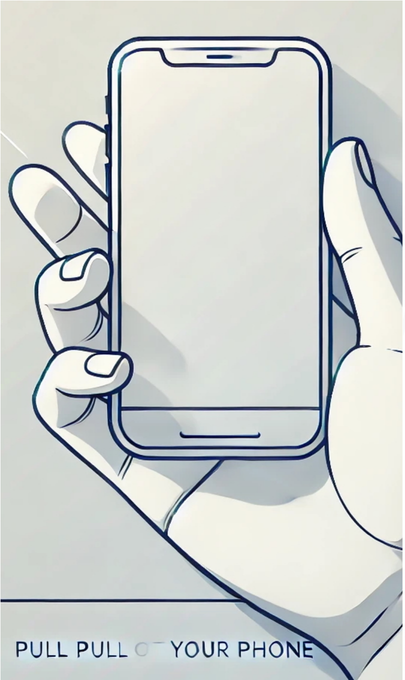
Empowering Innovation: Unlocking the Potential of Privacy-Enhancing Technologies

Univ.-Prof. Dr. Dominique Schröder

October 15, 2024

TU WIEN

PRIVACY
ENHANCING
TECHNOLOGIES


PULL PULL O YOUR PHONE

UNLOCKED

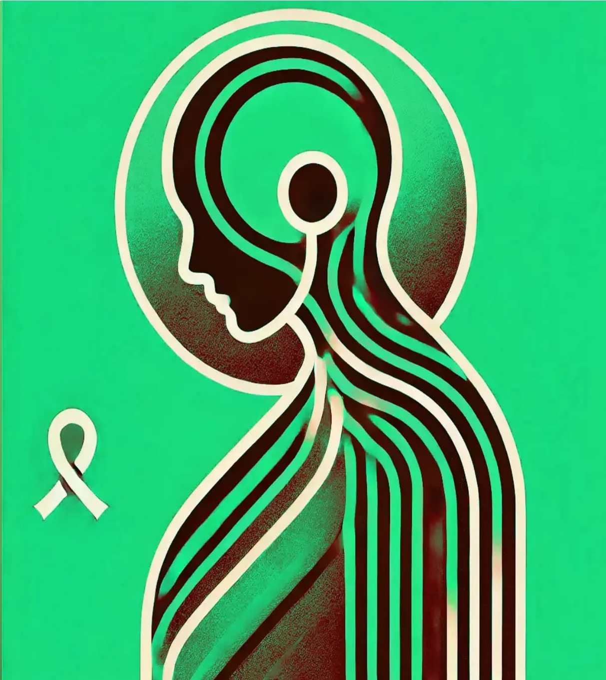

UNL
CK


UNLOCKED


NO DATA SHARING, NO INNOVATION
NO DATA SHARING
NO INNOVATION


Flo

Flo


Flo


The Flo App

PRIVACY
ENHANCING
TECHNOLOGIES

The Flo App

- 380 million downloads
- 68 million monthly active users
- ISO 270001 certification and refers to this certification as “the internationally recognized standard for information security”
- Collects information such as (in privacy mode!):
  - year of birth
  - place of residence
  - (… gender…)

PRIVACY
ENHANCING
TECHNOLOGIES

Starting Point: Matching Attacks

Anonymized dataset containing **confidenital information**

Zip	Age	Sex	Confidential
15XX	70-75	F	...
12XX	25-30	M	...
95XX	65-70	F	...
11XX	15-20	M	...
12XX	45-50	F	...
⋮	⋮	⋮	⋮

Unanonimized dataset containing **no confidenital information**

Identity	Zip	Age	Sex
Alice	1161	19	F
Bob	1234	27	M
Charly	4854	45	F
Dave	1277	28	M
Eve	9584	68	F
⋮	⋮	⋮	⋮

Adversarial goal: match the databases

Starting Point: Matching Attacks

Anonymized dataset containing **confidenital information**

Zip	Age	Sex	Confidential
15XX	70-75	F	...
12XX	25-30	M	...
95XX	65-70	F	...
11XX	15-20	M	...
12XX	45-50	F	...
⋮	⋮	⋮	⋮

Unanonimized dataset containing **no confidenital information**

Identity	Zip	Age	Sex
Alice	1161	19	F
Bob	1234	27	M
Charly	4854	45	F
Dave	1277	28	M
Eve	9584	68	F
⋮	⋮	⋮	⋮

Adversarial goal: match the databases

PRIVACY ENHANCING TECHNOLOGIES

Starting Point: Matching Attacks

Anonymized dataset containing **confidenital information**

Zip	Age	Sex	Confidential
15XX	70-75	F	...
12XX	25-30	M	...
95XX	65-70	F	...
11XX	15-20	M	...
12XX	45-50	F	...
⋮	⋮	⋮	⋮

Unanonimized dataset containing **no confidential information**

Identity	Zip	Age	Sex
Alice	1161	19	F
Bob	1234	27	M
Charly	4854	45	F
Dave	1277	28	M
Eve	9584	68	F
⋮	⋮	⋮	⋮

Adversarial goal: match the databases

Starting Point: Matching Attacks

Anonymized dataset containing **confidenital information**

Zip	Age	Sex	Confidential
15XX	70-75	F	...
12XX	25-30	M	...
95XX	65-70	F	...
11XX	15-20	M	...
12XX	45-50	F	...
⋮	⋮	⋮	⋮

Unanonimized dataset containing **no confidenital information**

Identity	Zip	Age	Sex
Alice	1161	19	F
Bob	1234	27	M
Charly	4854	45	F
Dave	1277	28	M
Eve	9584	68	F
⋮	⋮	⋮	⋮

Adversarial goal: match the databases

TU WIEN

PRIVACY ENHANCING TECHNOLOGIES

Starting Point: Matching Attacks

Anonymized dataset containing **confidenital information**

Zip	Age	Sex	Confidential
15XX	70-75	F	...
12XX	25-30	M	...
95XX	65-70	F	...
11XX	15-20	M	...
12XX	45-50	F	...
⋮	⋮	⋮	⋮

Unanonimized dataset containing **no confidenital information**

Identity	Zip	Age	Sex
Alice	1161	19	F
Bob	1234	27	M
Charly	4854	45	F
Dave	1277	28	M
Eve	9584	68	F
⋮	⋮	⋮	⋮

Adversarial goal: match the databases

PRIVACY
ENHANCING
TECHNOLOGIES

Starting Point: Matching Attacks

Anonymized dataset containing **confidenital information**

Zip	Age	Sex	Confidential
15XX	70-75	F	...
12XX	25-30	M	...
95XX	65-70	F	...
11XX	15-20	M	...
12XX	45-50	F	...
⋮	⋮	⋮	⋮

Unanonimized dataset containing **no confidenital information**

Identity	Zip	Age	Sex
Alice	1161	19	F
Bob	1234	27	M
Charly	4854	45	F
Dave	1277	28	M
Eve	9584	68	F
⋮	⋮	⋮	⋮

Adversarial goal: match the databases

Conditional Anonymity

The Dataset

Case Studies

Visual Anon

Open Question

How can we **access the unanonymized dataset**?

PRIVACY
ENHANCING
TECHNOLOGIES

Idea: Conditional Anonymity

- We gather publicly available statistical data.
- Using **population statistics**, we estimate the anonymity set size $\psi(\vec{a})$.
- We refine the set size by each **auxiliary information** we have.
- We define the conditional anonymity set for attributes $\vec{a}$ and $\vec{b}$ via

$$\mathrm{A}_{\mathcal{P}}(\vec{a} \mid \vec{b}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right].$$

PRIVACY
ENHANCING
TECHNOLOGIES

Idea: Conditional Anonymity

- We gather publicly available statistical data.
- Using **population statistics**, we estimate the anonymity set size $\psi(\vec{a})$.
- We refine the set size by each **auxiliary information** we have.
- We define the conditional anonymity set for attributes $\vec{a}$ and $\vec{b}$ via

$$\mathrm{A}_{\mathcal{P}}(\vec{a} \mid \vec{b}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right].$$

PRIVACY
ENHANCING
TECHNOLOGIES

Idea: Conditional Anonymity

- We gather publicly available statistical data.
- Using **population statistics**, we estimate the anonymity set size $\psi(\vec{a})$.
- We refine the set size by each **auxiliary information** we have.
- We define the conditional anonymity set for attributes $\vec{a}$ and $\vec{b}$ via

$$\mathrm{A}_{\mathcal{P}}(\vec{a} \mid \vec{b}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right].$$

PRIVACY
ENHANCING
TECHNOLOGIES

Idea: Conditional Anonymity

- We gather publicly available statistical data.
- Using **population statistics**, we estimate the anonymity set size $\psi(\vec{a})$.
- We refine the set size by each **auxiliary information** we have.
- We define the conditional anonymity set for attributes $\vec{a}$ and $\vec{b}$ via

$$\mathrm{A}_{\mathcal{P}}(\vec{a} \mid \vec{b}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right].$$

PRIVACY ENHANCING TECHNOLOGIES

Conditional Anonymity Sets

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$

$\psi(\vec{a}) = 10$

$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$

$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

Conditional Anonymity Sets

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$

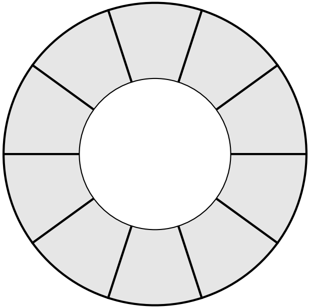
$\psi(\vec{a}) = 10$ $\quad$ $\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$ $\quad$ $\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

TU WIEN PRIVACY ENHANCING TECHNOLOGIES

Conditional Anonymity Sets

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$



$$\psi(\vec{a}) = 10$$

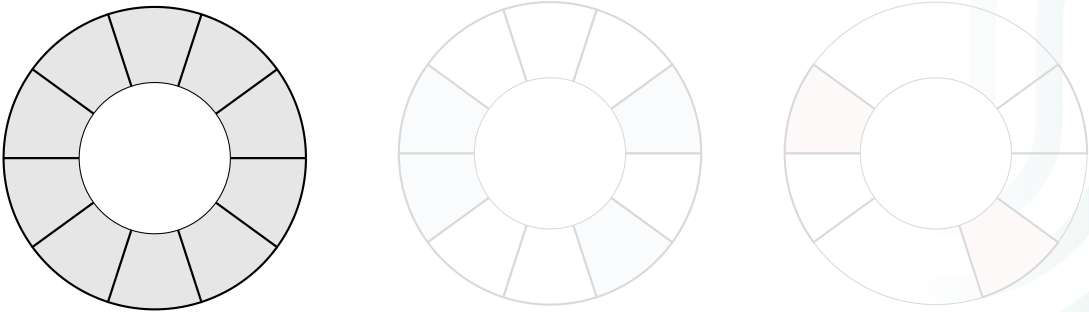
$$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$$

$$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

Conditional Anonymity Sets

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$



$\psi(\vec{a}) = 10$

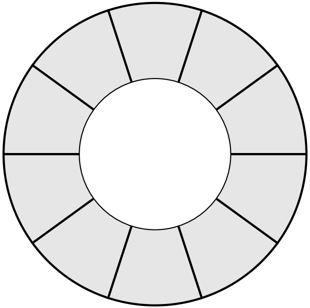
$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$

$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$

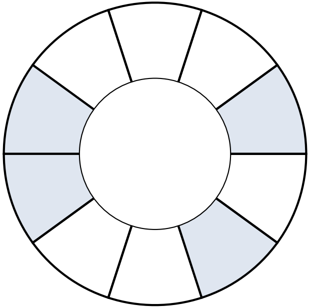
$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

Conditional Anonymity Sets

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$



$\psi(\vec{a}) = 10$



$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$

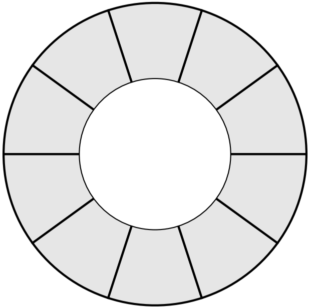
$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

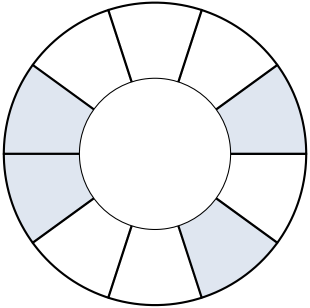
PRIVACY
ENHANCING
TECHNOLOGIES

Conditional Anonymity Sets

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$



$\psi(\vec{a}) = 10$



$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$

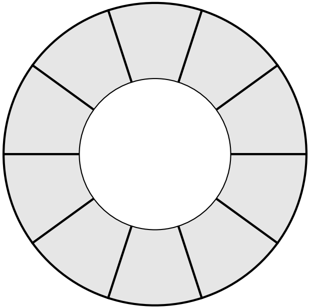
$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

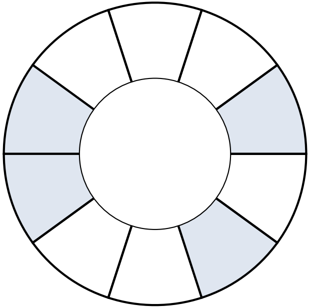
PRIVACY
ENHANCING
TECHNOLOGIES

Conditional Anonymity Sets

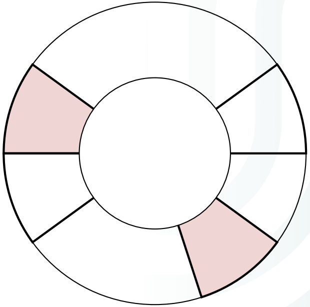
$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$



$$\psi(\vec{a}) = 10$$



$$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$$



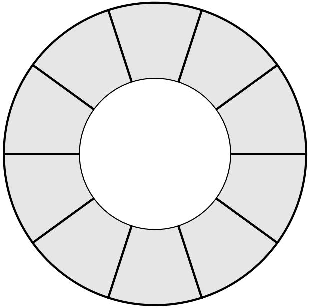
$$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

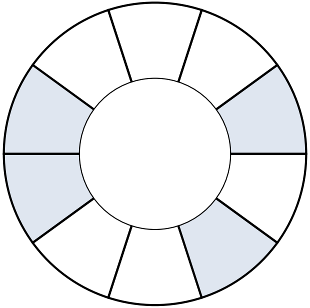
PRIVACY ENHANCING TECHNOLOGIES

Conditional Anonymity Sets

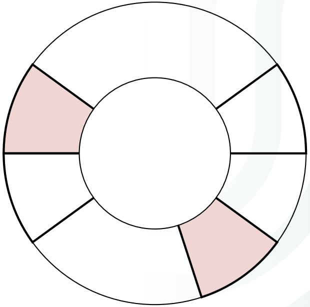
$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = \psi(\vec{a}) \cdot \Pr\left[\vec{b} \mid \vec{a}\right] \cdot \Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right]$$



$\psi(\vec{a}) = 10$



$\Pr\left[\vec{b} \mid \vec{a}\right] = 0.4$



$\Pr\left[\vec{c} \mid \vec{a} \wedge \vec{b}\right] = 0.5$

$$\mathsf{A}_{\mathcal{P}}(\vec{a} \mid \vec{b} \mid \vec{c}) = 10 \cdot 0.4 \cdot 0.5 = 2$$

Conditional Anonymity

The Dataset

Case Studies

Visual Anon

PRIVACY
ENHANCING
TECHNOLOGIES

Data Request

Paul Gerhart 22. November 2021 at 11:56

Consensus-data request for researching purposes

Bcc: census.customerservices@ons.gov.uk, Eurostat Helpdesk_EN, User Information Services Stats SA, leosanni@nigerianstat.gov.ng, STATCAN.infostats-infostats.STATCAN@canada.ca, Atencion a Usuarios, ibge@ibge.gov.br, info, Stat, info@stats.gov.cn, ddu.rgi@nic.in, pbs@pbs.gov.pk, client.services@abs.gov.au, info@stats.govt.nz, nstac-info@nstac.go.jp, statistics@un.org, statistics@afdb.org, nfo@tuik.gov.tr, Dominique Schröder, Pascal Berrang

Hide

To whom it may concern,
My name is Paul Gerhart, and I am part of a privacy research team at the chair of applied cryptography of ~~the Friedrich-Alexander-University Erlangen-Nürnberg~~ TU Wien :) in cooperation with the University of Birmingham.

My team and I are working on a web app to inform people about the anonymity set they are currently living in. That is the number of people who fit in the same data bucket created by several data points one may provide voluntarily without worries. With our app, we want to create awareness of how sensitive personal data is to help people protect their privacy.

Our work is based on the paper Pandemic Privacy by Berrang and Schröder, but we want to stress the insights to a worldwide dataset.

Therefore, we are interested in census data that gives insights into the population count by postcode separated by age groups and sex. Moreover, we are interested in the distribution of height and weight by age group and sex.

Based on this data alone, we cannot deanonymize people, but we can show how anonymity decreases by the publication of personal data that might seem irrelevant.

Hence we were hoping you could provide the desired data for us.

Best regards

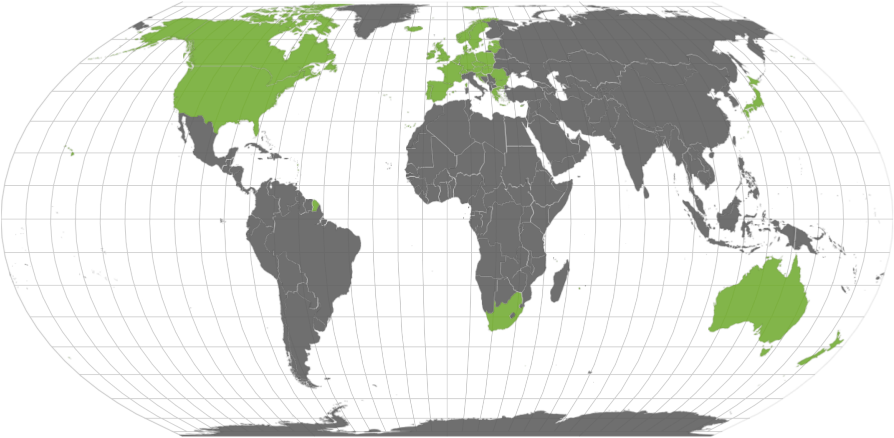
Paul Gerhart

--
Paul Gerhart @ TU Wien
~~paul.gerhart@fau.de~~
~~Lehrstuhl für Angewandte Kryptographie~~
~~Friedrich-Alexander-Universität Erlangen-Nürnberg~~

PRIVACY ENHANCING TECHNOLOGIES

Our Dataset

Currently, we can calculate anonymity sets for 1 084 230 346 people.



PRIVACY
ENHANCING
TECHNOLOGIES

Data Response I

S

Stat

Ответ на обращение

To: Paul Gerhart

VisualAnon 8. December 2021 at 13:33

Данные.xlsx

PDF **Подлинник.pdf**

Data Response II

МИНЭКОНОМРАЗВИТИЯ РОССИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА ГОСУДАРСТВЕННОЙ СТАТИСТИКИ (РОССТАТ)

Мясницкая ул., д. 39, стр. 1, г. Москва, 107450
Тел.: (495) 607-49-02, факс: (495) 607-22-06
http://www.gks.ru; e-mail: stat@gks.ru

08.12.2021 № 6116/01

на № ________________ от ____________

Герхарт П.

paul.gerhart@fau.de

Уважаемый господин Герхарт!

В связи с Вашим обращением направляем имеющуюся официальную статистическую информацию о распространенности роста и веса в разбивке по возрастным группам (в возрасте 15 лет и более) и полу. Данные предоставлены по итогам Выборочного наблюдения состояния здоровья населения 2020 года, материалы и база микроданных которого размещены на официальном сайте Росстата (https://rosstat.gov.ru/): Статистика/ Переписи и обследования/ Федеральные статистические наблюдения по социально-демографическим проблемам/ Итоги выборочного наблюдения состояния здоровья населения.

PRIVACY ENHANCING TECHNOLOGIES

Conditional Anonymity

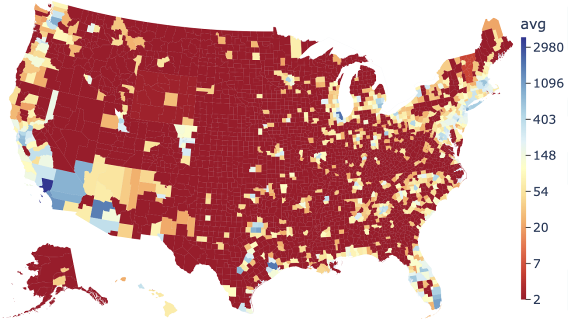
The Dataset

Case Studies

Visual Anon

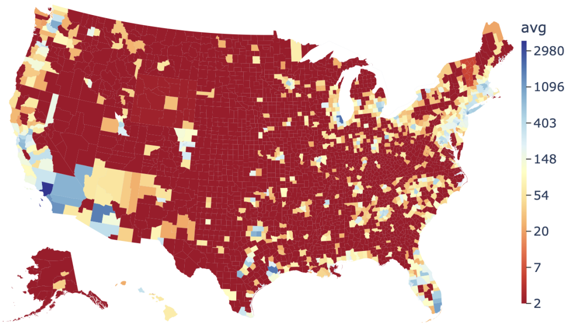
Case Study: USA

- Avg. CAS: 77
- Avg. CAS in red area: 2
- Avg. CAS below 5 in 97% of the counties



PRIVACY
ENHANCING
TECHNOLOGIES

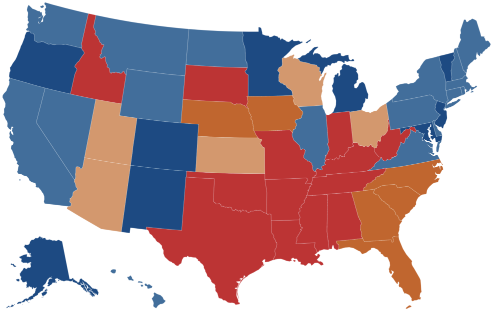
Roe v. Wade: Flo App



Status of Abortion Bans in the United States as of October 7, 2024

Hover over state for more details

- Abortion Banned (13 states)
- Gestational limit between 6 and 12 weeks LMP (6 states)
- Gestational limit between 15 and 22 weeks LMP (5 states)
- Gestational limit at or near viability (17 states)
- No gestational limits (9 states & DC)



Note: LMP refers to Last Menstrual Period. *Viability* is the point when a fetus can survive outside the womb and is generally presumed to occur at around 24 weeks gestation. However, viability it has never been properly defined by courts and depends on the individual pregnancy and on various factors, including gestational age, fetal weight and sex, and medical interventions available.
For more details please see our trackers on exceptions to state abortion bans and early gestational limits , abortion-related ballot initiatives , state and federal litigation , and our KFF State Health Facts page on abortion policies.

Source: KFF analysis of state policies and court decisions, as of October 7, 2024. • Get the data • Embed • Download PNG

KFF

PRIVACY
ENHANCING
TECHNOLOGIES

Visual Anon (Age)

Visual Anon Check

Country

Austria

District

Wien

Sex

Female

Age

50 - 54 years

Height

Nothing selected

Weight

Nothing selected

Your anonymity set

Providing this data you can be deanonymized up to **59 431** Persons.

8 401 940 People live in Austria	59 431 are in the ['50'] years bucket
1 714 227 of them in Wien	
741 717 are female	

Distribution of all variables

About our data quality

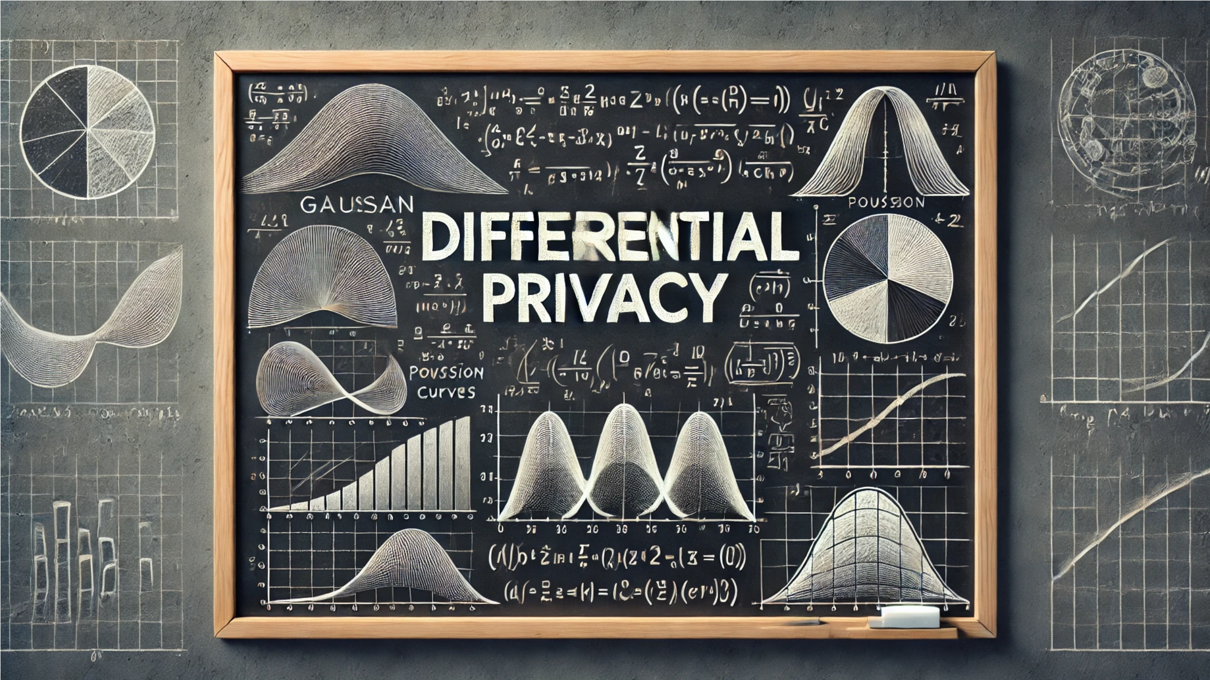
The range of the data we were able to fetch is limited. Therefore there might be existent people that are outside the range of our data.

For further simplification we assumed the weight and height data to be gaussian distributed. That is not exactly the case in reality but simplifies our assumptions.

We were not able to fetch any data for non-binary people, so you can just choose between male and female.

VisualAnon

PRIVACY
ENHANCING
TECHNOLOGIES


GAUSSAN
DIFFERENTIAL
PRIVACY
POUSSON
POVSSION
CURVES

Differential Privacy

Example: Grade Release in Schools

Grade	Count
1	2
2	4
3	6
4	3
5	1
Mean	2.8125

Differential Privacy

Example: Grade Release in Schools

Grade	Count	Revealed
1	2	2
2	4	4
3	6	6
4	3	3
5	1	0
Mean	2.8125	2.5

- There are 16 students in class
- Teacher publishes mean grade: 2.8125
- Students learn the grade of each student except for one
- The mean of the publishing students is 2.5 (assigning a 0 to the unpublishing student)
- They compute

$$(2.8125 - 2.5) * 16 = 5$$

and leak the unpublished grade

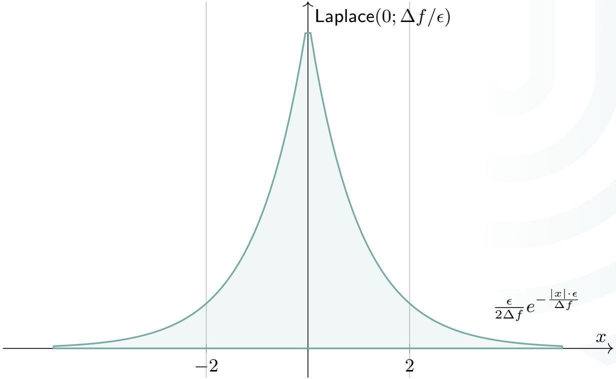
TU WIEN PRIVACY ENHANCING TECHNOLOGIES

Differential Privacy

Example: Histogram Queries

$$\mathsf{cnt}'(x) = \mathsf{cnt}(x) + \mathsf{Laplace}(0, 1/\epsilon)$$

x	$\mathsf{cnt}(x)$	$\epsilon = 2$
1	2	1.96
2	4	3.46
3	6	6.08
4	3	3.16
5	1	1.62
$\mathbb{E}(X)$	2.8125	2.9398



PRIVACY
ENHANCING
TECHNOLOGIES

Differential Privacy

Example: Grade Release in Schools

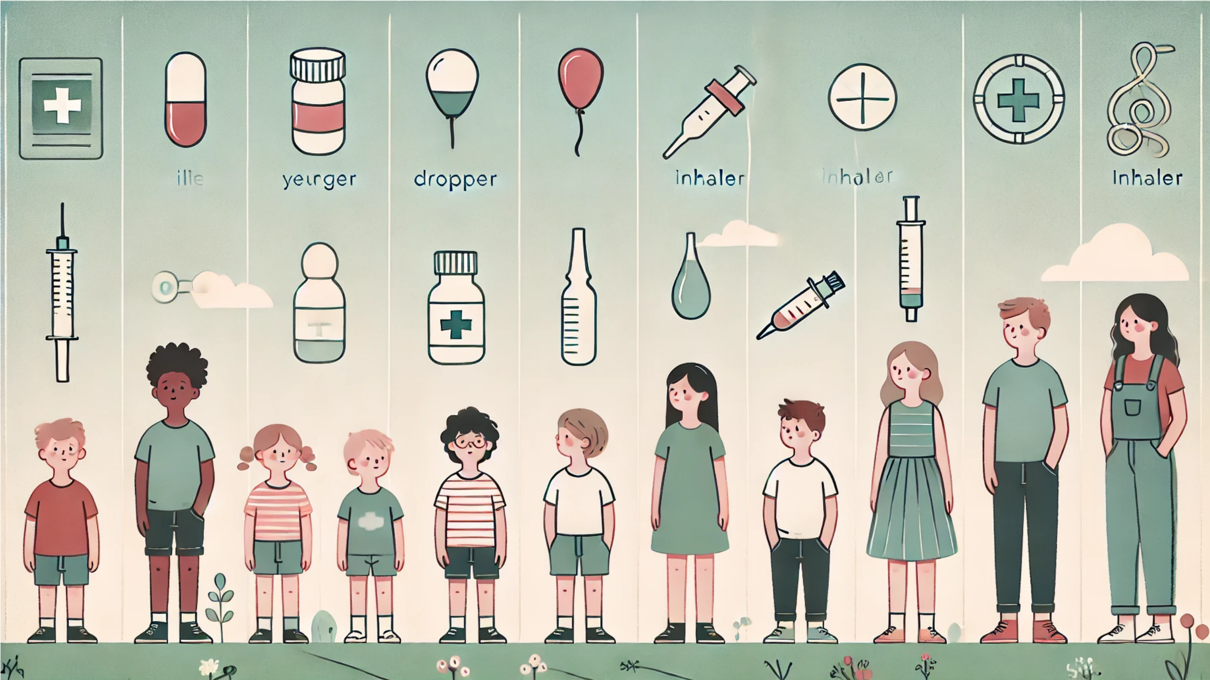
Grade	Count	Revealed
1	1.96	2
2	3.46	4
3	6.08	6
4	3.16	3
5	1.62	0
Mean	2.9398	2.5

Computing the missing grade:

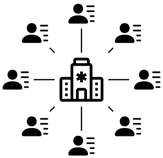
$$(2.9398 - 2.5) \cdot 16 = 7.03$$

Impact of Histogram Queries

Industry	Medicine
Customer Behavior *(Amazon, Walmart)* - Analyzes purchases - E.g., purchases per month	**Patient Health Data** *(Mayo Clinic, Cleveland Clinic)* - Summarizes patient data - E.g., age distribution of patients
Log Analysis *(AWS, Azure)* - Monitors system logs - E.g., server response times	**Drug Effectiveness** *(Pfizer, Novartis)* - Analyzes treatment responses - E.g., drug dosage effectiveness
Financial Risk *(JP Morgan, Goldman Sachs)* - Categorizes risk levels - E.g., asset risk distribution	**Epidemiology** *(CDC, WHO)* - Tracks infection rates - E.g., COVID-19 spread
Supply Chain *(FedEx, Toyota)* - Tracks delivery times - E.g., shipment times	**Medical Imaging** *(Radiology, MRI)* - Analyzes image intensity - E.g., MRI scan analysis

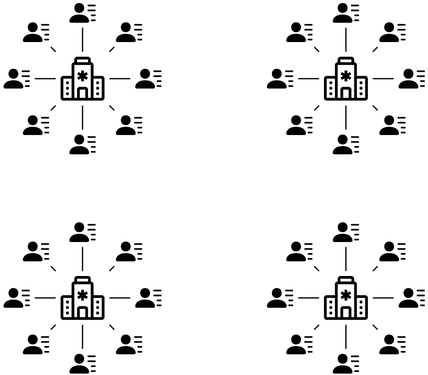

ille
yeırger
dropper
Inhaler
Inhaler
Inhaler

Applying PETs to Help Defeat Childhood Cancer



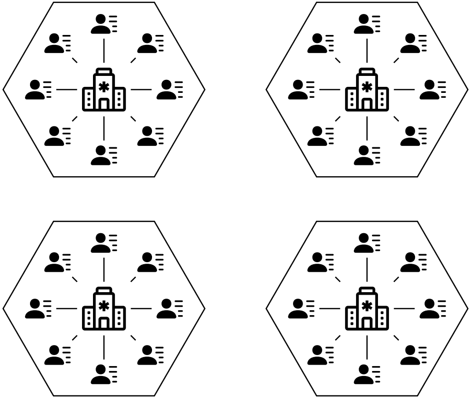
- The dataset of a single hospital is too sparse
- **Idea:** Combine the datasets of multiple hospitals
- **Problem:** The data cannot leave the hospital
- **Solution:** We design an MPC protocol and apply differential privacy

Applying PETs to Help Defeat Childhood Cancer



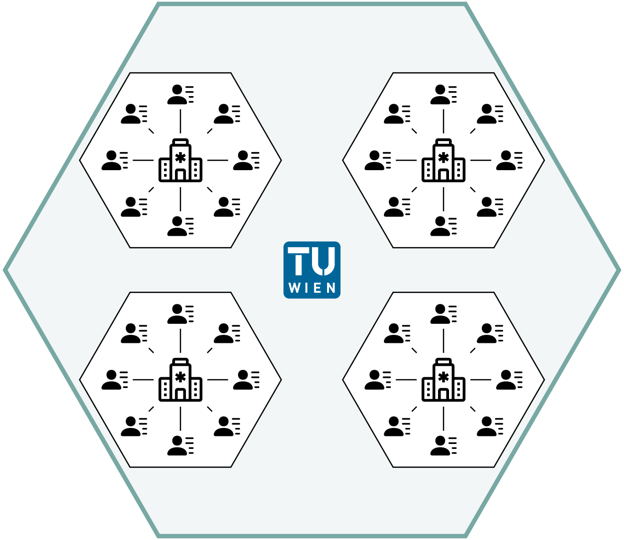
- The dataset of a single hospital is too sparse
- **Idea:** Combine the datasets of multiple hospitals
- **Problem:** The data cannot leave the hospital
- **Solution:** We design an MPC protocol and apply differential privacy

Applying PETs to Help Defeat Childhood Cancer



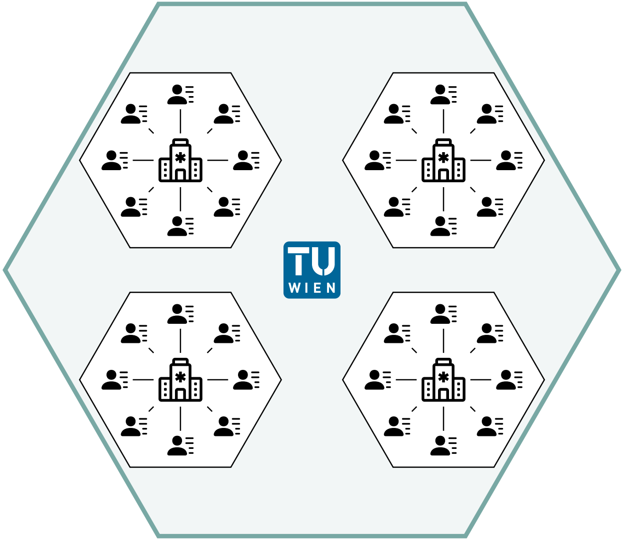
- The dataset of a single hospital is too sparse
- **Idea:** Combine the datasets of multiple hospitals
- **Problem:** The data **cannot** leave the hospital
- **Solution:** We design an MPC protocol and apply differential privacy

Applying PETs to Help Defeat Childhood Cancer



- The dataset of a single hospital is too sparse
- **Idea:** Combine the datasets of multiple hospitals
- **Problem:** The data cannot leave the hospital
- **Solution:** We design an MPC protocol and apply differential privacy

Applying PETs to Help Defeat Childhood Cancer



- The dataset of a single hospital is too sparse
- **Idea:** Combine the datasets of multiple hospitals
- **Problem:** The data cannot leave the hospital
- **Solution:** We design an MPC protocol and apply differential privacy

Privacy Guarantee

No patient data ever leaves any hospital

PRIVACY ENHANCING TECHNOLOGIES

How PETS Work Under the Hood

PreRound(pk)

$X \leftarrow pk$
$d_i, \leftarrow_{\$} \mathbb{Z}_p \,;\; e_i, \leftarrow_{\$} \mathbb{Z}_p$
$D_i \leftarrow g^{d_i} \,;\; E_i \leftarrow g^{e_i}$
$state_i \leftarrow (d_i, e_i)$
$\rho_i \leftarrow (D_i, E_i)$
$\textbf{return } (state_i, \rho_i)$

PreAgg$(pk, \{\rho_i\}_{i\in S})$

$X \leftarrow pk$
$\{(D_i, E_i)\}_{i\in S} \leftarrow \{\rho_i\}_{i\in S}$
$D \leftarrow \prod_{i\in S} D_i$
$E \leftarrow \prod_{i\in S} E_i$
$\rho \leftarrow (D, E)$
$\textbf{return } \rho$

Lagrange(S, i)

$\Lambda_i \leftarrow \prod_{j\in S\setminus\{i\}} j/(j-i)$
$\textbf{return } \Lambda_i$

SignRound$(sk_i, pk, S, state_i, \rho, m)$

$/\!/$ called at most once per secret state $state_i$
$\overline{x}_i \leftarrow sk_i \,;\; X \leftarrow pk$
$(D, E) \leftarrow \rho$
$(d_i, e_i) \leftarrow state_i$
$b \leftarrow \mathsf{H}_{\mathrm{non}}(X, S, \rho, m)$
$R \leftarrow DE^b$
$c \leftarrow \mathsf{H}_{\mathrm{sig}}(X, R, m)$
$\Lambda_i \leftarrow \mathsf{Lagrange}(S, i)$
$\sigma_i \leftarrow d_i + be_i + c\Lambda_i\overline{x}_i$
$\textbf{return } \sigma_i$

SignAgg$(pk, \rho, \{\sigma_i\}_{i\in S}, m)$

$X \leftarrow pk$
$(D, E) \leftarrow \rho$
$b \leftarrow \mathsf{H}_{\mathrm{non}}(X, S, \rho, m)$
$R \leftarrow DE^b$
$s' \leftarrow \sum_{i\in S} \sigma_i$
$\sigma \leftarrow (R, s)$
$\textbf{return } \sigma$

Verify(pk, m, σ)

$X \leftarrow pk$
$(R, s) \leftarrow \sigma$
$c \leftarrow \mathsf{H}_{\mathrm{sig}}(X, R, m)$
$\textbf{return } (g^s = RX^c)$

Practical Schnorr Threshold Signatures without the Algebraic Group Model
Hien Chu, Paul Gerhart, Tim Ruffing & Dominique Schröder
CRYPTO'23

PRIVACY ENHANCING TECHNOLOGIES

Current Research

Work Published by E192-08

Measuring Conditional Anonymity — A Global Study

PETS'24

SoK: Descriptive Statistics Under Local Differential Privacy

PETS'25

TU WIEN

PRIVACY
ENHANCING
TECHNOLOGIES