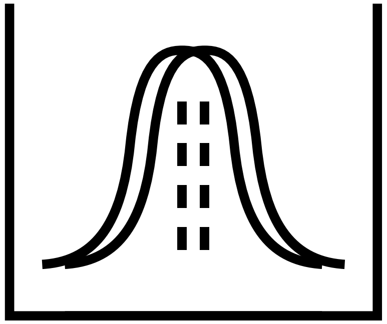
$$\Pr[M(x) \in E] \leq e^{\varepsilon} \cdot \Pr[M(x') \in E] + \delta.$$

Differential Privacy (DMNS06)



A randomized algorithm $M\colon \mathcal{X} \to \mathcal{Y}$ is (ε, δ)-differentially private if, for all *neighbouring* $x, x' \in \mathcal{X}$ and all measurable $E \subseteq \mathcal{Y}$, we have

$$\Pr[M(x) \in E] \leq e^{\varepsilon} \cdot \Pr[M(x') \in E] + \delta.$$



“Differential”

$q($

Name	Age	SSN
Doc	50	443667
Snow White	24	503935
Happy	89	748735
Grumpy	76	291711
Dopey	19	542494
Bashful	36	600430

$) \approx q($

Name	Age	SSN
Doc	50	443667
Snow White	24	503935
Gimli	154	698752
Grumpy	76	291711
Dopey	19	542494
Bashful	36	600430

$)$

Important:

Statistical inference is not a privacy violation

- Studies [in which Mr. X did not participate]: “Smoking causes cancer”
- Mr. X, 60 years old, has been smoking for 40 years
- Conclusion: Mr. X has an elevated risk of cancer

This conclusion [based on aggregate statistical patterns] does not violate Mr. X’s [individual] privacy!

Some comments and criticisms

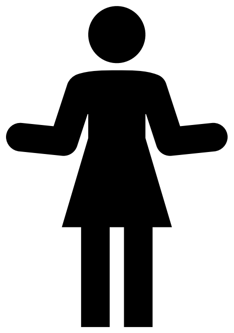
- Adding noise to the data?!
- The guarantees/parameters are hard to set or understand
- The threat model is overly pessimistic!
- This is overkill/unnecessary/impractical/unrealistic
- We have been doing fine for years without that
- We can’t afford the utility drop

“Privacy parameter?”

Two parameters: ε and δ. “The smaller, the better!”

What do they mean? How to choose them? How to compare them?

Is $\varepsilon=10$ “good”?



“Privacy parameter?”

Two parameters: ε and δ.

“It depends.”

“Privacy parameter?”

Two parameters: ε and δ.

(And they don’t necessarily give you the whole story.)

“Privacy parameter?”

Two parameters: ε and δ.

(And they don’t necessarily give you the whole story.)

Mechanism 1:
- Get a sensitive database D of 10,000 salaries
- Clamp the salaries, compute the mean
- Add carefully calibrated random (Gaussian) noise
- Publish the result to the world

Mechanism 2:
- Get a sensitive database D of 10,000 salaries
- Select at random 1 pair (salary, name)
- Publish that record to the world 💥

“Privacy parameter?”

Two parameters: ε and δ.

It’s also crucial to understand what is being promised here!

“Privacy parameter?”

Two parameters: ε and δ.

The DP definition promises a worst-case guarantee, the worst that could happen against an adversary who knows pretty much everything besides the sensitive data itself.

“Privacy parameter?”

Two parameters: ε and δ.

The DP definition promises a worst-case guarantee, the worst that could happen against an adversary who knows pretty much everything besides the sensitive data itself.

Side information? ✅

Computational resources? ✅

Arbitrary priors? ✅

“Privacy parameter?”

Two parameters: ε and δ.

The DP definition promises a worst-case guarantee, the worst that could happen against an adversary who knows pretty much everything besides the sensitive data itself.

This is what makes the DP guarantees composable and future-proof!

“Privacy parameter?”

Two parameters: ε and δ.

The DP definition promises a worst-case guarantee, the worst that could happen against an adversary who knows pretty much everything besides the sensitive data itself.

This is what makes the DP guarantees “conservative”

“Privacy parameter?”

- Strong guarantees, with a specific meaning
    - This meaning might not be what you think it is!
- Choosing parameters is a policy decision
    - … informed by theory and practice
- Large values of parameters might not be bad!
    - Or they might.
    - But they can only get better in the future!
- They seem opaque, but they allow one to transparently reason and account for privacy loss and budget

But… “How”?

Many techniques to achieve this:

- Carefully calibrated random noise
  - Laplace mechanism
  - Gaussian mechanism
  - Poisson mechanism
- You don’t have to implement it yourself! (OpenDP, TumultLabs…)
- …

Used in practice!

https://desfontain.es/privacy/real-world-differential-privacy.html

But… “How”?

Many techniques to achieve this:

- Carefully calibrated random noise
    - Laplace mechanism
    - Gaussian mechanism
    - Poisson mechanism
- You shouldn’t implement it yourself! (OpenDP, TumultLabs…)
- …

Used in practice!

https://desfontain.es/privacy/real-world-differential-privacy.html

Limitations: DP is not all you need

https://www.youtube.com/watch?v=6pDH66X3ClA

Limitations: DP is not all you need

- Secure and Multi Party Computation (MPC)
- Other principled approaches to data privacy
- Synthetic Data Generation (+DP?)
- Data retention laws and standards
- Education and data literacy

Limitations: DP is not all you need

- Comes at a (necessary) cost: do you need these guarantees?
- Does not address all threat models
- Complementary to cryptographic approaches. Not the same goal!
- Hard to interpret and set parameters
- Structured data is tricky

Key Takeaways:

Statistical inference is not a privacy violation

(If it is, DP will not help with it, and nothing else will)

The best way to protect privacy is not to collect data in the first place

If someone promises something too good to be true, chances are that it is

Choice of privacy parameters is a policy decision

Do not implement your own differential privacy pipeline from scratch

Thank you

Snow White and the Seven Dwarfs (1937)

Some resources and pointers

- https://differentialprivacy.org/resources/

  This website is intended to serve as a resource for the differential privacy research community, as well as for those seeking to learn more about the subject.

- https://opendp.org/

  OpenDP is a community effort to build trustworthy, open-source software tools for statistical analysis of sensitive private data.

- https://desfontain.es/privacy/friendly-intro-to-differential-privacy.html

  “A friendly, non-technical introduction to differential privacy”

- https://arxiv.org/abs/2303.00845

  21st Century Statistical Disclosure Limitation: Motivations and Challenges. John M. Abowd, Michael B. Hawes (In press, 2023)