

# CONNECT REIMAGINE

June 10 & 11, 2021 | Virtual Event

WOMEN WHO  
CODE

## Privacy-Preserving AI – Perform Data Science on Data You Cannot See

Technical Talk

Data Science

Zarreen Reza (she/her)

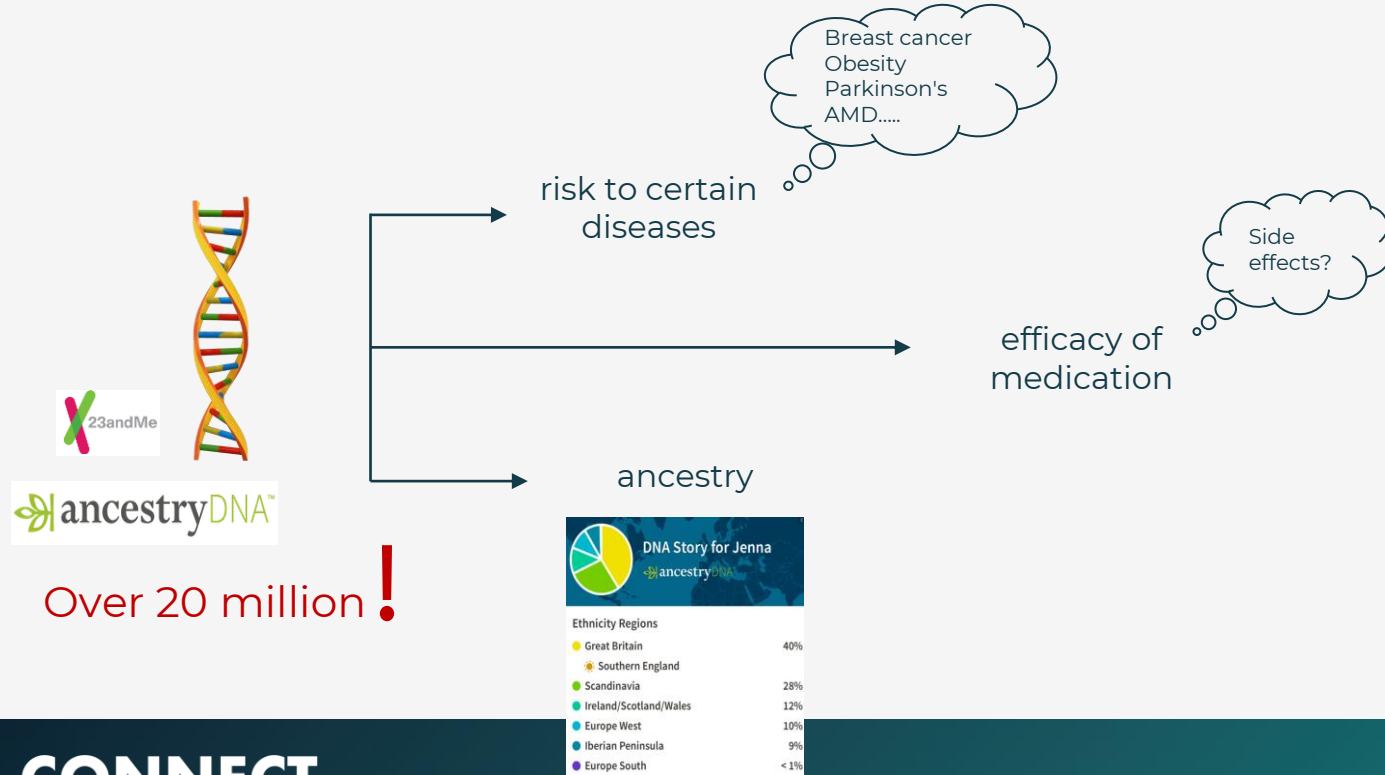
Data Scientist



# Outline

- Why should you care about privacy
- Privacy Preserving AI Tools
  - Federated Learning
  - Differential Privacy
  - Secure Multi-party Computation
- Where to go from here to get started

# Direct-to-consumer genetic testing

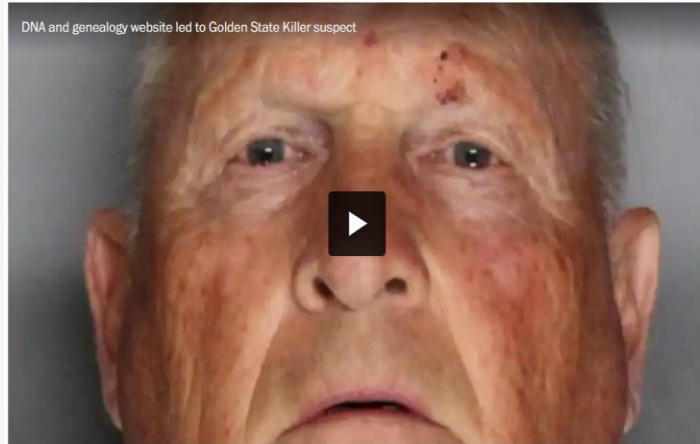


What else can be done with your DNA profile?

# DNA Forensics

True Crime

## The ingenious and 'dystopian' DNA technique police used to hunt the 'Golden State Killer' suspect



Police used DNA information on a genealogy website to track down the Golden State Killer suspect. (Reuters)

Police used DNA information on a genealogy website to track down the **Golden State Killer** suspect by matching the DNA found in crime scene with one of his distant family members, who uploaded his DNA profile to the genetic testing website.

# DNA Phenotyping

Things that can be inferred from  
your DNA profile

- Height
- Weight
- Body mass index
- Voice
- Age
- Sex
- Eye color
- Skin color

3D facial structure



Figure 1: Examples of real images on the left and their predicted DNA phenotyping reconstruction on the right (Lippert et al., 2017)

Source: [Identification of individuals by trait prediction using whole-genome sequencing data , Lippert et al., 2017](#)

Your data is your digital footprint....



@womenwhocode  
#WWCode

# What is a digital footprint?

- Your digital footprint refers to all the personal data and information available about you online.
- Your active digital footprint includes your emails, social media interactions, and other messages with your name attached.
- Your passive digital footprint is information you unintentionally leave behind, like your IP address, cookies, geolocation data when you use maps etc.



[Business Insider Intelligence](#)



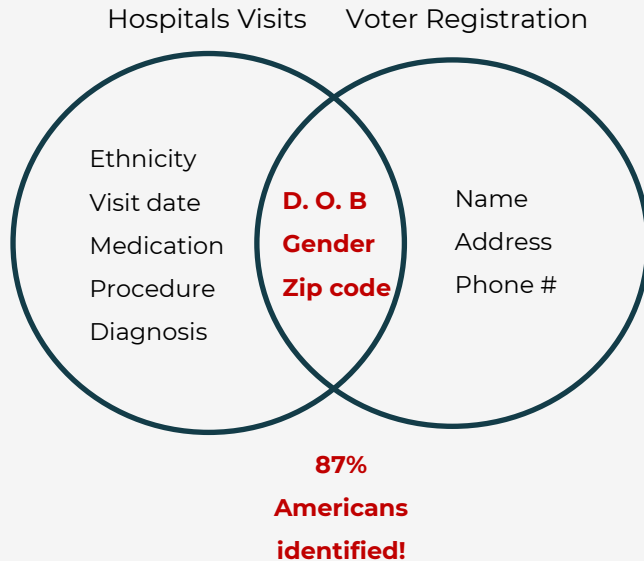
But these data are not private, why should I care?

# Companies do CARE

- We don't yet know how it can be used against us!
- What if our medical data ended up in the hands of health insurance companies that could misuse it to charge us accordingly?
- What if our DNA data gave away the possibility of developing a disability in future that would limit our access to the job market or to certain professions?
- What if instead of helping fight criminals, it creates discrimination or bias against a community, race or religion?

What if the dataset is made anonymous?

# Linkage Attack



**ars TECHNICA**    BIZ & IT    TECH    SCIENCE    **POLICY**    CARS    GAMING & CULTURE

POLICY —

## “Anonymized” data really isn’t—and here’s why not

Companies continue to store and sometimes release vast databases of “ ...

NATE ANDERSON - 9/8/2009, 7:25 AM

### Robust De-anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset)

Arvind Narayanan and Vitaly Shmatikov  
The University of Texas at Austin  
February 5, 2008

### MIT News

ON CAMPUS AND AROUND THE WORLD

#### The privacy risks of compiling mobility data

Merging different types of location-stamped data can make it easier to discern users’ identities, even when the data is anonymized.

Rob Matheson | MIT News Office  
December 7, 2018

### 'Anonymous' browsing data can be easily exposed, researchers reveal

A journalist and a data scientist secured data from three million users easily by creating a fake marketing company, and were able to de-anonymise many users

## Your Old Tweets Give Away More Location Data Than You Think

Researchers built a tool that can predict where you live and work, as well as other sensitive information, just by using geotagged tweets.

How can we ensure data privacy?  
How to build AI models using private data?

# Privacy Preserving AI

- The art of performing data science and build AI solutions by training or querying on data without the need to collect, distribute or even look at them.
- Tools
  - ✓ Federated Learning
  - ✓ Differential Privacy
  - ✓ Homomorphic Encryption
  - ✓ Secure multi-party computation (SMPC)

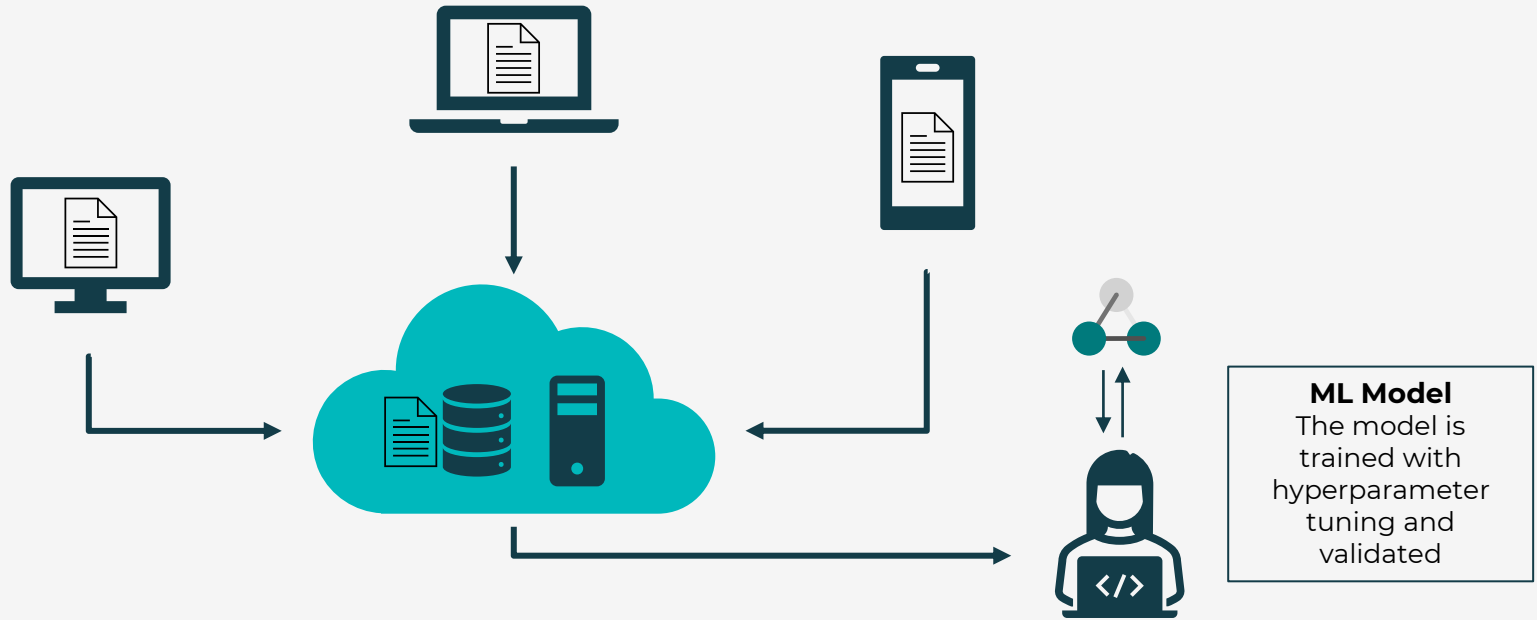
# Federated Learning

# Standard Machine Learning

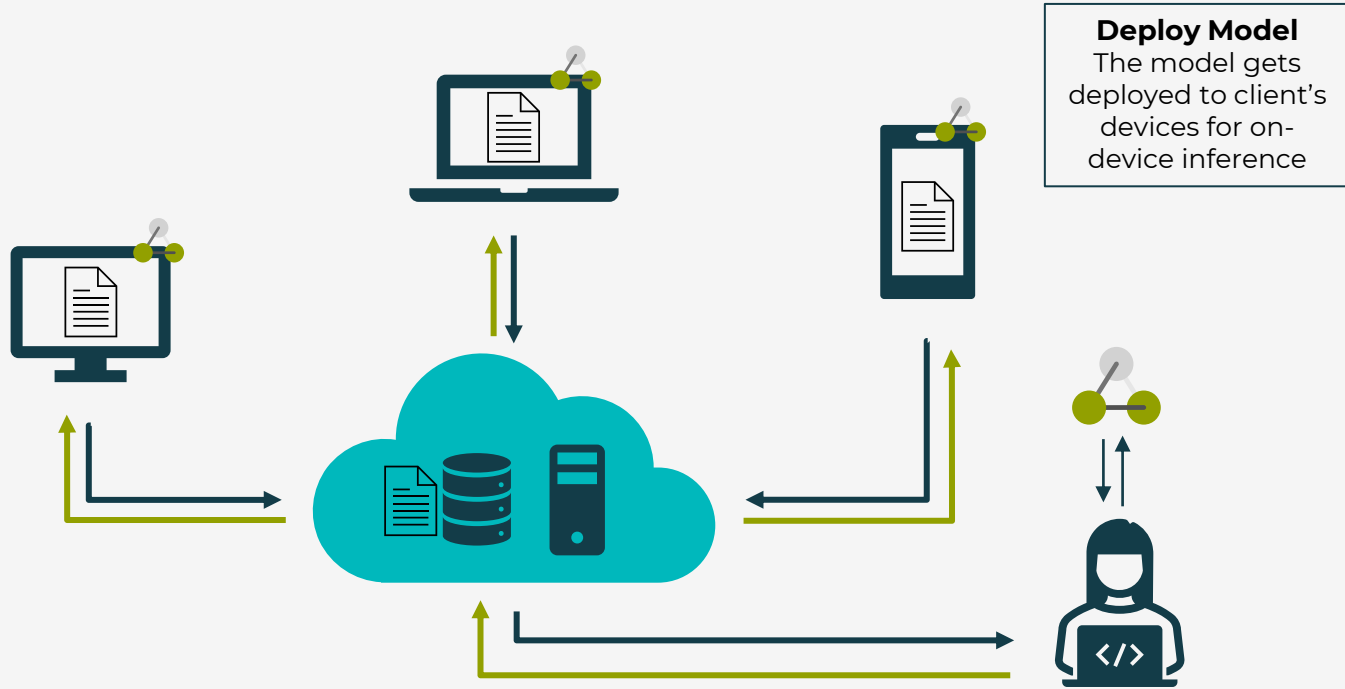




# Standard Machine Learning



# Standard Machine Learning



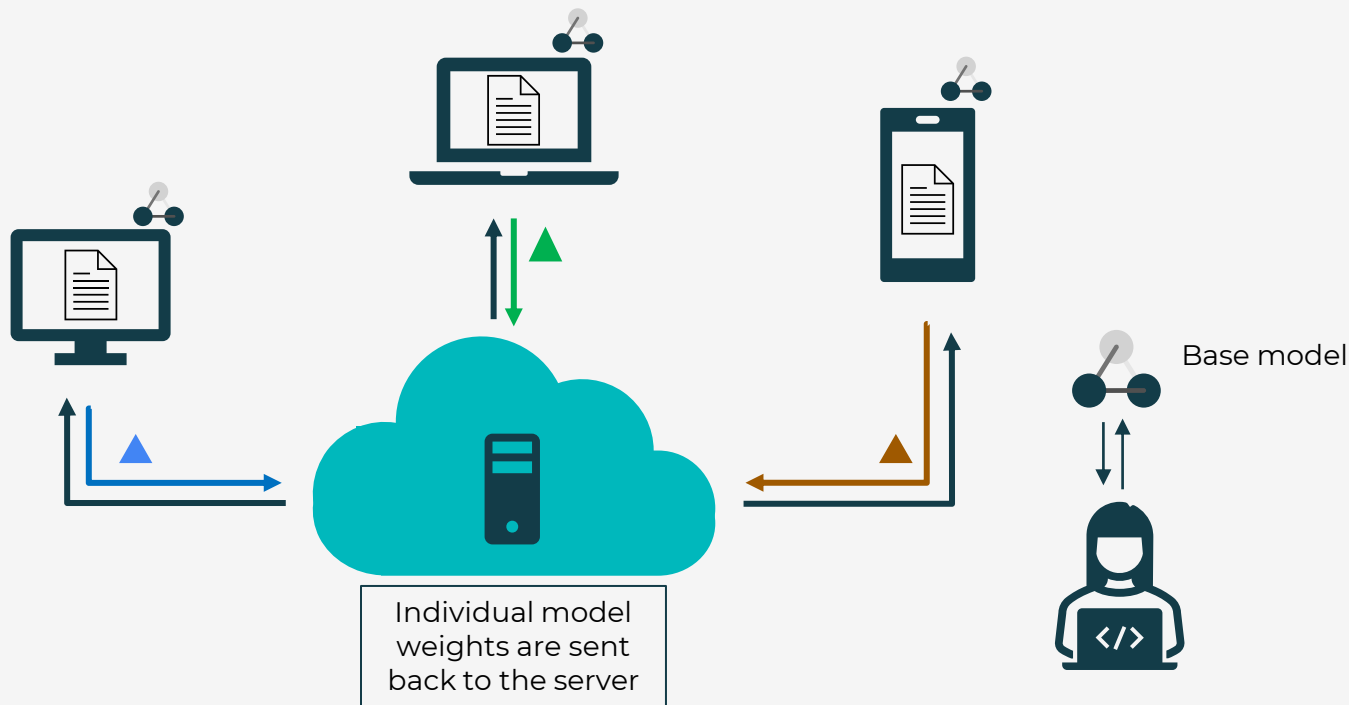
# Federated Learning

- Federated Learning is a set-up for training machine learning algorithms on data without the owner having to share, transfer or expose their data with the developer and the service provider.
- ✓ Cross-device Federated Learning
- ✓ Cross-silo Federated Learning

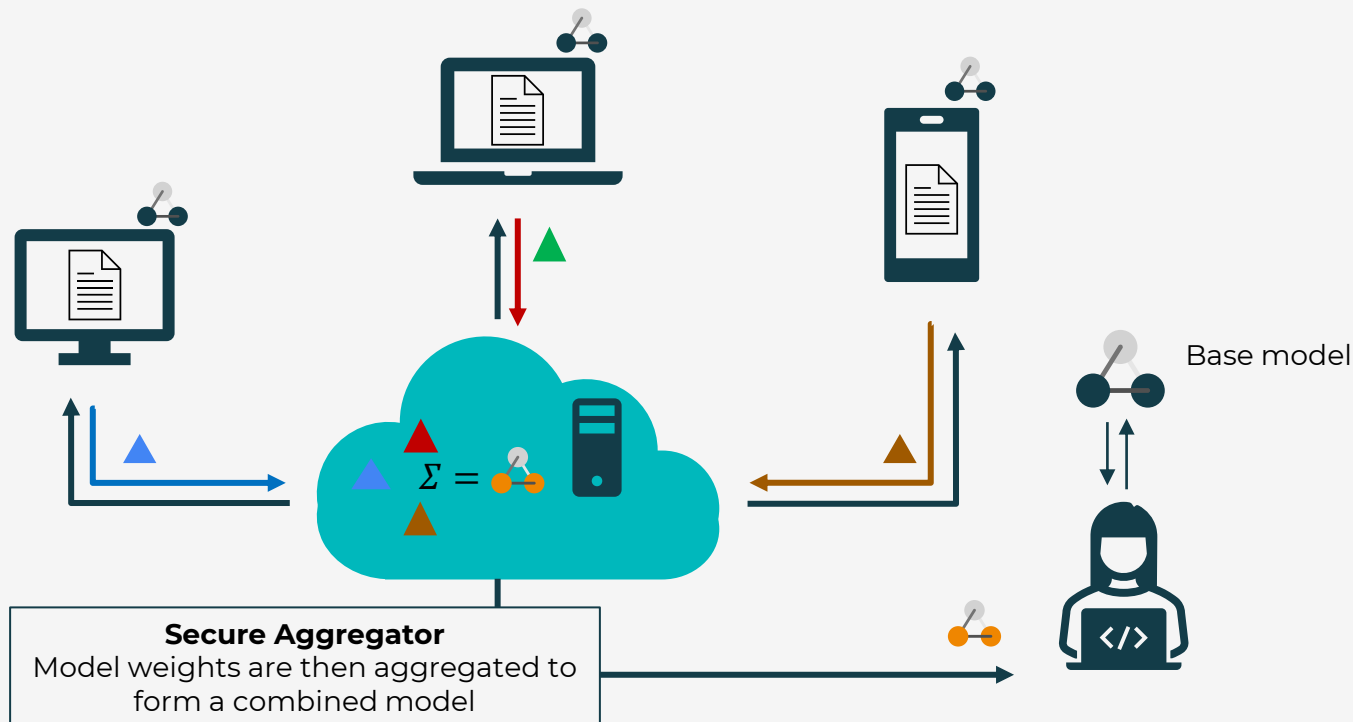
# Cross-device Federated Learning



# Cross-device Federated Learning



# Cross-device Federated Learning



# Cross-device Federated Learning



# Cross-device Federated Learning





# Cross-silo Federated Learning



# Cross-silo Federated Learning



# What about the model weights?

- Model weights can be reverse engineered to trace back to the data it was trained on.
- Models can memorize data and cause data leakage.
- Federated Learning on its own does not guarantee complete data privacy, needs to be incorporated with DP and/or SMPC.

# Differential Privacy

# Objective

“If I were to reveal this updated model to the data scientist, what’s the maximum amount of private information of the people in the dataset I may leak?”



Differential Privacy helps answer this question!

# Ensure privacy

D

Name	Age
Alice	30
Bob	32
⋮	⋮
Natalie	64
⋮	⋮
Veronica	41

“When querying database D, if I remove someone from the database, would the output of the query change?”

D'

Name	Age
Alice	30
<del>Bob</del>	<del>32</del>
⋮	⋮
Natalie	64
⋮	⋮
Veronica	41

$$f(D) == f(D') ?$$

# Ensure privacy

D

Name	Age
Alice	30
Bob	32
⋮	⋮
Natalie	64
⋮	⋮
Veronica	41

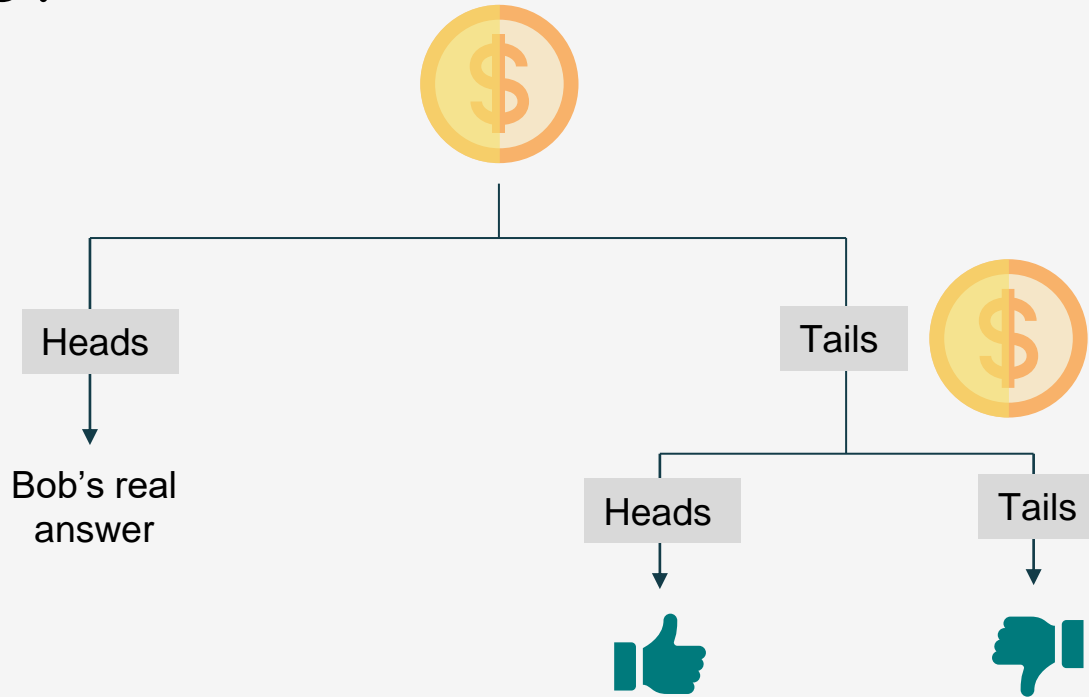
“When querying database D, if I remove someone from the database, would the output of the query change?”

- ✓ Privacy of each individual present in D is guaranteed to be ensured **IF**
- ✓ the output of a query to D is the same between this database D and any identical database D' with one row removed or replaced.

# “Do you smoke?”



Bob is  
asked to  
flip a coin

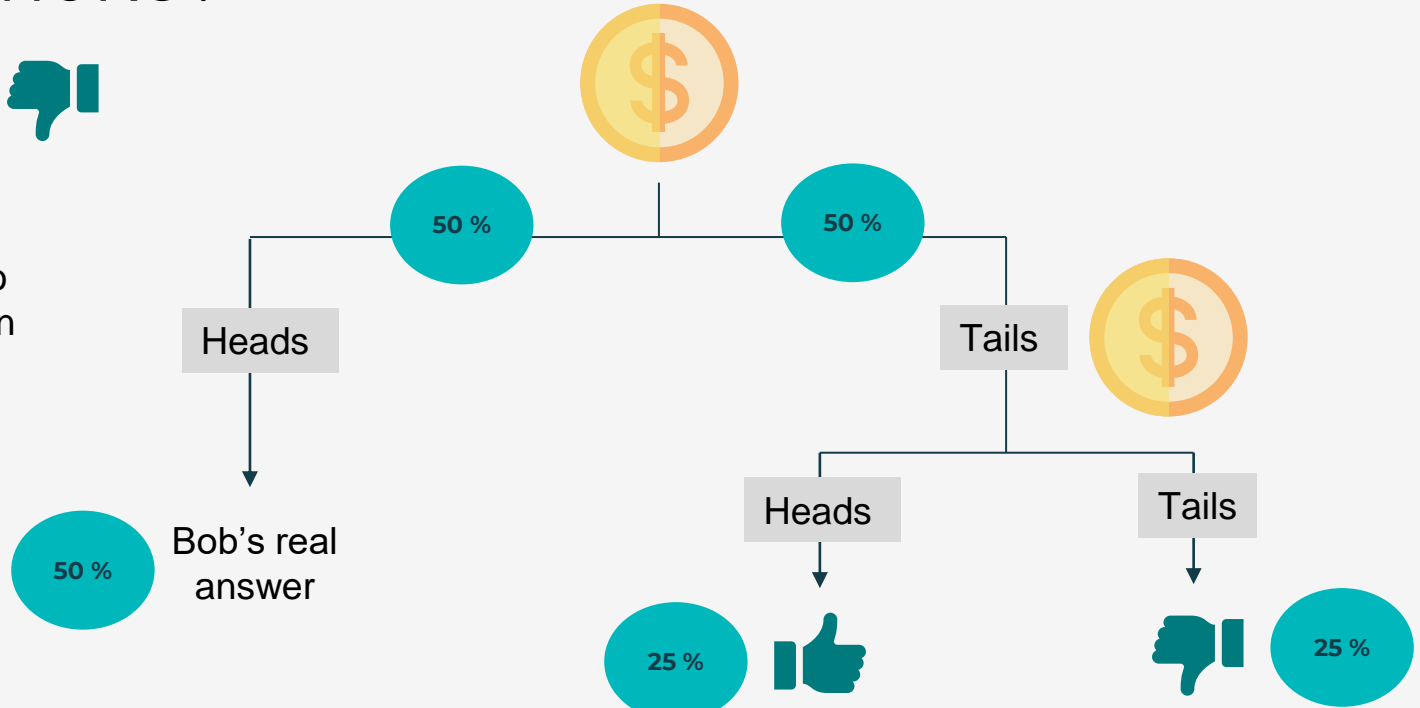




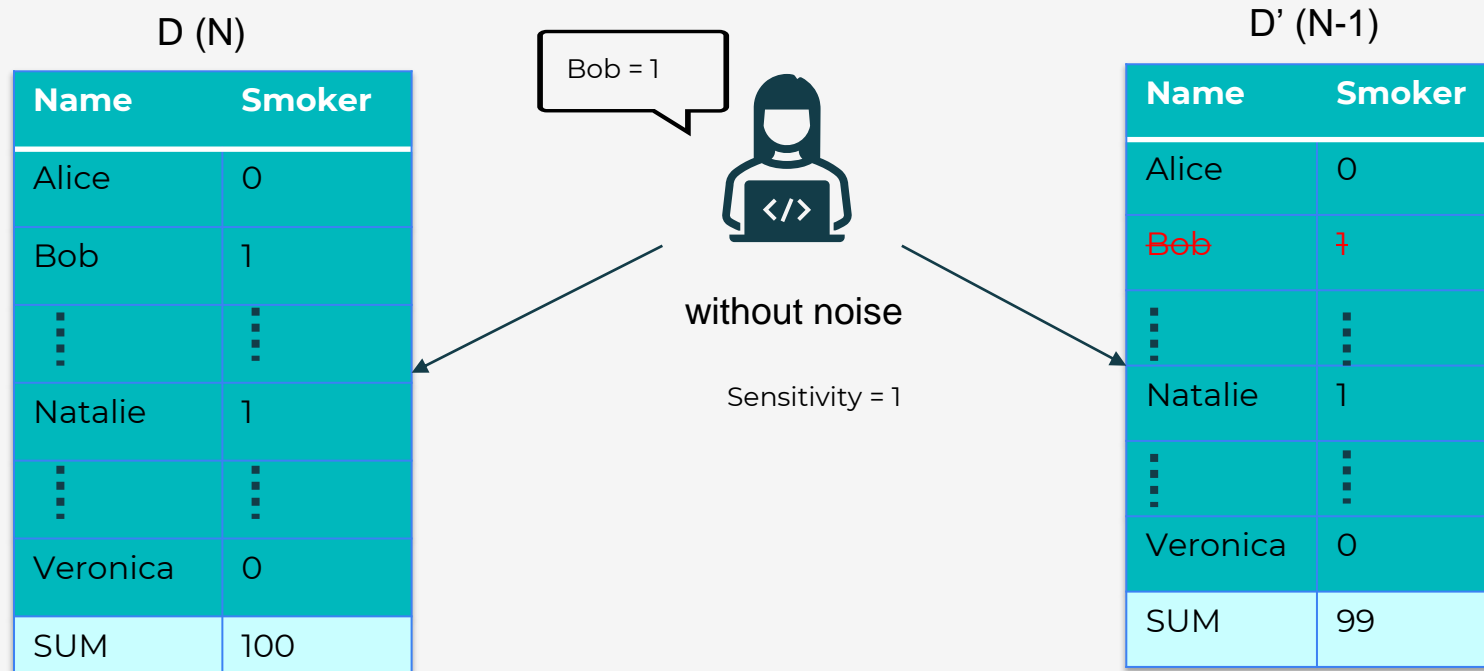
# “Do you smoke?”



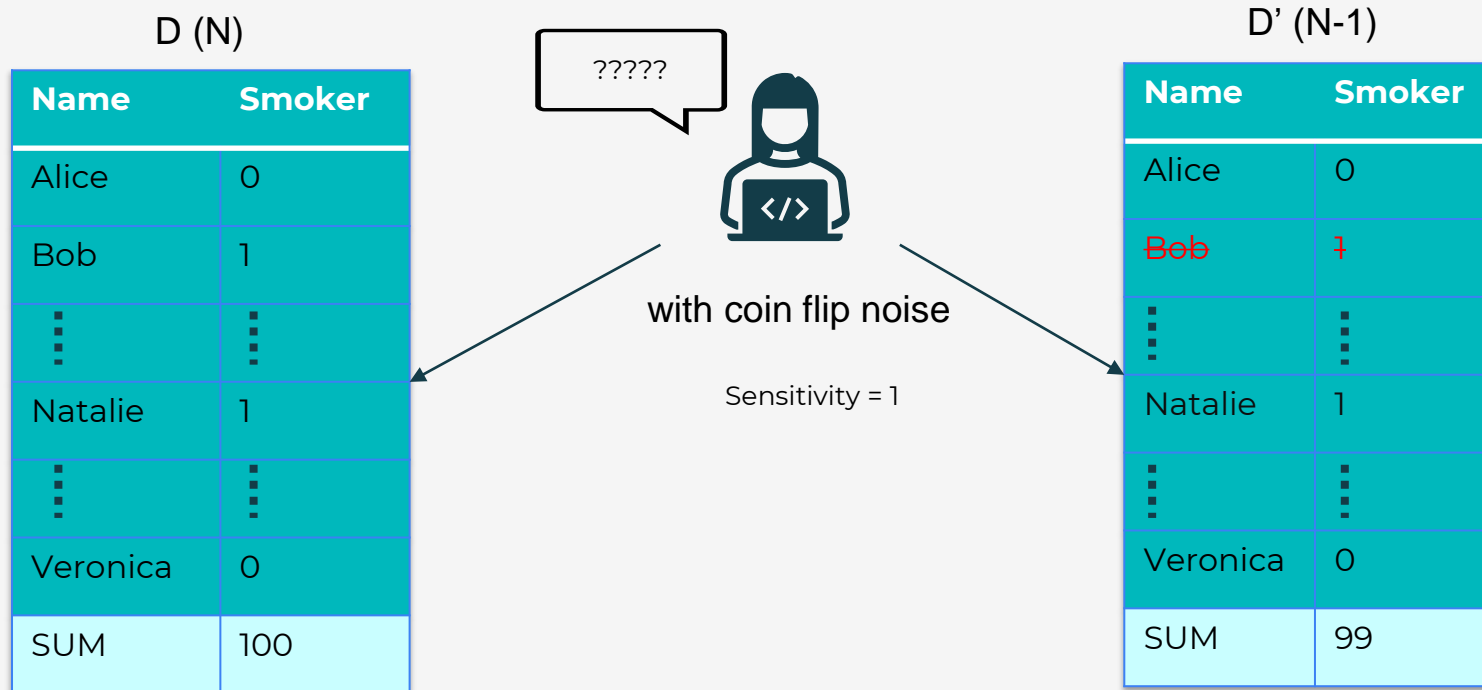
Bob is  
asked to  
flip a coin



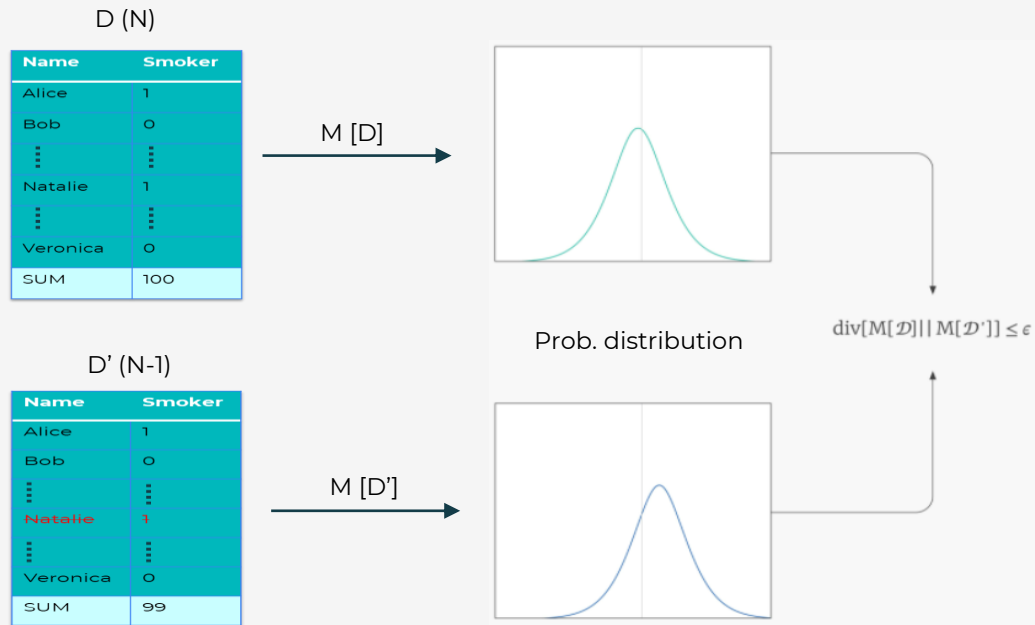
# Sum Query



# Sum Query



# Privacy Budget



M [•] = Randomized Mechanism

The mechanism is ε - differentially private if and only if

$$\text{div} [M[D] \parallel M[D']] \leq \epsilon$$

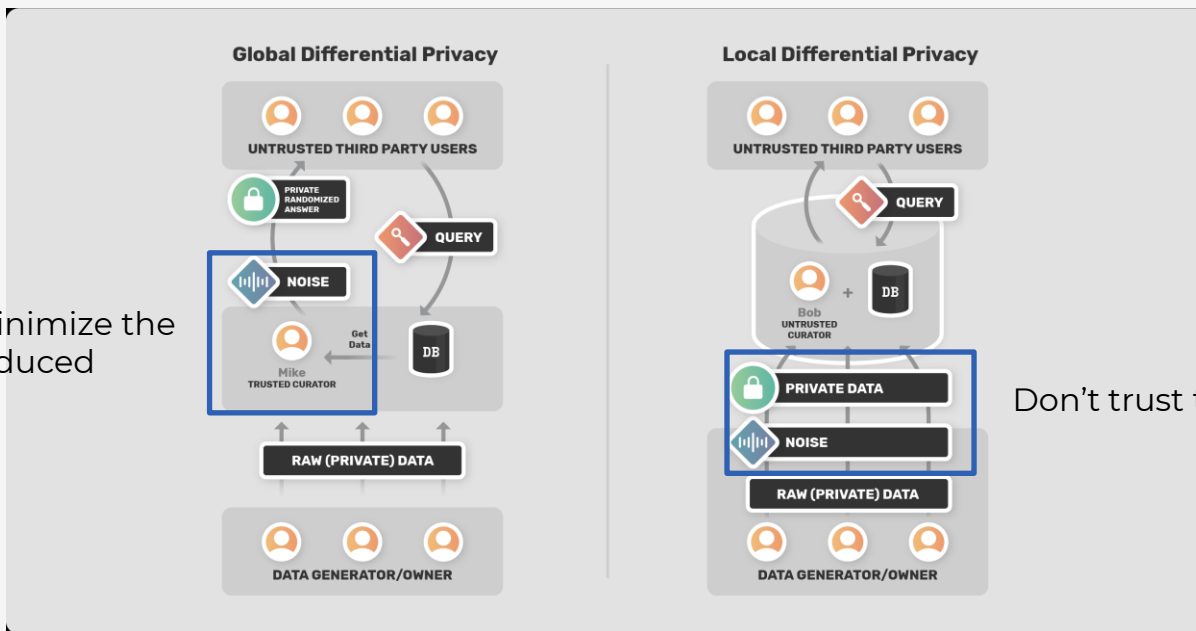
(Renyi divergence = a measure of the difference between probability distributions)

ε = privacy budget

= how large the divergence can be between the distributions

# Local DP and Global DP

Want to minimize the noise introduced

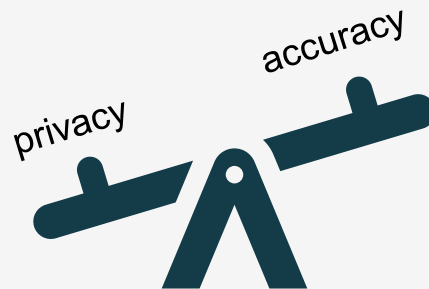


Don't trust the curator

<https://blog.openmined.org/basics-local-differential-privacy-vs-global-differential-privacy/>

# Noise Mechanisms

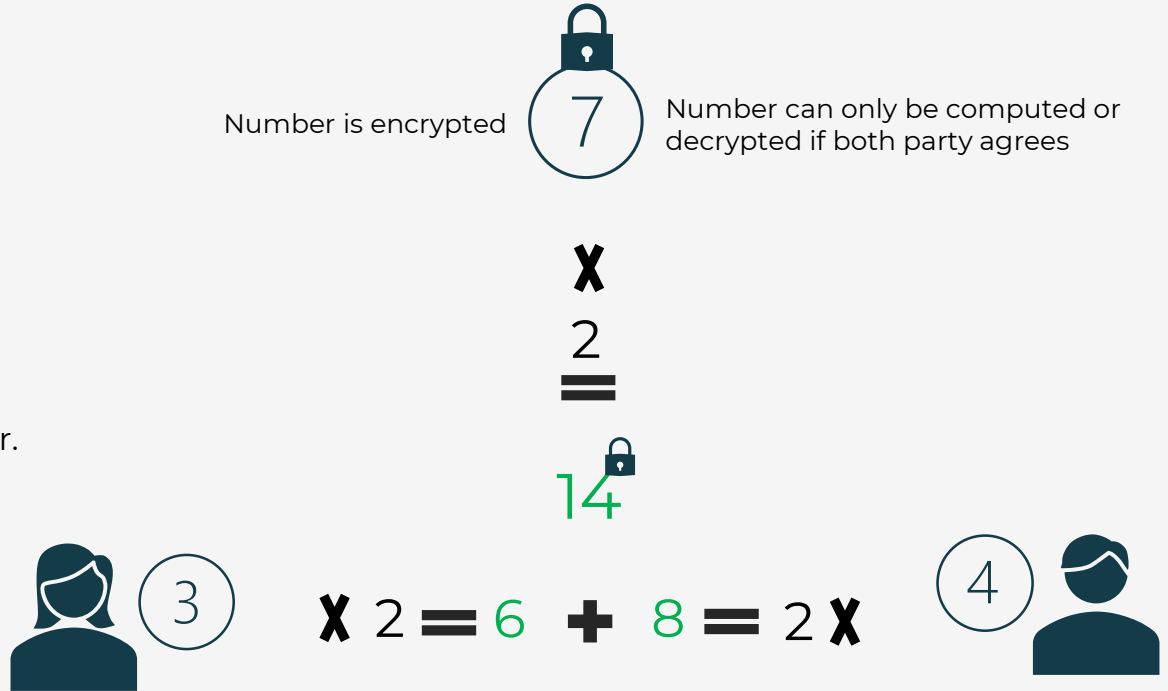
- ✓ Laplace Mechanism
- ✓ Exponential Mechanism
- ✓ Gaussian Mechanism



# Secure Multi-party Computation (SMPC)

# Definition

SMPC allows multiple people to combine their private inputs to compute a function, without revealing their inputs to each other.





# SMPC in AI

- Models and datasets are just large collections of numbers which can be encrypted and computed in that state.
- The data owner and model owner can make inference using encrypted model on encrypted data.
- Model weights can be securely aggregated during Federated Learning.

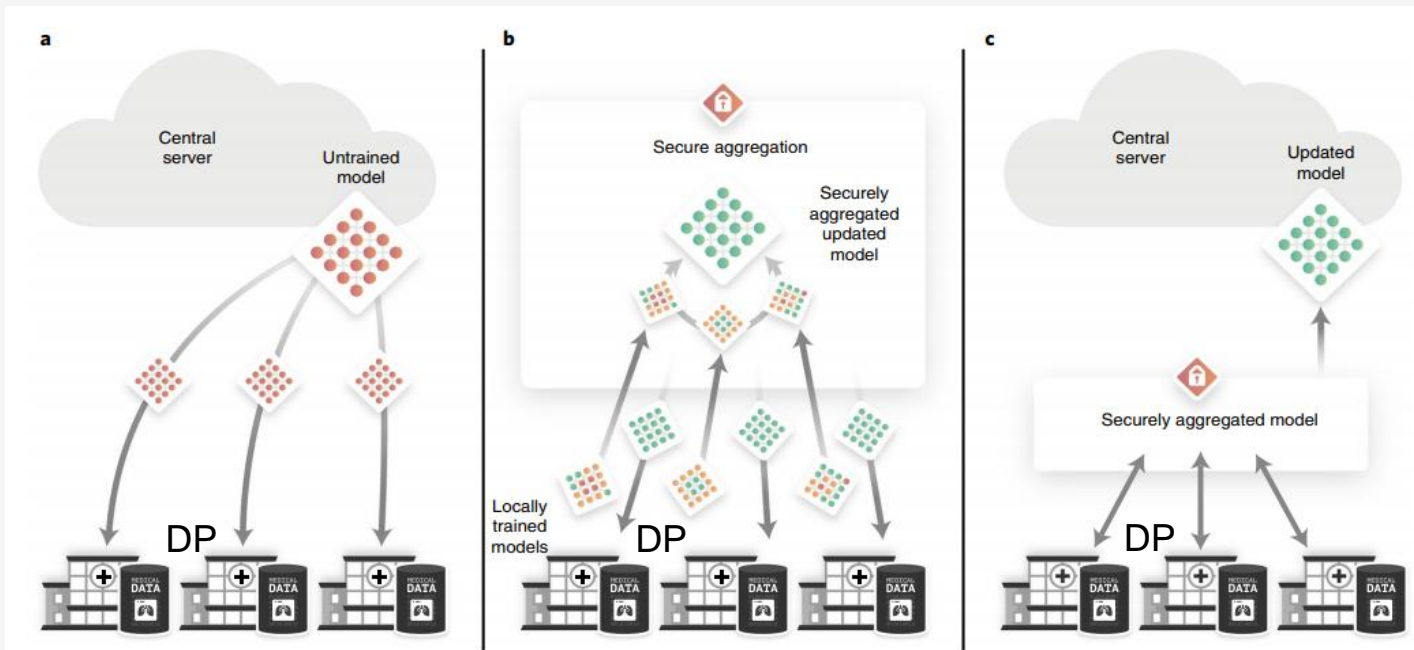
Let's tie all these together.....



@womenwhocode  
#WWCode

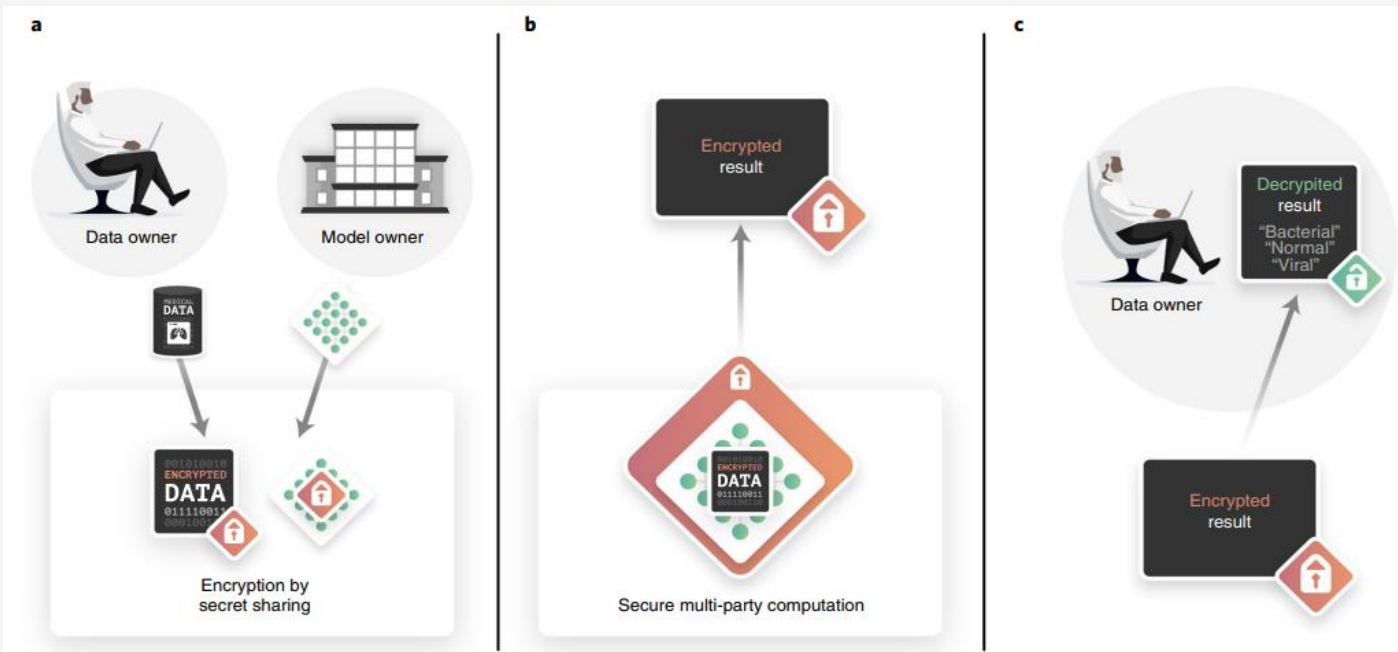
# End-to-end privacy preserving deep learning on multi-institutional medical imaging

Georgios Kaissis<sup>1,2,3,4,13</sup>, Alexander Ziller<sup>1,2,4,13</sup>, Jonathan Passerat-Palmbach<sup>3,4,5</sup>, Théo Ryffel<sup>4,6,7</sup>, Dmitrii Usynin<sup>1,2,3,4</sup>, Andrew Trask<sup>4,8</sup>, Ionésio Lima Jr<sup>4,9</sup>, Jason Mancuso<sup>4,10</sup>, Friederike Jungmann<sup>1</sup>, Marc-Matthias Steinborn<sup>11</sup>, Andreas Saleh<sup>11</sup>, Marcus Makowski<sup>1</sup>, Daniel Rueckert<sup>2,3</sup> and Rickmer Braren<sup>1,12,13</sup>



# End-to-end privacy preserving deep learning on multi-institutional medical imaging

Georgios Kaissis<sup>1,2,3,4,13</sup>, Alexander Ziller<sup>1,2,4,13</sup>, Jonathan Passerat-Palmbach<sup>3,4,5</sup>, Théo Ryffel<sup>4,6,7</sup>, Dmitrii Usynin<sup>1,2,3,4</sup>, Andrew Trask<sup>4,8</sup>, Ionésio Lima Jr<sup>4,9</sup>, Jason Mancuso<sup>4,10</sup>, Friederike Jungmann<sup>1</sup>, Marc-Matthias Steinborn<sup>11</sup>, Andreas Saleh<sup>11</sup>, Marcus Makowski<sup>1</sup>, Daniel Rueckert<sup>2,3</sup> and Rickmer Braren<sup>1,12,13</sup>




Where to go from here?



@womenwhocode  
#WWCode

# Resources

- Join OpenMined 
- Check out the course [Foundations of Private Computation](#)
- Tools and Libraries
  - ✓ PySyft
  - ✓ Deepee
  - ✓ OpenDP
  - ✓ Opacus
  - ✓ TenSEAL
  - ✓ Tensorflow Federated (TFF)



# thank you

for attending CONNECT REIMAGINE

WOMEN WHO  
**CODE**

# Contact me



@ZarreenNReza



<https://www.linkedin.com/in/zarreennreza/>



<https://ai-diary-by-znreza.com/>



znreza