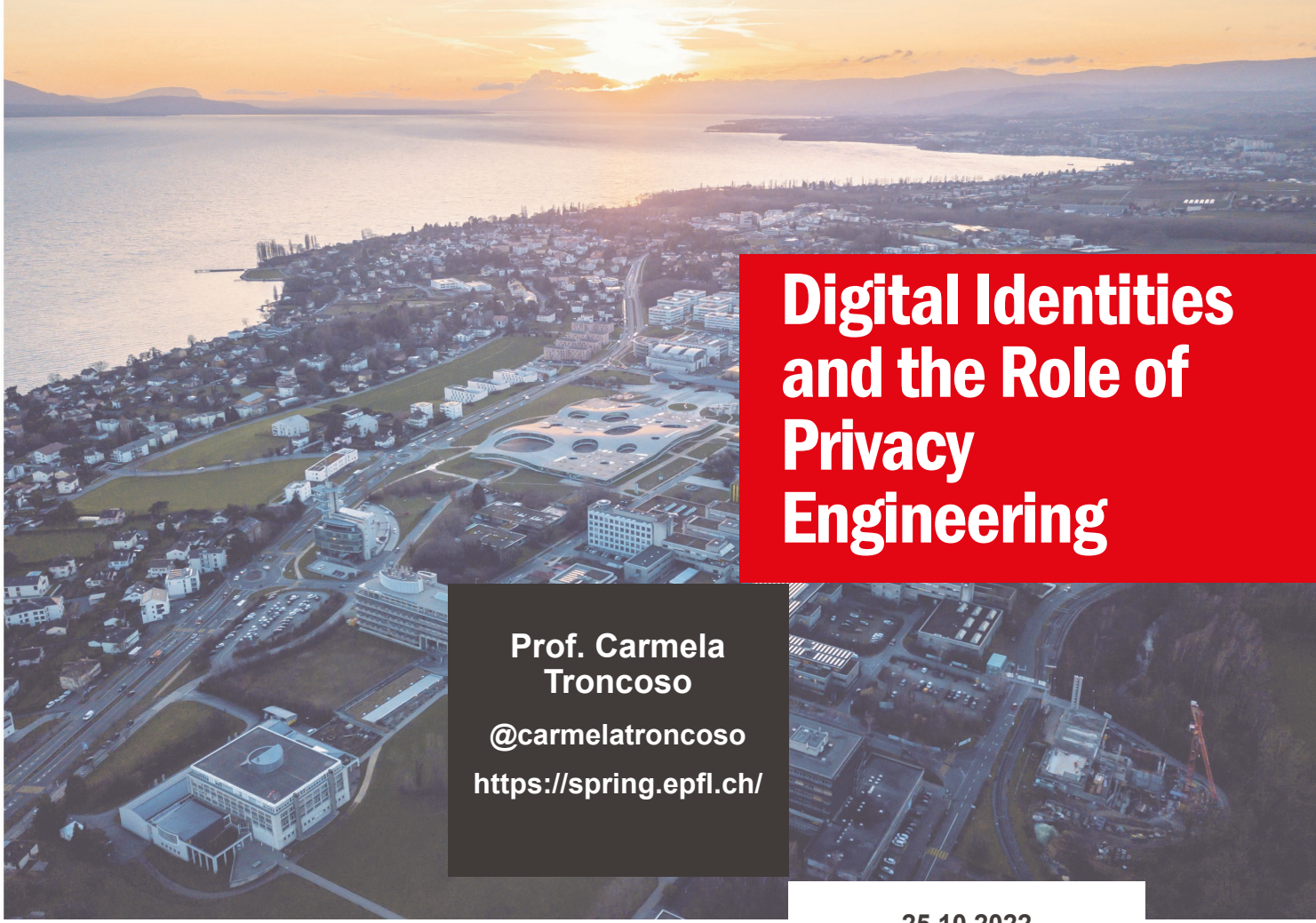


Digital Identities and the Role of Privacy Engineering

Prof. Carmela Troncoso

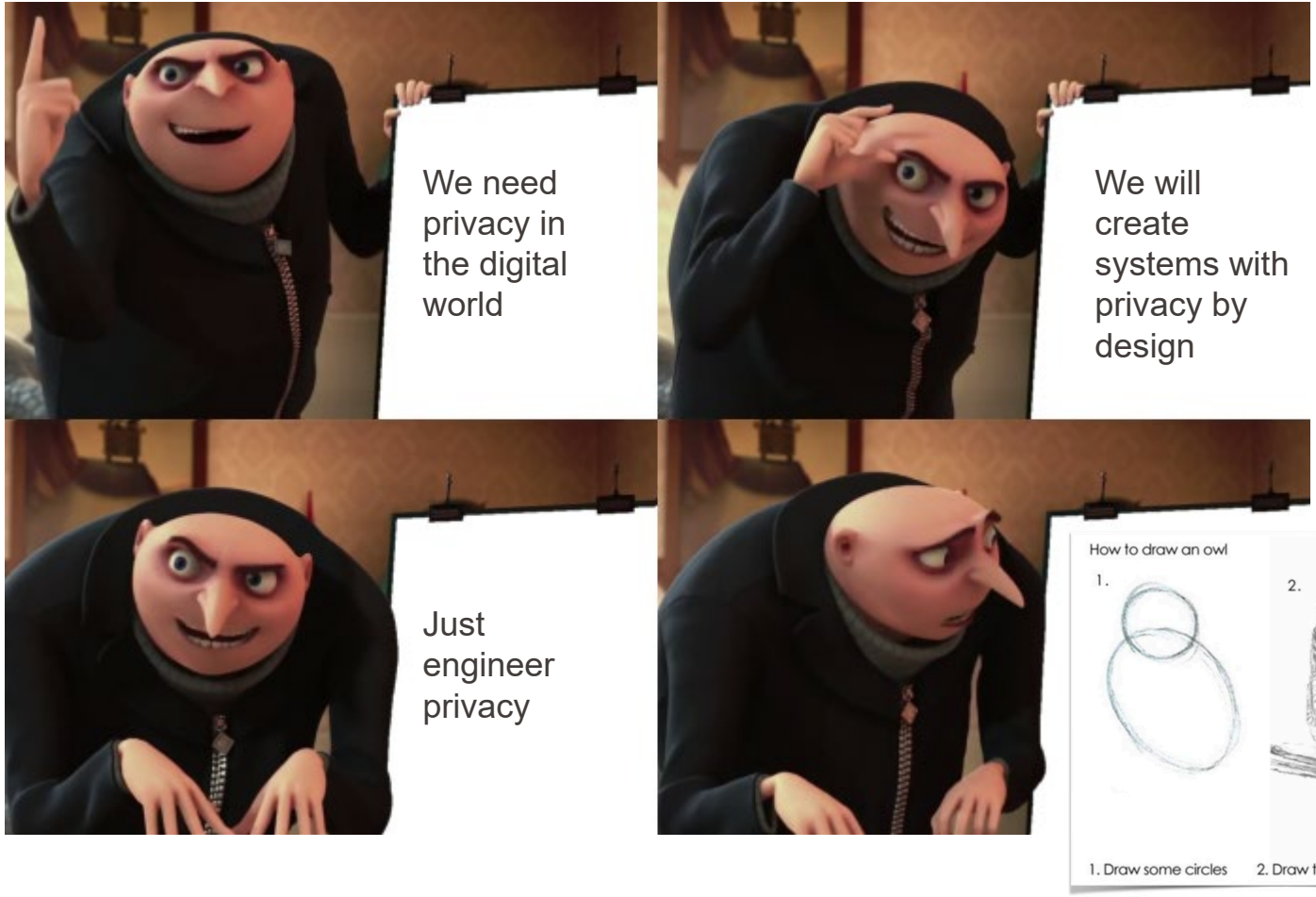
@carmelatroncoso

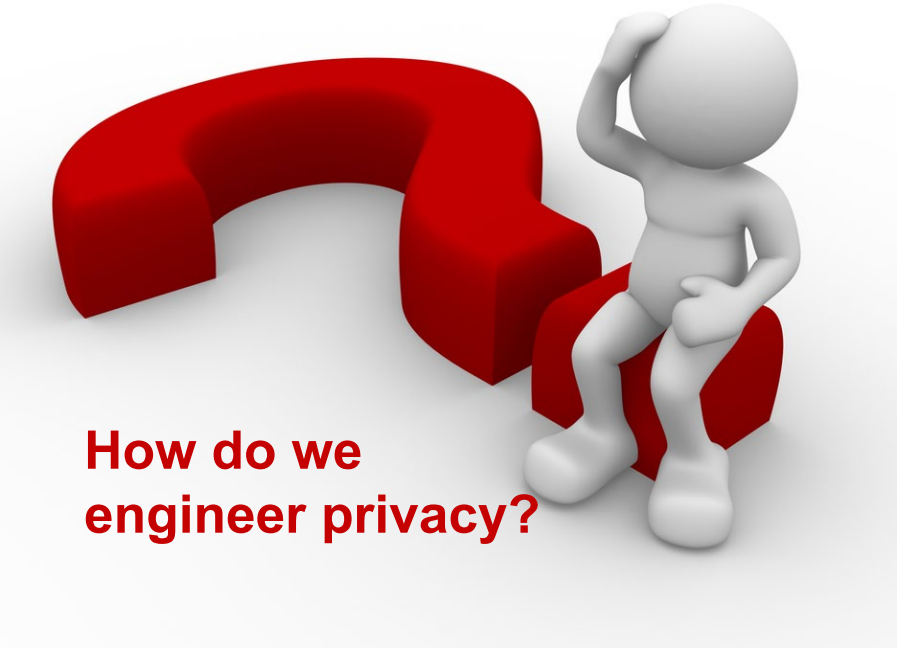
https://spring.epfl.ch/

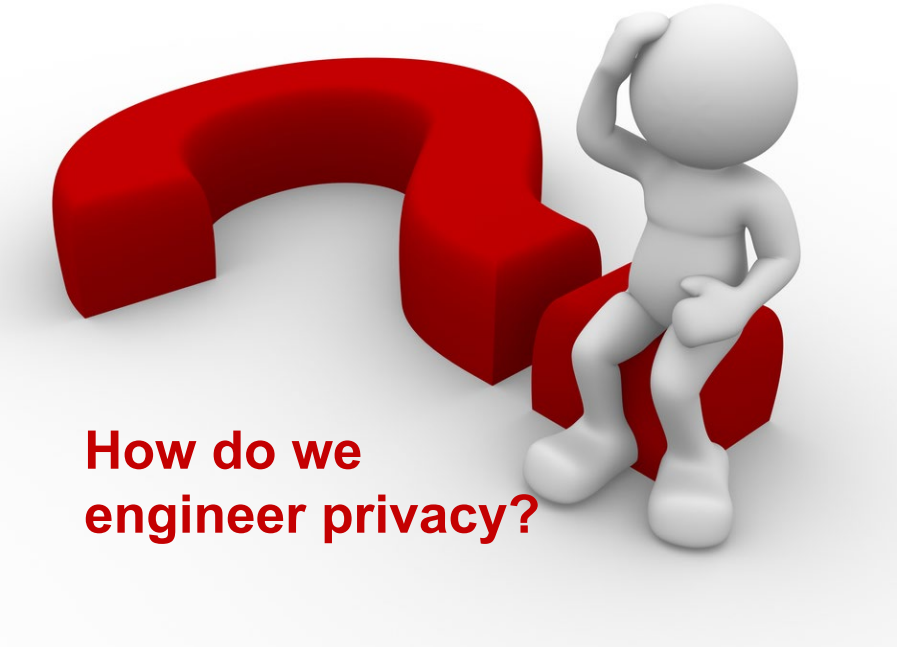
25.10.2022

École polytechnique fédérale de Lausanne


We need privacy in the digital world
We will create systems with privacy by design
Just engineer privacy


We need privacy in the digital world
We will create systems with privacy by design
Just engineer privacy
How to draw an owl
1.
2.
1. Draw some circles
2. Draw the rest of the **** owl


How do we
engineer privacy?



How do we engineer privacy?

Data minimization

- Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design.Computers, Privacy & Data Protection. 2011

Privacy as data minimization

The less data in the system, the more privacy-preserving it is

Clearly related to a regulation principle

- Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design Reloaded. Amsterdam Privacy Conference. 2015

Privacy as data minimization

The less data in the system, the more privacy-preserving it is
Clearly related to a regulation principle

but, **it's not "data" that is minimized** (in the system as a whole)
data is kept in user devices
sent encrypted to a server (only client has the key)
distributed over multiple servers
…

and, **no considerations on data use**

- Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design Reloaded. Amsterdam Privacy Conference. 2015

Privacy as data minimization

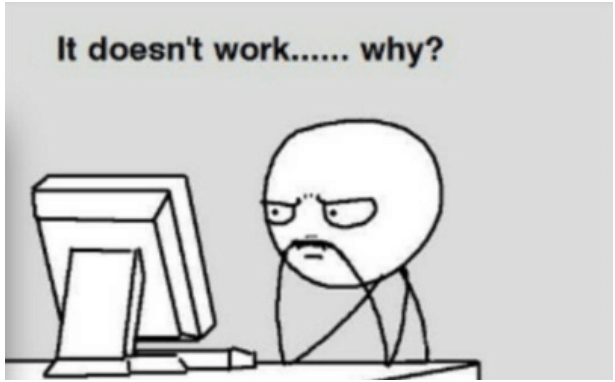
The less data in the system, the more privacy-preserving it is
Clearly related to a regulation principle

but, **it's not "data" that is minimized** (in the system as a whole)
data is kept in user devices
sent encrypted to a server (only client has the key)
distributed over multiple servers
…

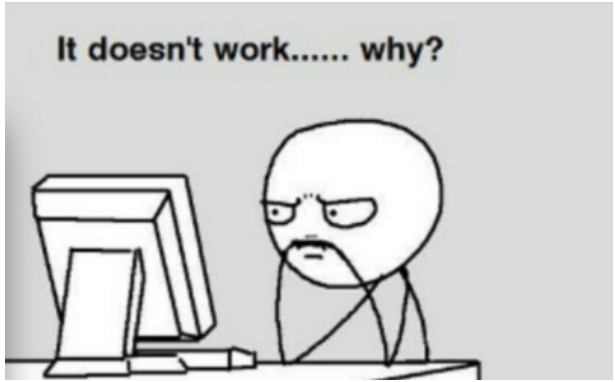
and, **no considerations on data use**

"data minimization" *on its own*
is a ***BAD*** *metaphor*
for privacy-preserving engineering

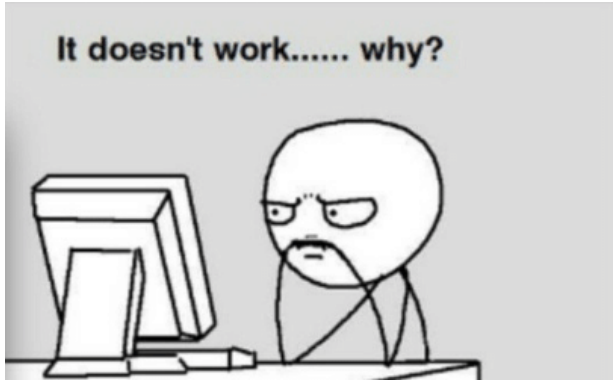
- Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design Reloaded. Amsterdam Privacy Conference. 2015


It doesn't work..... why?

Privacy is not the end goal

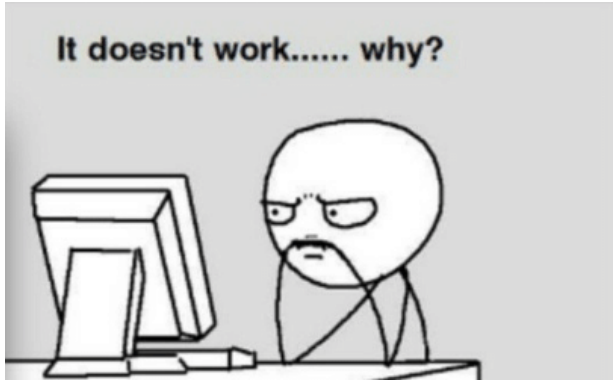


Privacy is not the end goal



Privacy **is a means** to protect
ourselves from
influence
intervention
manipulation
coercion
…

Privacy is not the end goal



Privacy **is a means** to protect
ourselves from
influence
intervention
manipulation
coercion
…

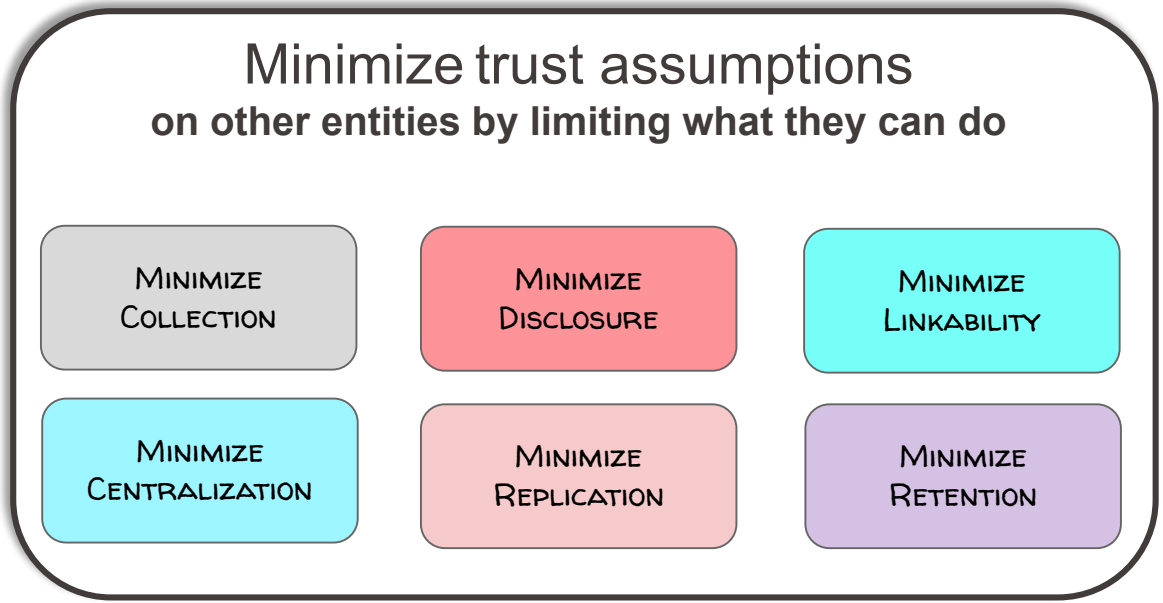
to keep our freedom

No need to trust the system
because
The system cannot misbehave

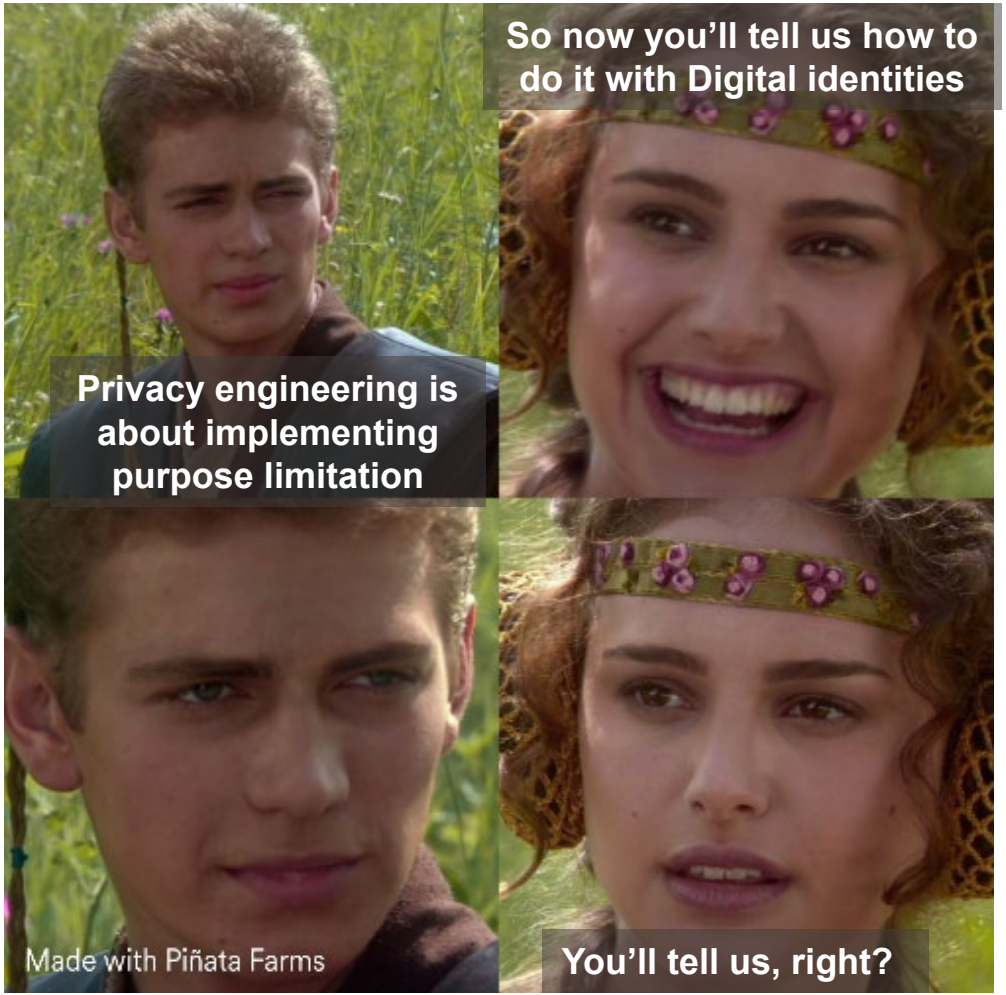
No need to trust the system
because
The system cannot misbehave

Purpose limitation is a GOOD metaphor for privacy-preserving
(data minimization is still necessary)

Towards purpose limitation



- Seda Gurses, Carmela Troncoso, Claudia Diaz. Engineering Privacy by Design Reloaded. Amsterdam Privacy Conference. 2015


So now you'll tell us how to do it with Digital identities
Privacy engineering is about implementing purpose limitation
Made with Piñata Farms
You'll tell us, right?

Digital identities are mostly linkable

Digital traces

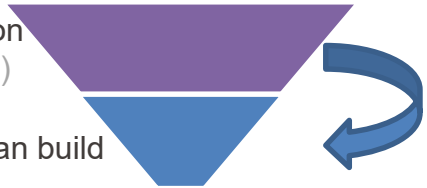
Profile

Cannot limit purpose!!

Privacy engineering requires new thinking

The Usual approach

Digitalize the offline solution
(as much data as possible)



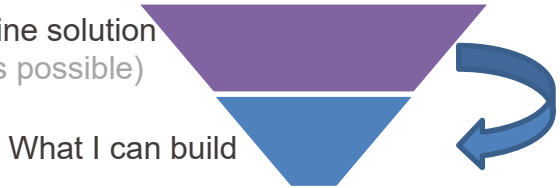
What I can build

Regulatory compliance
(e.g., data protection)

Privacy engineering requires new thinking

The Usual approach

Digitalize the offline solution
(as much data as possible)



What I can build

Regulatory compliance
(e.g., data protection)

The Privacy engineering approach

Operational purposes

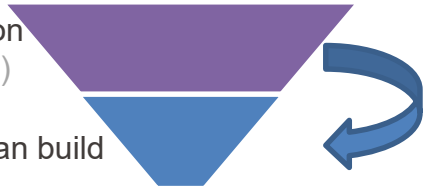
Minimal system to achieve **purpose**

What I need to build

Privacy engineering requires new thinking

The Usual approach

Digitalize the offline solution
(as much data as possible)



What I can build

Regulatory compliance
(e.g., data protection)

May not require an identity!

The Privacy engineering approach

Operational purposes

Minimal system to achieve **purpose**

What I need to build

Contact tracing apps

- **Purpose**: notify users of potential infection
- Does not matter who infects them – all infected people count the same
- Unlinkable Bluetooth random identifiers do the job
- Data exchanged in the system cannot be used for anything else
  - Only “useful” data is decentralized

Decentralized search engine

- **Purpose**: find documents of interest for investigations

- Who has the documents is not relevant
  - In fact hiding identities is necessary for safety!
- … but they need to be members of ICIJ

- Attribute-based credentials do the job!
  - Zero-knowledge proof of membership to organization

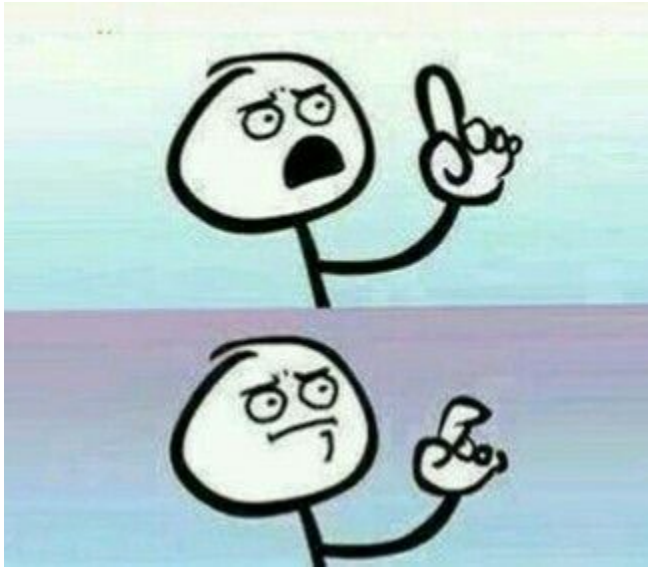
- Data in the system cannot be used to endanger journalist or their users

Safe and secure aid distribution

ICRC

- **Purpose**: distribute aid to those in need
- Make sure only registered beneficiaries receive the correct amount
  - It is not relevant who receives aid or when, only that it is correct
- Privacy-preserving audits and blacklisting
  - And decentralized biometric-based authentication
- Data in the system cannot be used to endanger beneficiaries

What if identity is needed for the purpose?



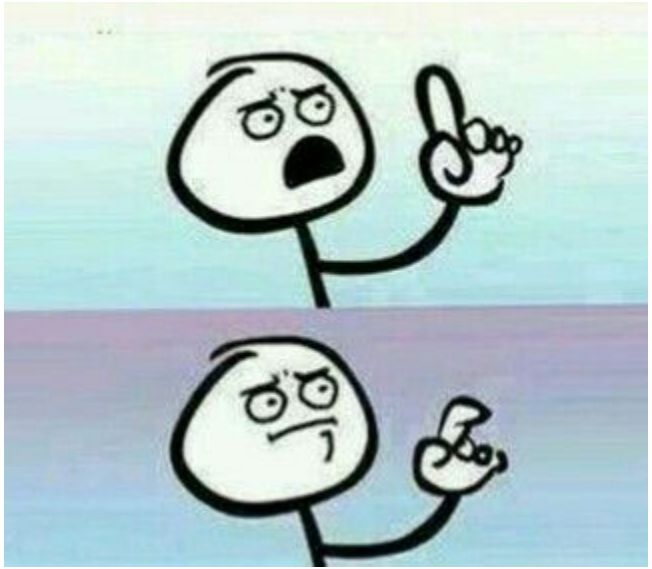
Is identity needed for the purpose

…or is it needed to enable multiple purposes?

Multi-purpose privacy-preserving engineering is close to impossible

It’s ok, just the system cannot give strong technical protection to users

What if identity is needed for the purpose?



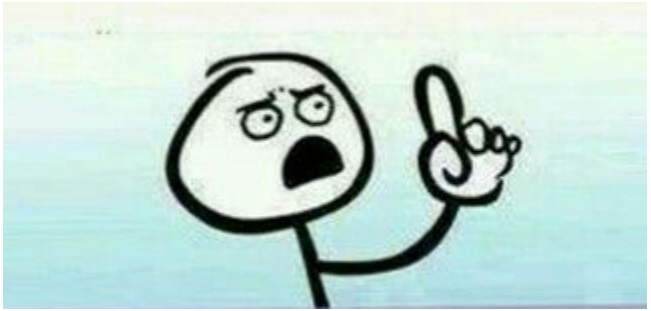
Is identity needed for the purpose

…or is it needed to enable multiple purposes?

Multi-purpose privacy-preserving engineering is close to impossible

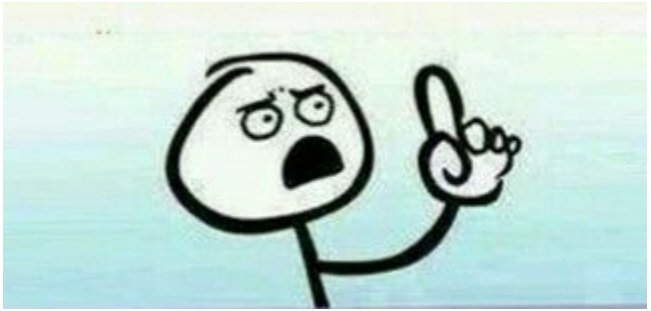
It’s ok, just the system cannot give strong technical protection to users

What if identity is needed for the purpose?



1. Think again! Is it actually needed?
   - If not, don’t use digital identities

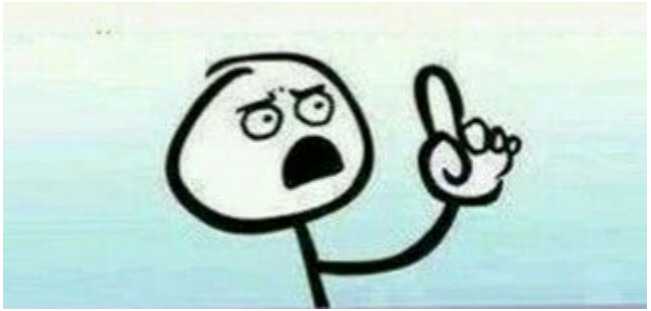
What if identity is needed for the purpose?



1. Think again! Is it actually needed?
   - If not, don't use digital identities

2. If identity truly is necessary
   - Reduce profiling by using PETs to avoid data disclosure/collection/centralization
   - Use PETs to create identities that minimize disclosure/collection/centralization

What if identity is needed for the purpose?



1. Think again! Is it actually needed?
   - If not, don't use digital identities
2. If identity truly is necessary
   - Reduce profiling by using PETs to avoid data disclosure/collection/centralization
   - Use PETs to create identities that minimize disclosure/collection/centralization
3. Think again if identity was really needed…

Key takeaways

- Privacy engineering is about
  - Minimizing trust – through **purpose limitation**
  - Identifying architectures and technologies that enforce this purpose limitation
- Digital identities are most times **not** needed when building systems following privacy engineering
- The more purposes a system has, the harder it is to limit the purpose of the system
  - Privacy engineering cannot do miracles