ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

The German Self-Determination Act

MPC as a Tool for Better Privacy in Administrative Data Exchange?

Speaker: Andreas Brüggemann (they/them)

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contact

https://encrypto.de

Passed in 2024, aimed to protect trans* people

Yet: Almost (and might again) enable building register of trans* people

Collaboration & Publications

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

- Interdisciplinary collaboration between
  - Law: Linda Seyda & Gerrit Hornung
  - Cryptography: Andreas Brüggemann & Thomas Schneider

UNIKASSEL VERSITÄT

TECHNISCHE UNIVERSITÄT DARMSTADT

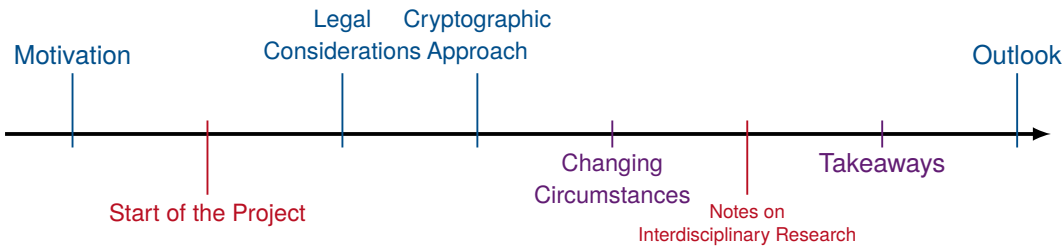
- within Research Training Group Privacy and Trust for Mobile Users
- Results published at “Workshop Recht und Technik” (Law and Engineering) 2024 [SBH+24]
- and as a poster at Decrypting Diversity Summit 2025 [SBH+25].

[SBH+24] L. Seyda, A. Brüggemann, G. Hornung, and T. Schneider. “Multi-Party Computation als Instrument zur Umsetzung datenschutzkonformer behördlicher Datenabgleiche: Eine interdisziplinäre Analyse am Beispiel der Diskussionen um das Gesetz zur Selbstbestimmung über den Geschlechtseintrag”. *INFORMATIK 2024, Workshop Recht und Technik: Datenschutz im Diskurs (RuT'24)*. LNI. Wiesbaden, Germany, 2024

[SBH+25] L. Seyda, A. Brüggemann, G. Hornung, and T. Schneider. *POSTER: The German Self-Determination Act—Ignoring Cryptography and Endangering Trans* People.* Decrypting Diversity Summit. 2025

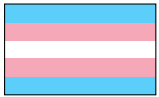
Outline

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING



Some Terms & Definitions

- trans
- non-binary
- inter
- queer, LGBTQIA+, …



Background
The Transsexual Act (TSG)

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Required lengthy, expensive, and degrading process to change name and gender entries
- **Expert Assessment to confirm gender identity**
- Parts declared unconstitutional by the Federal Constitutional Court (BVerfG) in 6 decisions
- E.g., one decision connected to prior forced sterilization

$\Rightarrow$ Superseded 2024 by the SBGG

The German Self-Determination Act (SBGG)

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Official title: *Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag (SBGG)* (law on self-determination with regard to gender entry)
- Active since November 2024
- **Enables trans/inter/nonbinary people to change first name(s) / gender entry by self-declaration**
- § 2: Declaration of entry changes at civil registation office
- § 4: 3 months waiting time
- § 6 & § 9: Severe issues enabling future discrimination, *not our focus here*
- **§ 13: Prohibition of disclosure**, § 14: fines

But What About Policework?

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Hypothetical threat: Criminals might use the SBGG to evade law enforcement agencies (LEAs)

$\Rightarrow$ LEAs should be proactively informed about any name changes using the SBGG

- Note: LEAs are not proactively informed about name changes due to
  - priorly: TSG as predecessor of the SBGG
  - marriage
  - divorce
  - being hard to spell/pronounce
  - …

Original Idea for Data Transfer

Draft from November 2023 [BT23]

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Exception (para. 5) to § 13: Registration office must send

- last name, birth date, ...
- **deadname & new name**
- **prior & new gender entry**

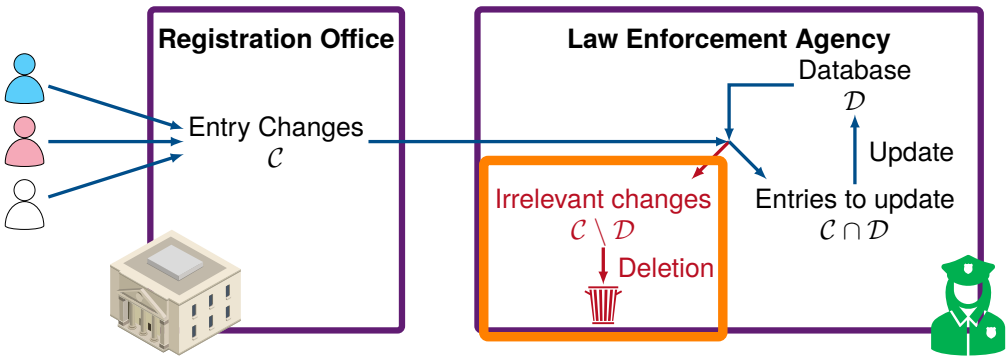
to

- Federal Criminal Police Office (BKA)
- Federal Police (BPOL)
- ...
- Federal Office for the Protection of the Constitution (BfV)
- Military Counterintelligence Service (MAD)
- ...

for keeping their databases up to date.

[BT23] *BT-Drs. 20/9049*. 2023. URL: https://dserver.bundestag.de/btd/20/090/2009049.pdf

Original Idea for Data Transfer



Agencies using Lists of Queer People?

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- „Rosa Listen“—Lists of (supposed) homosexual people used in Nazi Germany
- Some German LEAs have used tag for homosexual people in their databases until at least 2005 [Ve]
- AG of Texas tried building registry of trans* people from driver license changes already in 2022 [WP22]
- Largest German police union reports worries in LEAs about information falling into the wrong hands [ZDF24]
- German police interfering with and now also stopping Pride, e.g. [GEW25]
- I gave up updating this list, search the internet for “USA transgender”...

[Ve] VelsPol e.V. *Geschichte der Rosa Listen*. URL: https://www.velspol-nrw.de/html/rosa-listen.html

[WP22] “Texas Attorney General’s Office Sought State Data on Transgender Texans”. *The Washington Post* Dec. 14 (2022)

[ZDF24] “Polizisten fürchten AfD-Regierungsbeteiligung”. *ZDFheute* Aug. 12 (2024)

[GEW25] T. Gropius, F. von der Eltz, and M. Wilczek. “CSD in Schönebeck frühzeitig beendet: Veranstalter kritisiert Behörden”. *MDR Sachen-Anhalt* Jun. 11 (2025)

Start of the Research

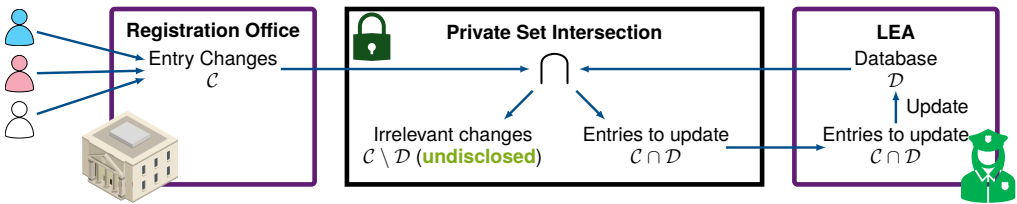
ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Discovered topic from a meme (Sep. or Okt. 23)

- First articles about the proposed data transfer (Aug. 23) [Kö23a; Kö23b]
- Fairly obvious and immediate risk
- Big share of the risk clearly avoidable

[Kö23a] C. Köver. “Selbstbestimmungsgesetz: Datenweitergabe an den gesamten Sicherheitsapparat”. *netzpolitik.org* Aug. 30 (2023)
[Kö23b] C. Köver. “Selbstbestimmungsgesetz: Unter Generalverdacht”. *netzpolitik.org* Aug. 30 (2023)

Cryptographic Means not to Trust Police to Delete



The RTG Privacy and Trust for Mobile Users

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Privacy and Trust
for Mobile Users

- RTG: Research Training Group (German: GRK)
- “DFG’s idea of a Lightweight Graduate School”
- Here: Focus on **interdisciplinary** collaboration between **computer science**, **law**, sociology, economics, psychology
- Research areas;
  - A: Privacy and Trust in Service Networks
    - A.1 Privacy Mechanisms in Applications Considering the Digital Economy
  - B: Privacy and Trust in Social Networks
  - C: Privacy and Trust in Sensor Augmented Environments
    - C.2 Privacy Protection in Human-Distant IoT Environments
  - D: Privacy and Trust via AlterEgo

Building a Team

Not what really actively happened—It already existed

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

We (Linda and I) had already been searching for a possible collaboration project

Possibly relevant domains to be involved:

- Law ⇒ Linda (researched, e.g., GDPR, surveillance), Gerrit
- Cryptography ⇒ me, Thomas
- Queer Rights ⇒ me, also in contact with other queer activists
- LEAs ⇒ none, deliberately
- Lawmakers ⇒ none, so far

In favor of Data Transfer to LEAs

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Legimitate Interest

- LEAs need correct data about citizens in their registers for inner security (?)

Accuracy Principle, Art. 5(1d) GDPR

- Personal data to be accurate and up to date
- Incorrect data to be deleted or corrected

$\Rightarrow$ Need to update outdated name and gender entries

Against Data Transfer to LEAs

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Data Minimisation Principle, Art. 5(1c) GDPR

- Data to be strictly limited to what is necessary
- Processing only permissible if goal cannot be reached otherwise [Roß19]
- Legimitate Interest?

$\Rightarrow$ **But: Only regarding data of people already in the database**

[Roß19] A. Roßnagel. “DSGVO Art. 5”. *Simitis, S.; Hornung, G.; Spiecker gen. Döhmann, I. (Hrsg.): Datenschutzrecht*. 1st ed. Nomos, 2019

Federal Data Protection Commissioner—Statement [BfDI23]

- **Data Minimisation Principle outweighs Accuracy Principle here**
- Also supported by the “general right of personality”, Art. 2 GG (German constitution)
- Possible compromise: At least, do not transfer the gender entry (?)

[BfDI23] *Stellungnahme des BfDI zum SBGG-E*. 2023. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Selbstbestimmung-Geschlechtseintrag.pdf?__blob=publicationFile&v=2

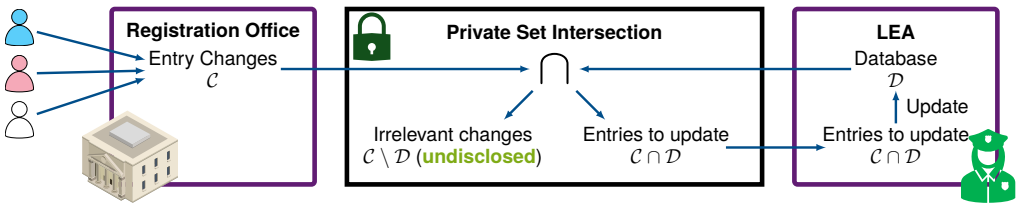
Possible Resulting Requirements

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

R1 Entry changes regarding persons unknown to a security agency must not be disclosed to this agency.

R2 (Parts of) the database held by a security agency must not be disclosed to others.

Possible Solution to this Dilemma



Infeasibility of PSI?

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

„Die Mitteilungen über Namensänderungen können nicht auf die Personen beschränkt werden, über die das Register eine Eintragung enthält, da dies den [. . .] Behörden, [. . .], regelmäßig nicht bekannt ist.“

[BT96, S. 30]

“The notifications about name changes cannot be limited to the persons on whom the register contains an entry, as this is routinely unknown to the [. . .] authorities.”

[BT96, p. 30, translated]

[BT96] *BT-Drs. 13/4709*. 1996. URL: https://dserver.bundestag.de/btd/13/047/1304709.pdf

Requirements for a PSI Solution

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

PSI clearly can be practical: Password protection [NNS+19; App21]

But:

- Likely expensive (computation, communication, deployment, . . .)
- PSI with payload
- Fuzzy PSI [UCK+21]
- Threshold for legitimate transfer? [TMS+22]
- Security assumptions, mistakes in protocol/implementation, . . .

[NNS+19] P. Nepper, K. C. Nair, V. Sukhanov, and V. Khaneja. “Better password protections in Chrome - How it works”. *Google Security Blog* (2019). URL: https://security.googleblog.com/2019/12/better-password-protections-in-chrome.html

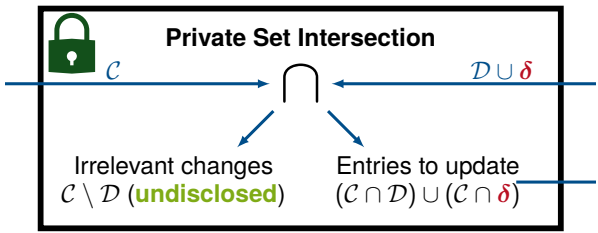
[App21] Apple Support. *Password Monitoring*. 2021. URL: https://support.apple.com/en-ie/guide/security/sec78e79fc3b/web

[UCK+21] E. Uzun, S. P. Chung, V. Kolesnikov, A. Boldyreva, and W. Lee. “Fuzzy Labeled Private Set Intersection with Applications to Private Real-Time Biometric Search”. *USENIX Security*. 2021

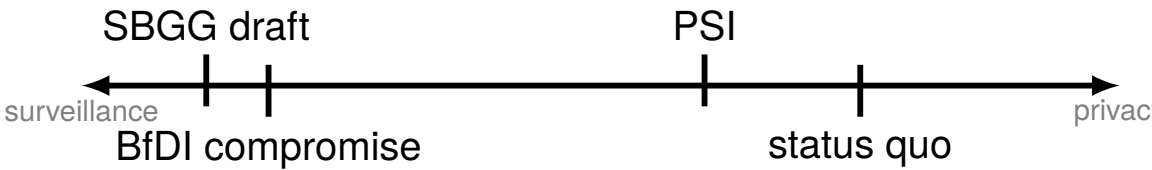
[TMS+22] A. Treiber, D. Müllmann, T. Schneider, and I. Spiecker genannt Döhmann. “Data Protection Law and Multi-Party Computation: Applications to Information Exchange between Law Enforcement Agencies”. *Workshop on Privacy in the Electronic Society (WPES)*. ACM, 2022

PSI Does Not Resolve All Concerns!

- Risk for people *in* LEA databases
- Automatizing surveillance mechanism, making surveillance more scalable
- Misuse harder to detect due to privacy guarantees
- Vulnerable ideal functionality:

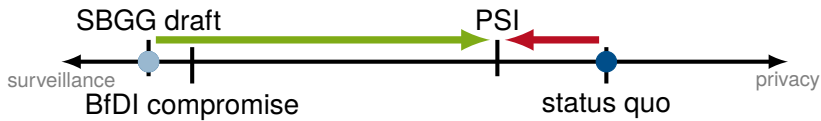


Spectrum of Possible Solutions



SBGG Saved Last Minute?

Sudden Removal of Planned Data Transfer



- § 13 para. 5 SBGG fully removed
- Reason: Avoid inconsistency
- Reasoning does not mention data protection
- Alongside: Plan to reintroduce data transfer for **all** name changes…
- …extending risks to, e.g., people with “foreign sounding” names

⇒ **Danger not eliminated, only delayed**

A Couple Notes on Interdisciplinary Research

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Interaction between law and cryptography unclear at many places
- Difficulties due to
  - different backgrounds
  - different terminology
  - different working & writing styles
- Political & ethical considerations
- Time required to establish a “common language”
  - Time investment vs fitting and good conference venue problematic for many PhD students
- Communicating the results

Takeaway 1

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

We need more interdisciplinary exchange and work!

Available cryptographic tools
unclear or unknown to lawmakers.

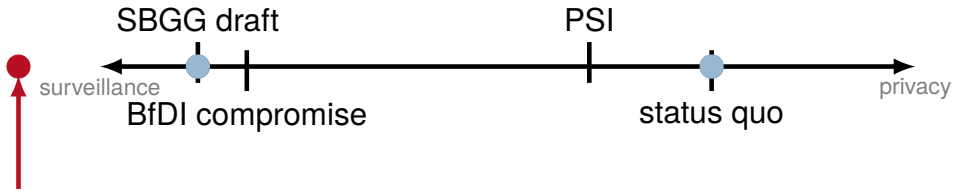
Takeaway 2

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

We should be wary about the risk of cryptographic tools
enabling/justifying processes that
should not be done at all!

Outlook

They Managed to Make it Worse [BMI25]



- Automatic data transfer and indefinite storage
- Only for the SBGG ⇒ Targeted at trans* people
- Gender entry crucial to identify people (ignoring and contradicting [BfDI23])
- “Alternatives: None”
- *But it is good for the environment*

[BfDI23] *Stellungnahme des BfDI zum SBGG-E*. 2023. URL: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2023/StgN_Selbstbestimmung-Geschlechtseintrag.pdf?__blob=publicationFile&v=2

[BMI25] Bundesministerium des Inneren. *Verordnungsentwurf zur Umsetzung des Gesetzes über die Selbstbestimmung in Bezug auf den Geschlechtseintrag im Meldewesen*. 2025. URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/VII2/RefE-VO-meldewesen-geschlechtseintrag.pdf?__blob=publicationFile&v=2

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Questions?

Paper (German)

http://dx.doi.org/10.18420/inf2024_11

Poster (English)

https://encrypto.de/papers/SBHS25Poster.pdf