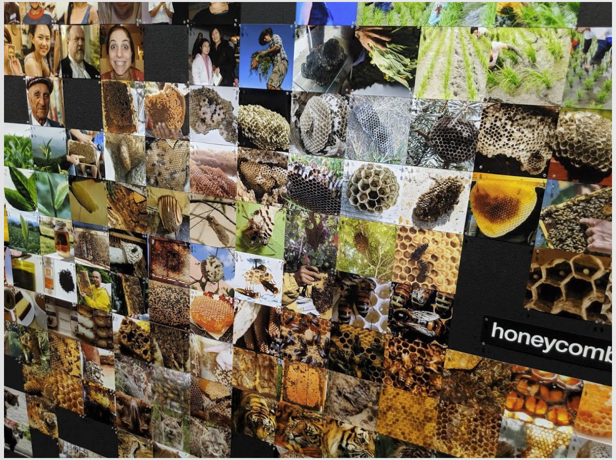
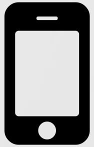
Privacy-preserving Machine Learning

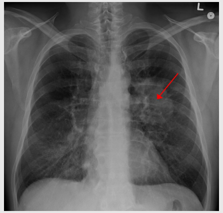
Michał Kuźba

Goal

- We want to respect people's privacy while using their data
- Dataset that really matter might have restricted access because of privacy, e.g. medical data, GDPR
- Ideally, we use data without seeing it :)
- We want to learn general patterns not individual data points anyway
- Now data is aggregated or removed after some time
- We would like to use Cloud services with our private data






https://www.cleanerblast.com/blog

(De)Anonymization?

How To Break Anonymity of the Netflix Prize Dataset

Arvind Narayanan, Vitaly Shmatikov

We present a new class of statistical de-anonymization attacks against high-dimensional micro-data, such as individual preference transaction records and so on. Our techniques are robust to perturbation in the data and tolerate some mistakes in the adversary' We apply our de-anonymization methodology to the Netflix Prize dataset, which contains anonymous movie ratings of 500,000 subscribers world's largest online movie rental service. We demonstrate that an adversary who knows only a little bit about an individual subscriber can easily identi this subscriber's record in the dataset. Using the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information.

Robust De-anonymization of Large Sparse Datasets

Arvind Narayanan and Vitaly Shmatikov
The University of Texas at Austin

Broken Promises of Privacy: Responding to Surprising Failure of Anonymization

UCLA Law Review, Vol. 57, p. 1701, 2010
U of Colorado Law Legal Studies Research Paper No. 9-12

77 Pages • Posted: 13 Jul 2012 • Last revised: 22 Feb 2015

Who's Watching?
De-anonymization of Netflix Reviews using Amazon Reviews

Maryam Archie, Sophie Gershon, Abigail Katcoff, and Aaron Zeng
{marchie, sgershon, akatcoff, a2z}@mit.edu

Revisiting the Uniqueness of Simple Demographics in the US Population

SZKOLENIA KONTAKT

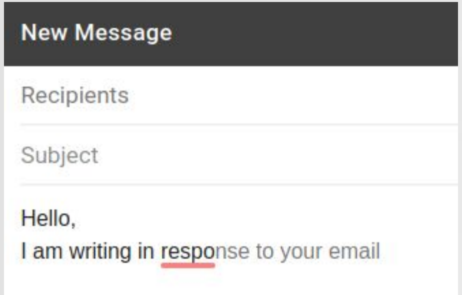
Zaufana Trzecia S

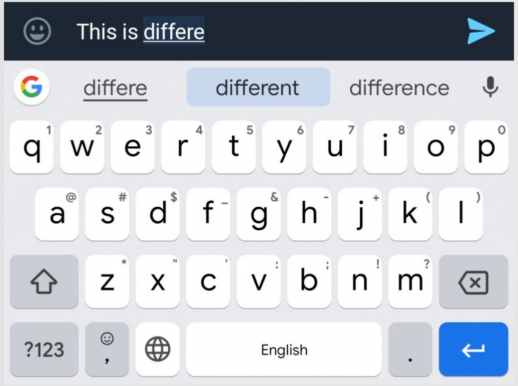
Dane o waszej lokalizacji są na sprzedaż.
Zanonimizowane, ale to nie przeszkadza

Topics

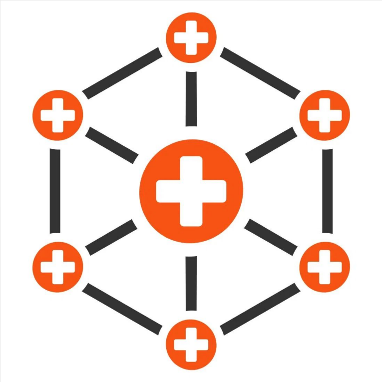
- Synthetic datasets
- Encryption
  - Encrypted Deep Learning
  - Data encryption
  - Homomorphic encryption
- Remote execution
  - Federated Learning
  - Secure Multi-Party Computation
- Differential Privacy
- Secure aggregation

Federated Learning - usecases



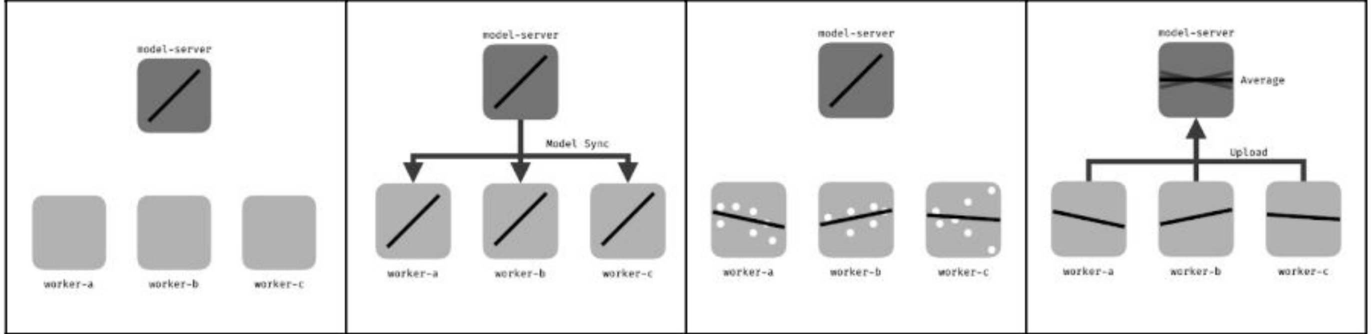


https://www.androidpolice.com/2019/05/10/gboard-8-2-improves-autocorrect-hints-apk-download/



https://lisabalboa.com/2017/10/15/network-level-strategies-for-tackling-the-deficit-of-nhs-hospitals/

Federated Learning



Step 1	Step 2	Step 3	Step 4
Central server chooses a statistical model to be trained	Central server transmits the initial model to several nodes	Nodes train the model locally with their own data	Central server pools model results and generate one global mode without accessing any data

https://en.wikipedia.org/wiki/Federated_learning

Federated Learning

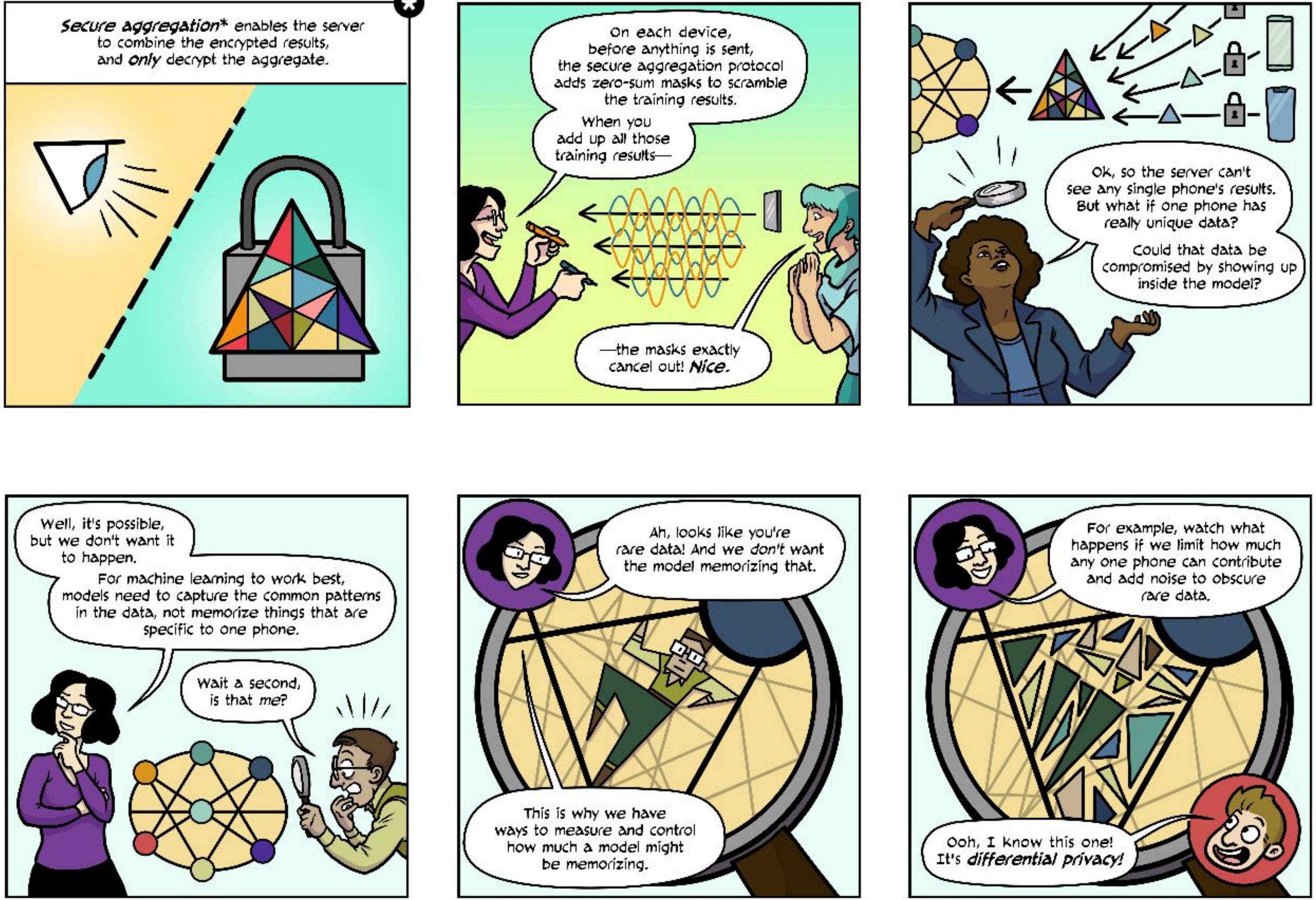
- Federated Learning vs Distributed Learning
- Pass gradients or weights
- Learning rounds
- Personalized learning - share some layers

Problems:

- Heavily correlated data - coming from one device
- Different size of datasets
- Temporal (time) heterogeneity
- Model size limitations, battery and network usage
- Fault tolerations
- Lack of understanding the training data (biases, no explainability, difficult to analyze data)
- Federated Learning leaks information by itself, is not secure (might memorize the data) - we need something more!

Federated Learning frameworks

- TFF - Tensorflow Federated
  - Allows also to make non-learning computations such as aggregated analytics
  - Tensorflow
- PySyft
  - PyTorch
  - Pointers to tensors
  - Remote execution



https://federated.withgoogle.com/

Differential Privacy

- Learn about patterns and groups and not disclose information about individuals
- Algorithm is differentially private if an observer seeing its output cannot tell if a particular individual's information was used in the computation

- Toss a coin
- If heads, then toss the coin again (ignoring the outcome), and answer the question honestly.
- If tails, then toss the coin again and answer "Yes" if heads, "No" if tails.

- Local vs global noise on the query
- Accuracy decreases
- Data-hungry, the more data the more privacy and less noise
- Ensembling example

Name	Has Diabetes (X)
Ross	1
Monica	1
Joey	0
Phoebe	0
Chandler	1
Rachel	0

https://en.wikipedia.org/wiki/Differential_privacy

Differential Privacy

- We don’t want the model to memorize data, that could be later reverse-engineered
- DP on neural net’s weights or input might not be a good idea
- Tensorflow Privacy, e.g. Differentially Private SGD (clipping, noising)

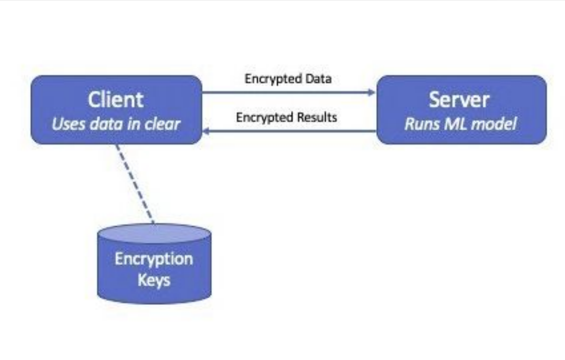
```
optimizer = optimizers.dp_optimizer.DPGradientDescentGaussianOptimizer(
    l2_norm_clip=FLAGS.l2_norm_clip,
    noise_multiplier=FLAGS.noise_multiplier,
    num_microbatches=FLAGS.microbatches,
    learning_rate=FLAGS.learning_rate,
    population_size=60000)
train_op = optimizer.minimize(loss=vector_loss)
```

https://www.youtube.com/watch?v=fCxp_lHo5ek

Some adoption:

- Telemetry, statistics at Apple, Microsoft, Google, LinkedIn

Homomorphic encryption



https://medium.com/blueprint-by-intuit/machine-learning-on-encrypted-data-no-longer-a-fantasy-58e37e9f31d7

$Enc(a + b) = Enc(a) \oplus Enc(b)$ and

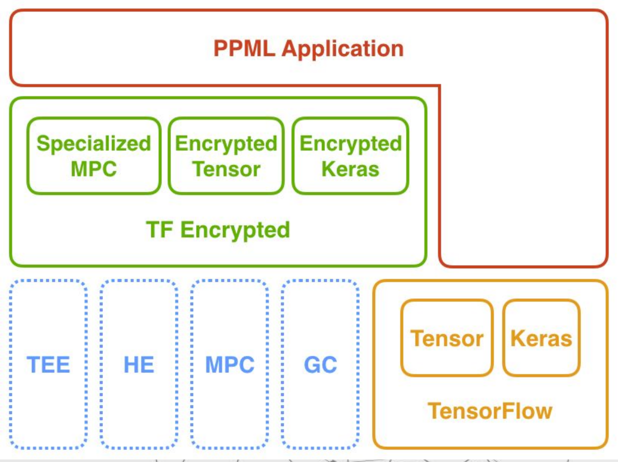
$Enc(a * b) = Enc(a) \otimes Enc(b)$

In other words, while performing any operations on data encrypted using a traditional cipher would result in gibberish, homomorphic encryption allows you to do it without corrupting the data. This goes further than basic operations. Being able to perform addition and multiplication also means that you can compute polynomials. And, with polynomials you can approximate essentially any function.

Homomorphic Encryption

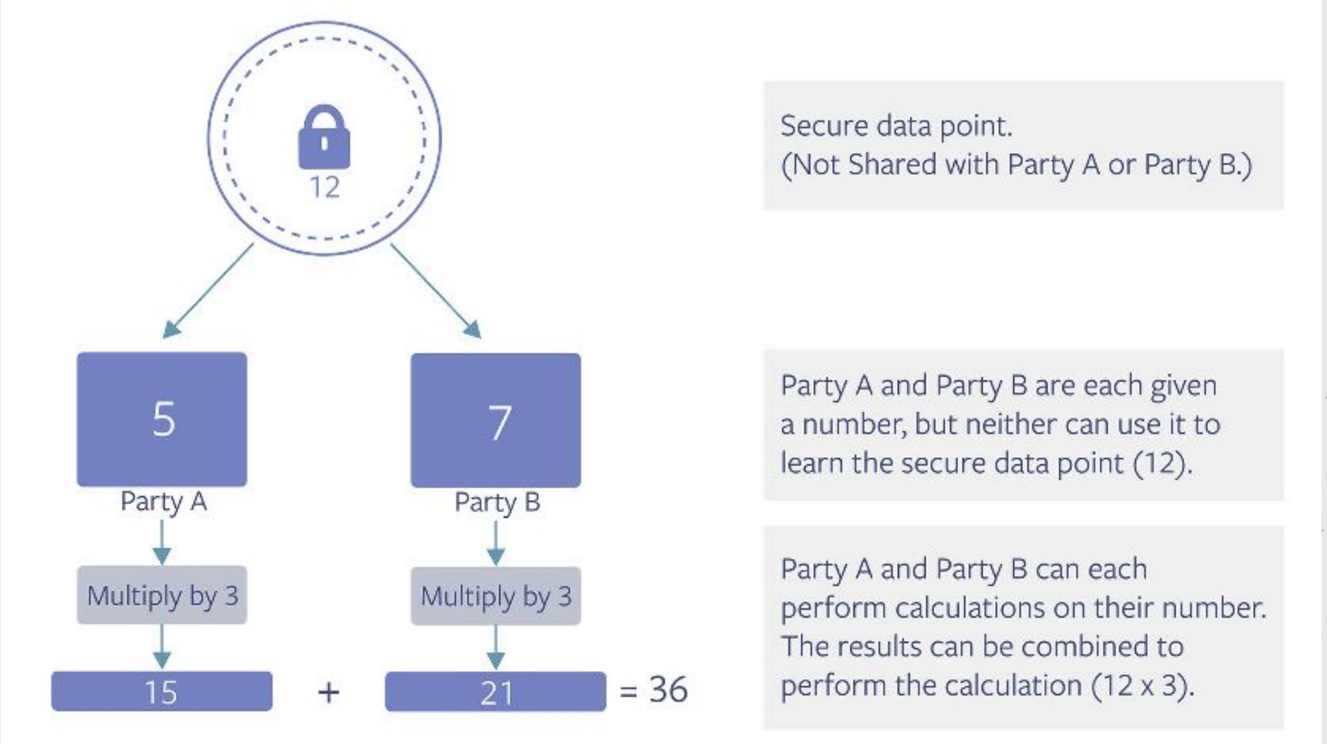
- Partial, Full HE
- Neural nets - cryptonets
- Performance downgrades for several reasons (sparsity, length, approximation, some noise
- y is 1 if x>T, otherwise y is 0
    - The function is approximated by a polynomial which in turn can be computed homomorphically. This becomes a building block in the homomorphic evaluation of the decision tree, as the tree is a sequence of conditional ("if") statements.

- Ciphertext's size might explode
- Frameworks:
    - Microsoft SEAL
    - Tensorflow Encrypted
    - Facebook Crypten



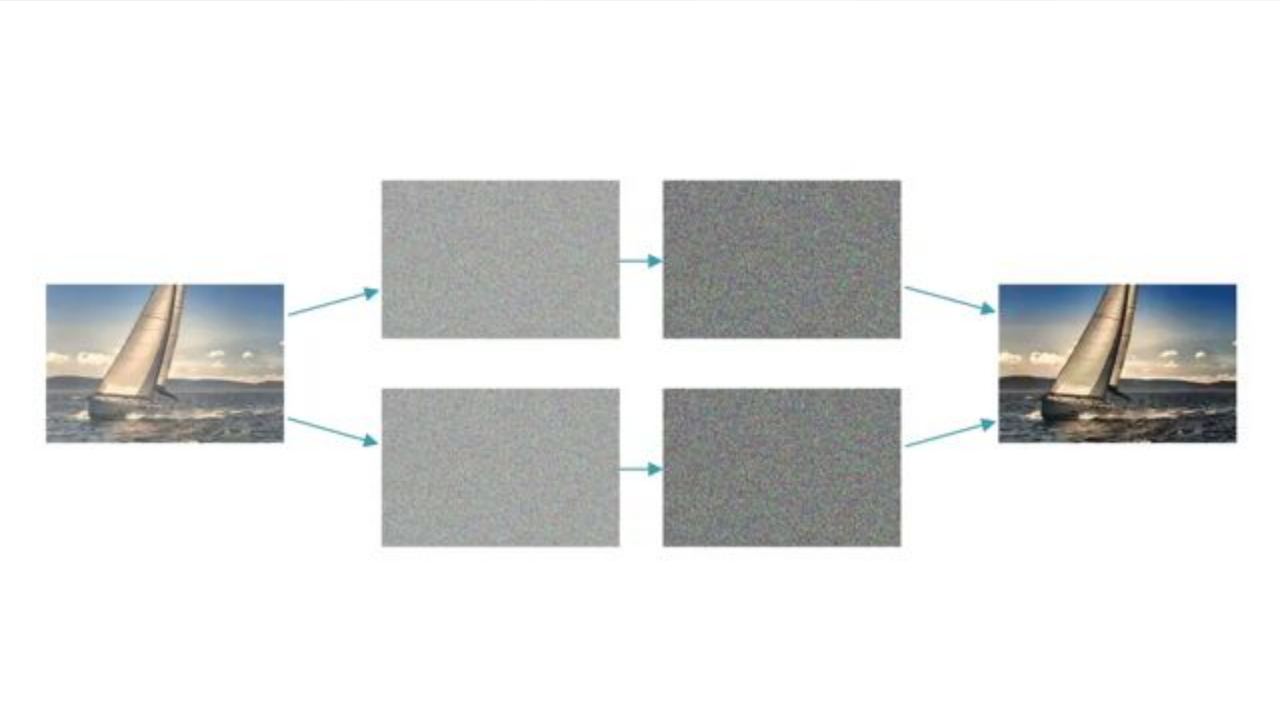
https://github.com/tf-encrypted/tf-encrypted

Secure Multi-Party Computation



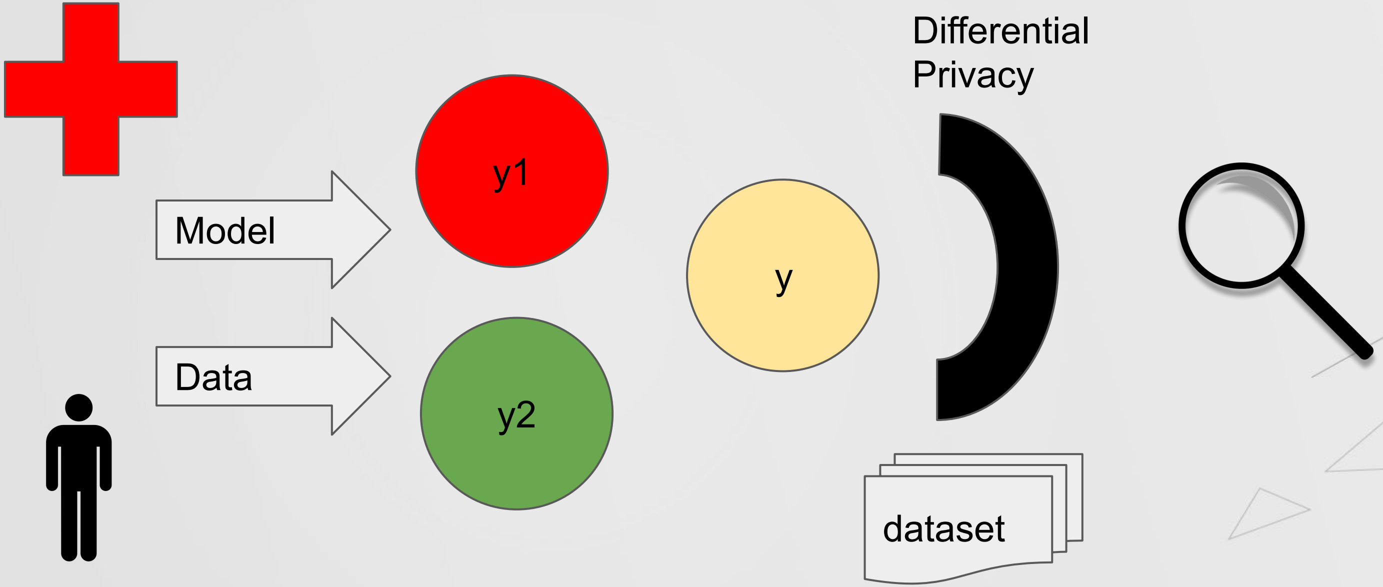
https://ai.facebook.com/blog/crypten-a-new-research-tool-for-secure-machine-learning-with-pytorch/

Secure Multi-Party Computation



https://ai.facebook.com/blog/crypten-a-new-research-tool-for-secure-machine-learning-with-pytorch/

Secure Multi-Party Computation



Synthetic datasets

- How to do it well?
  - Preserve statistical properties
  - Remove personal information
- Fraud detection
- Keep some original data for sanity check
- https://www.kaggle.com/mlg-ulb/creditcardfraud - PCA features
- Generating differentially private datasets using GANs

Resources

- https://www.udacity.com/course/secure-and-private-ai--ud185
- https://github.com/OpenMined/PySyft
- https://www.youtube.com/watch?v=4zrU54VIK6k - Andrew Trask, Lex Fridman
- https://medium.com/blueprint-by-intuit/machine-learning-on-encrypted-data-no-longer-a-fantasy-58e37e9f31d7

- Workshop Nips '19

THANKS