Foundations of Data Privacy

Devansh Gupta

Why Privacy Matters

- Organizations collect vast amounts of personal data: health, finance, location, online activity $\Longrightarrow$ important to preserve privacy of individual data
- Anonymized datasets can be re-identified

Anonymity and the Netflix Dataset

Last year, Netflix published 10 million movie rankings by 500,000 customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using. The data was anonymized by removing personal details and replacing names with random numbers, to protect the privacy of the recommenders.

Arvind Narayanan and Vitaly Shmatikov, researchers at the University of Texas at Austin, de-anonymized some of the Netflix data by comparing rankings and timestamps with public information in the Internet Movie Database, or IMDb.

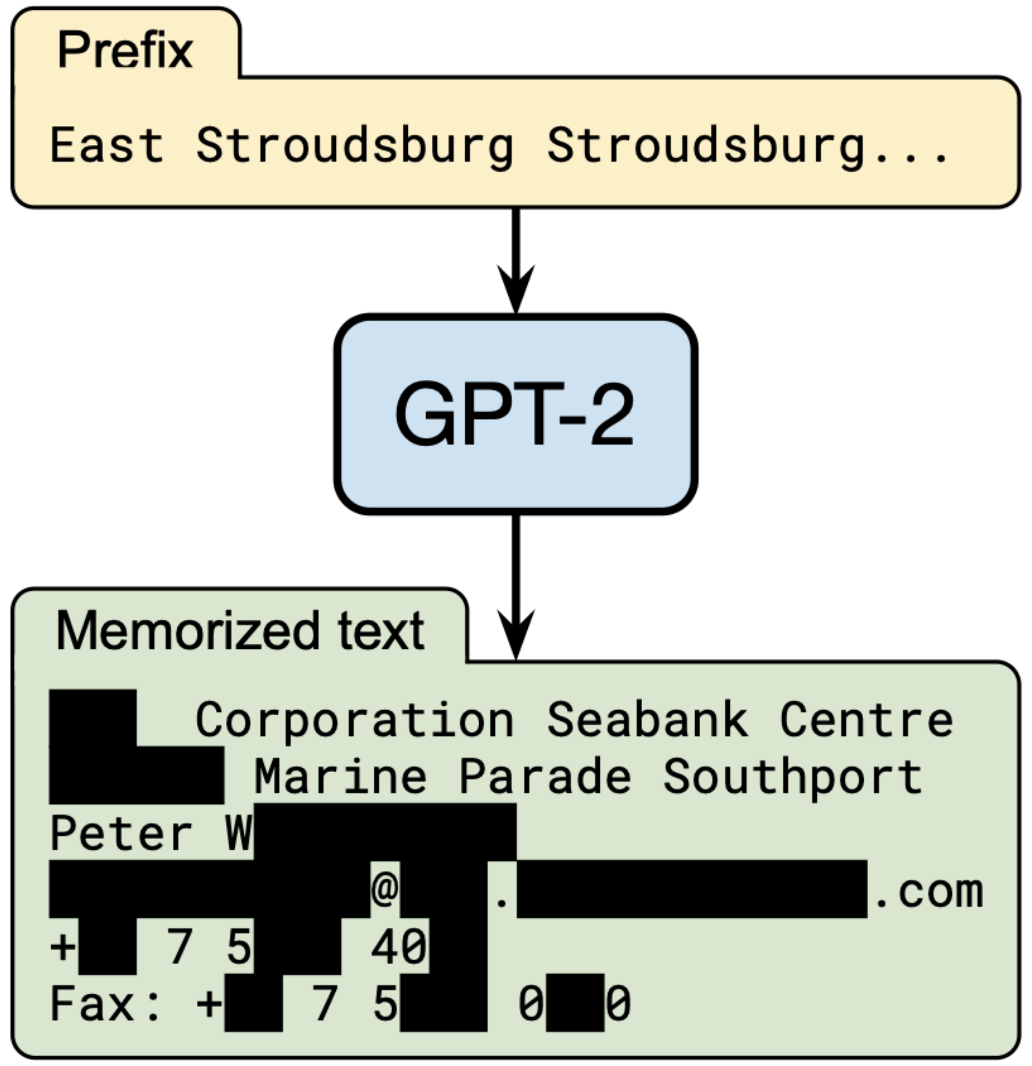
https://www.schneier.com/blog/archives/2007/12/anonymity_and_t_2.html

Why Privacy Matters

- In machine learning, large language models (LLMs) can leak private data

Extracting Training Data from Large Language Models

Nicholas Carlini[1] Florian Tramèr[2] Eric Wallace[3] Matthew Jagielski[4]
Ariel Herbert-Voss[5,6] Katherine Lee[1] Adam Roberts[1] Tom Brown[5]
Dawn Song[3] Úlfar Erlingsson[7] Alina Oprea[4] Colin Raffel[1]



- Data privacy laws like General Data Protection Regulation and California Consumer Protection Act mandate privacy of individual data

Carlini, N., Tramèr, F., Wallace, E., Jagielski, M., Herbert-Voss, A., Lee, K., … Raffel, C. (2021, August). Extracting Training Data from Large Language Models. 30th USENIX Security Symposium (USENIX Security 21), 2633–2650. Retrieved from https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting

Building Towards a Definition of Privacy

- How can one learn about population of data whilst preserving individual level privacy?
- Thought experiments:
    - If we take a lot of individuals and release a statistic, then the influence of one person's data becomes considerably low $\implies$ data privacy is inherent when population is high?
    - NO! Consider the following scenario…

Building Towards a Definition of Privacy

<u>Data Curator</u>

$x_1, x_2, \cdots x_n$

<u>Adversary</u>

How many points do you have?

n

Give me the mean of those points

m_1

Remove any one point and return the mean again

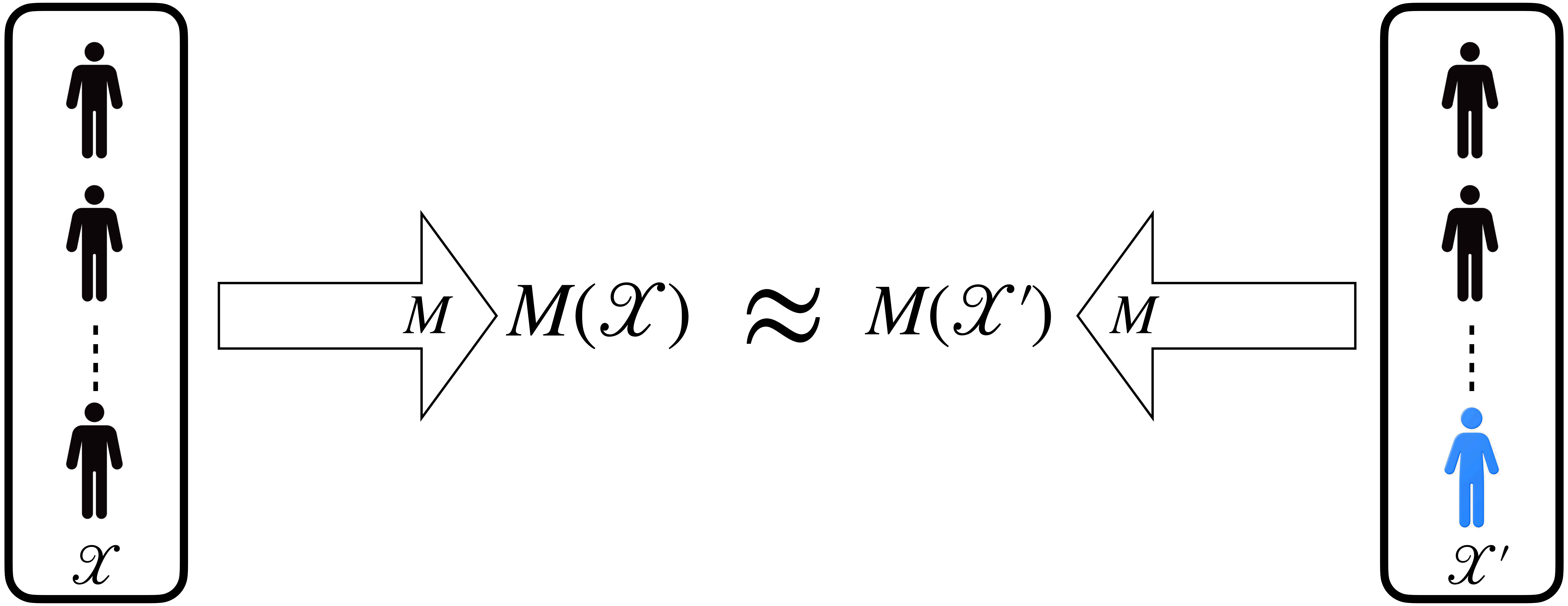
m_2

One of your points is $nm_1 - (n-1)m_2$

Building Towards a Definition of Privacy

- How can one learn about population of data whilst preserving individual level privacy?
- Thought experiments:
    - If we take a lot of individuals and release a statistic, then the influence of one person's data becomes considerably low $\implies$ data privacy is inherent when population is high?
    - NO! Consider mean of n data points…
- <u>**Goal:**</u> Ensure that the output of an analysis does not noticeably change whether any one person's data is included or not.

Differential Privacy



- A randomized algorithm M is (ϵ, δ) **differentially private** if for every databases $\mathscr{X}$ and $\mathscr{X}'$ which differ by one entry ($\mathscr{X} \sim \mathscr{X}'$) and all $S \subseteq Range(M)$

$$Pr[M(\mathscr{X}) \in S] \leq e^{\epsilon} Pr[M(\mathscr{X}') \in S] + \delta$$

Cynthia Dwork and Aaron Roth (2014), "The Algorithmic Foundations of Differential Privacy"

Differential Privacy: Some Features

- **<u>In simple terms:</u>** Your data does not have a significant influence on the distribution of the result.
- ε (epsilon): Privacy loss. Smaller is better
- δ (delta): Probability of a "failure" of privacy
- It is immune to any kind of data independent post processing
- Can be achieved by adding a carefully decided amount of noise?
  - In the mean example, if the curator simply adds some zero mean Gaussian noise to its answers $\Longrightarrow$ much much tougher for the adversary to guess the exact number

Real World Applications and Deployments

- **US Census:** DP is used in releasing Census data
- **Apple:** Uses DP for keyboard suggestions
- **Google:** Chrome data collection uses local DP
- **Meta, Microsoft:** Research and product applications

https://machinelearning.apple.com/research/differential-privacy-aggregate-trends

https://www.census.gov/programs-surveys/decennial-census/decade/2020/planning-management/process/disclosure-avoidance/differential-privacy.html

https://developers.googleblog.com/en/sharing-our-latest-differential-privacy-milestones-and-advancements/

https://engineering.fb.com/2022/06/14/production-engineering/federated-learning-differential-privacy/

https://blogs.microsoft.com/ai-for-business/differential-privacy/