PRIVACY:

Privacy means "Proof of Privacy".

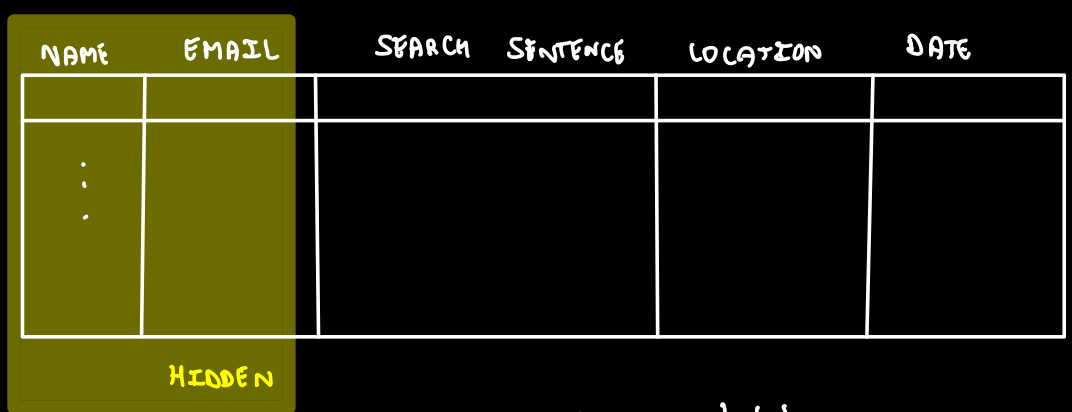
SENSITIVE DATASETS:

→ Medical Records

→ Genetic Data

→ Search Logs

SEARCH LOGS:



AOL: Released such a database.

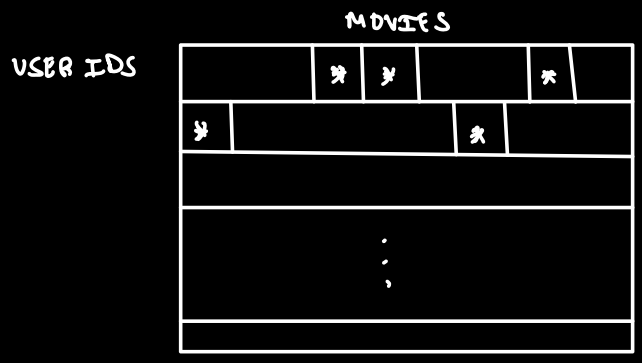
Con: Can be reverse-engineered.

NY TAXICAB:

* FOIL Request to get taxi fare data.
* Medallion, License (HASHED), Vender_id, rate_type, pickup.time, drop.off time, pickup-location, dropoff_location, fare ...

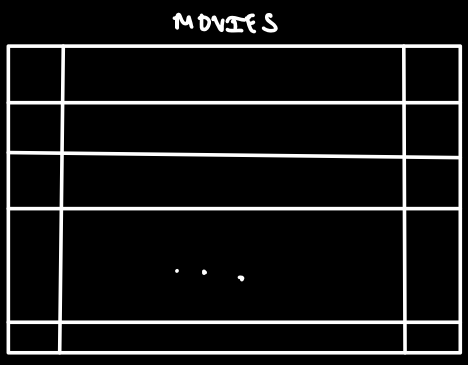
Con; To calculate income earned by various cab drivers.

NETFLIX CHALENGE DATASET:



Narayan and Shmatikov (2008)

IMDB Ratings Database:



LINK

Netflix Challenge 2: 10 Million $ - was cancelled because of a lawsuit for violating privacy.

MASSECHUSETTS : GROUP INSURANCE COMMISSION:

William Weld Governor

→ Every State employees hospital visit records are available (but anonomized to preserve privacy).

Name	SSN	ID	SEX	AGE	ZIP	HEIGHT	WEIGHT	...

are available by voter records database.

Sweeney:

Sent the Governor his medical record information.

"Reconstruction Attacks".

How to get "guaranteed" privacy?

→ First example:

Simplest data analysis tool

→ Person 1 : $x_1 \in \{0,1\}$ "You like Star Wars"

Person 2 : $x_2 \in \{0,1\}$

⋮ ⋮

Person n : $x_n \in \{0,1\}$

→ What we want is to estimate the average $\frac{x_1 + x_2 + \dots + x_n}{n}$. ← p

Silliest:

No Privacy:

x_1, x_2, ⋮, x_n } Released to public ↓ Can compute p exactly.

Full Privacy:

y_1 : "Noisy version of x_1"

y_2

⋮

y_n : "Noisy version of x_n".

"Low p accuracy"

WARNER 1965: "RANDOMIZED RESPONSE" (RR)

Each user $y_i = \begin{cases} x_i & \text{with prob } \frac{1}{2} + \gamma \\ 1 - x_i & \text{with prob } \frac{1}{2} - \gamma \end{cases}$

$$0 < \gamma < \tfrac{1}{2}$$

$\gamma = 0$: "Full Privacy"

$\gamma = \frac{1}{2}$: "No privacy" at all.

$\tilde{p}$ is going to be a function of $y_1, y_2, \dots, y_n$.

$$E[y_i] = \left(\frac{1}{2} + \gamma\right) x_i + \left(\frac{1}{2} - \gamma\right)(1 - x_i)$$

$$= \frac{1}{2} - \gamma + 2\gamma \cdot x_i$$

$$x_i = \frac{E[y_i] - \left(\frac{1}{2} - \gamma\right)}{2\gamma}$$

Suggests: Given the noisy information $y_1, \dots$

Estimate

$$\bar{p} = \frac{\left(\frac{y_1 + \dots + y_n}{n}\right) - \left(\frac{1}{2} - \gamma\right)}{2\gamma}$$

Claim:

$$\Pr\left[\,|\bar{p}-p| > \delta\,\right] \leq \frac{\delta}{\gamma\cdot\sqrt{n}}$$

(Comes from computing variance of $\bar{p}-p$)

Claim:

With 75% chance my estimate $\bar{p}$

$$|\bar{p}-p| \leq \frac{1}{\gamma\sqrt{n}}$$

If we need α accuracy

$$\frac{1}{\gamma\sqrt{n}} \geq \alpha$$

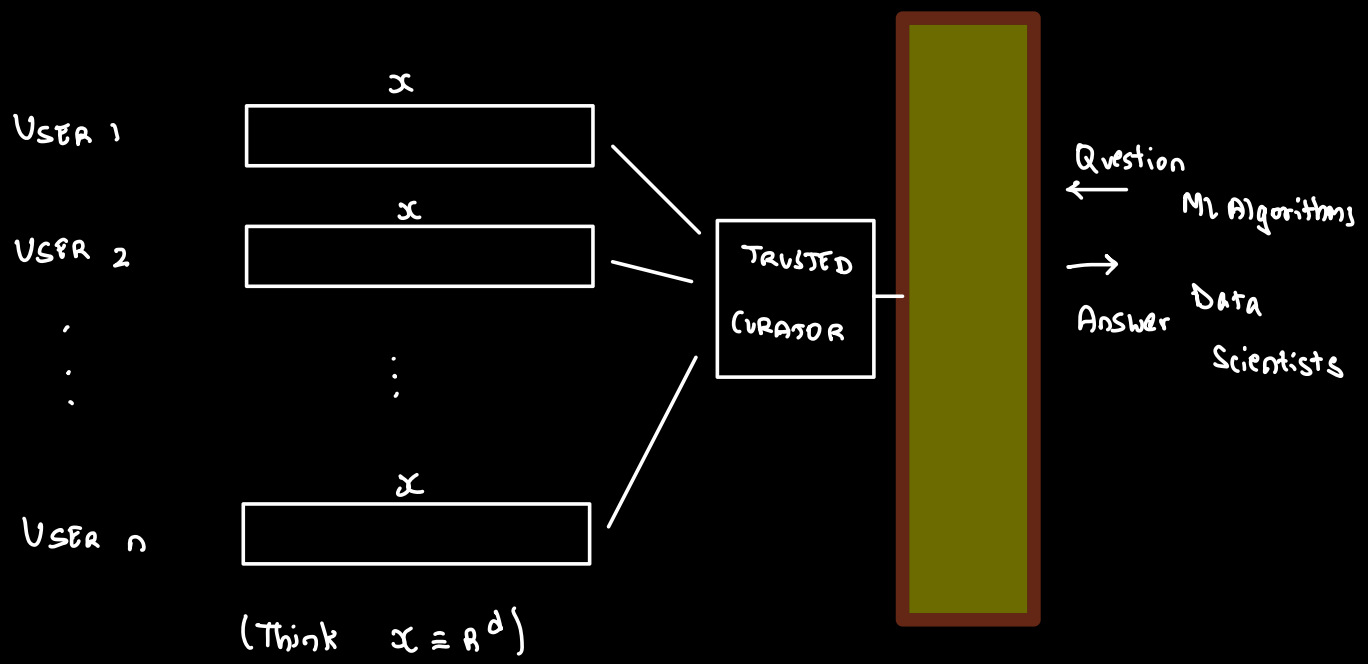
$$n \geq \frac{1}{\gamma^2\cdot\alpha^2}$$

You need at least $n \geq \frac{1}{\gamma^2\cdot\alpha^2}$ people.

DIFFERENTIAL PRIVACY:

"CENTRAL DIFFERENTIAL PRIVACY"

"TRUSTED CURATOR MODEL"



(Think $x \equiv R^d$)

Curator adds noise based on sensitivity of question.

Curator $M: X^n \longrightarrow Y$ (R)

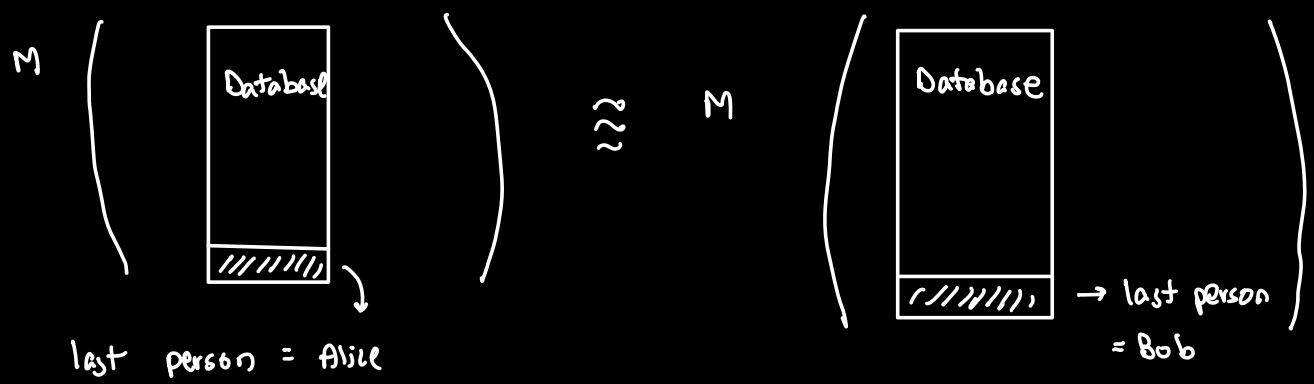
(answer for the query)

↓

database

Idea: Removing one person's data should not change the answers much.

(or replacing)



DEFINITION:

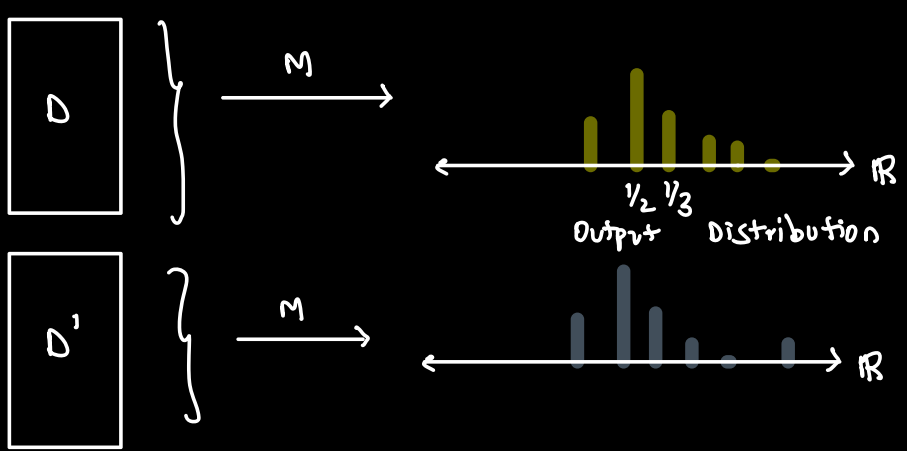
$D, D' \in X^n$ are neighboring if they differ in exactly one row.

DIFFERENTIAL PRIVACY: $M : X^n \to Y$

is ε - Differentially private if $\forall$ neighboring databases D, D', $\forall\ y \in Y$

$$Pr[M(D) = y] \approx Pr[M(D') = y]$$

i.e. $$e^{-\varepsilon} \cdot Pr[M(D') = y] \leq Pr[M(D) = y] \leq e^{\varepsilon} Pr[M(D') = y]$$



Its not enough if outputs similar. Similar distribution is essential.

INTERPRETATION:

$$e^{-\varepsilon} \cdot \Pr[M(D') = y] \leq \Pr[M(D) = y] \leq e^{\varepsilon} \Pr[M(D') = y]$$

$e^{-\varepsilon} \simeq (1 - \varepsilon)$

$e^{\varepsilon} \simeq (1 + \varepsilon)$

DMNSOR : Apple, Google, Microsoft, US Census Bureau 2020.

* Differential Privacy is quantitative
* Small ε corresponds to better privacy.
* ε should be thought of as $\varepsilon = 0.01$.
* This is a worst-case guarantee on the data bases.
* Probabilities are close multiplicatively.
* e^{ε} vs $1 \pm \varepsilon$ is just a convenience.