institute iMdea software

NEXTLEAP
H2020-ICT-15 GA 688722

Engineering Privacy by Design *Reloaded*

Seda Gürses[1], Carmela Troncoso[2], Claudia Diaz[3]

[1] New York University / Princeton University
[2] IMDEA Software Institute
[3] KU Leuven

Privacy by Design – Let's have it!

Information and Privacy Commissioner of Ontario

Privacy by Design

Privacy by Design principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. **Privacy Embedded into Design**
4. Full Functionality: Positive-Sum, not Zero-Sum
5. End-to-End Security — Full Lifecycle Protection
6. Visibility and Transparency — Keep it Open
7. Respect for User Privacy — Keep it User-Centric

Cavoukian et al. (2010)

Article 25 European General Data Protection Regulation

GDPR

EU General Data Protection Regulation

"the controller shall [...] implement appropriate technical and organisational measures [...] which are designed to implement data-protection principles[...] in order to meet the requirements of this Regulation and protect the rights of data subjects."

🤔 Actually... "Data Protection by design and by default"

BUT HOW ???????????

https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Engineering PbD 1.0

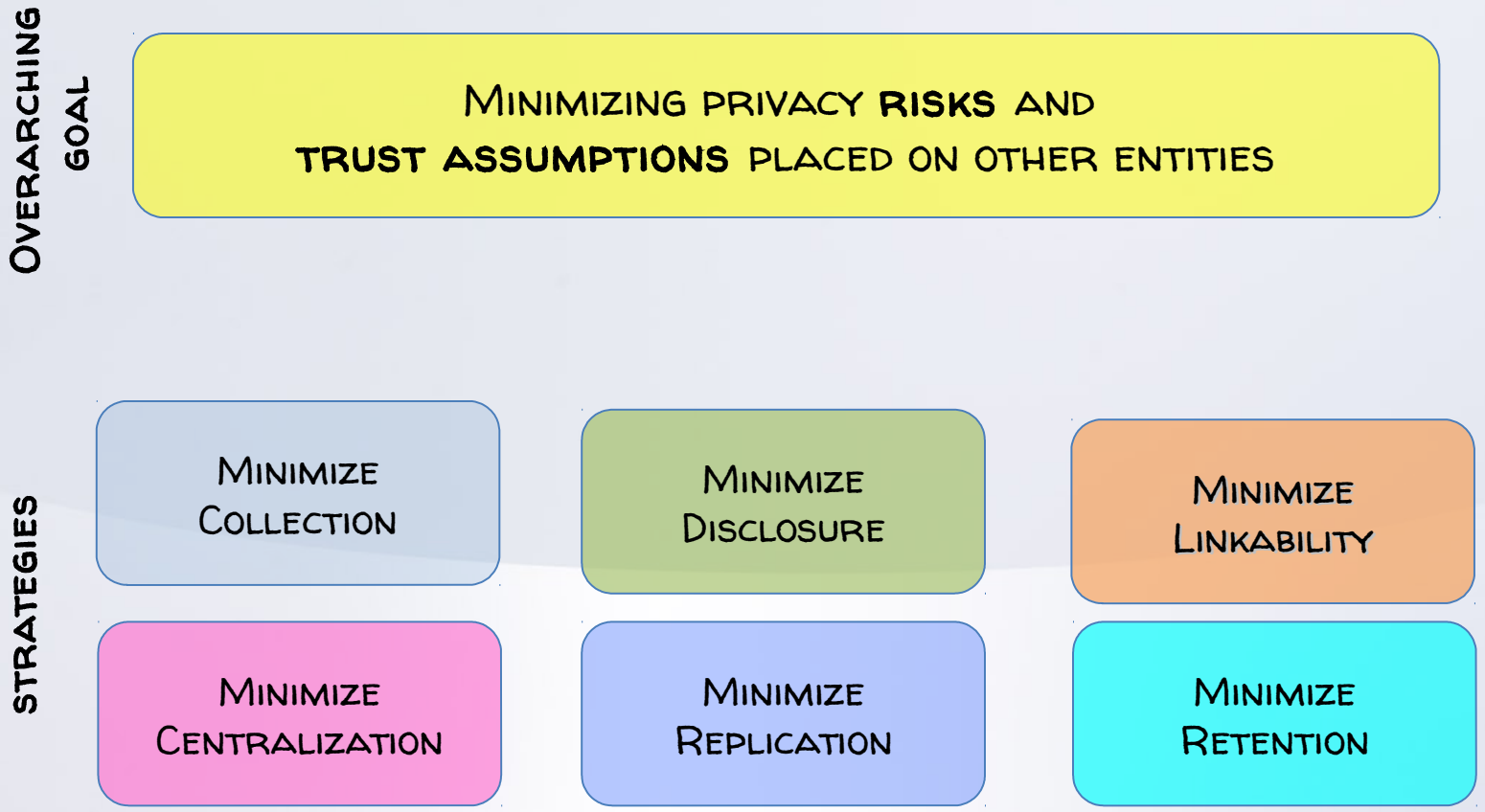
- "The key is *data minimization*"
  - Two case studies:
    - anonymous e-petitions: no identity attached to petitions
    - privacy-preserving road tolling: no fine grained data
- **BUT**, it's not "data" that is minimized (in the system as a *whole*)
  - kept in user devices
  - sent encrypted to a server (only client has the key)
  - distributed over multiple servers: only the user, or colluding servers, can recover the data

"DATA MINIMIZATION" IS A BAD METAPHOR!!!

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

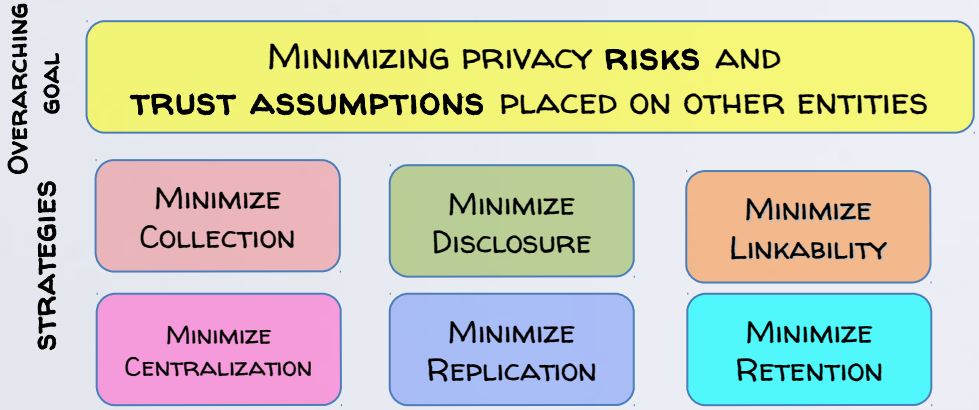
Privacy by Design Strategies

[Strategies (abstract approaches) vs patterns (recurring solutions – implemented by PETs)]



Hoepman, Jaap-Henk. "Privacy design strategies." ICT systems security and privacy protection. Springer Berlin Heidelberg, 2014. 446-459.

Great! but again... how do I use these strategies?



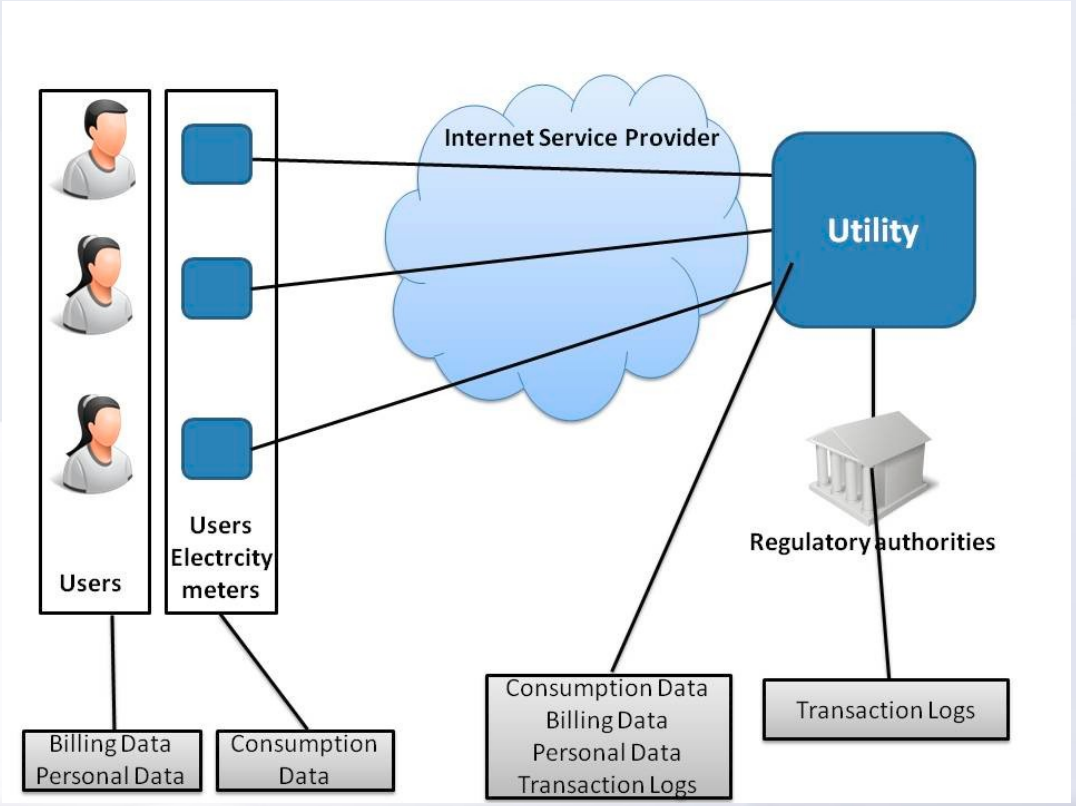
- No existing methodology... is privacy engineering practice: a craft?
  - We look at privacy/ security engineer
  - We try to make explicit the activities in their **design** process

    ("Activities" not disjoint, not ordered, multiple iterations)

Out of scope: requirements elicitation, software implementation and maintenance

Starting Assumptions

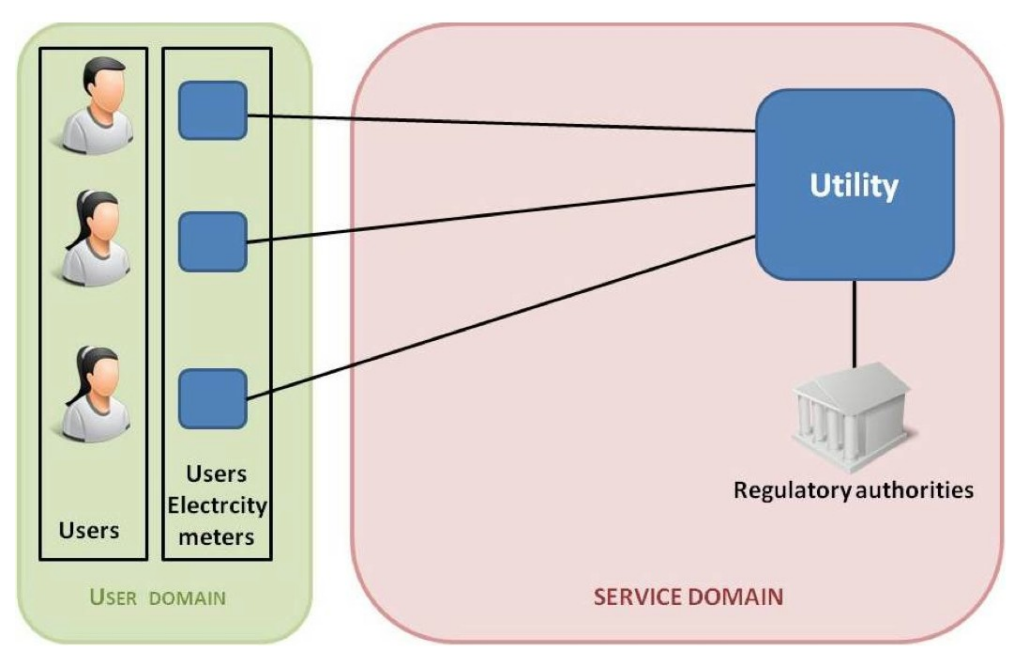
- Functionality is well defined
- Basic system and information models exist
- Stakeholders and privacy & service integrity requirements are elicited
- Initial reference system



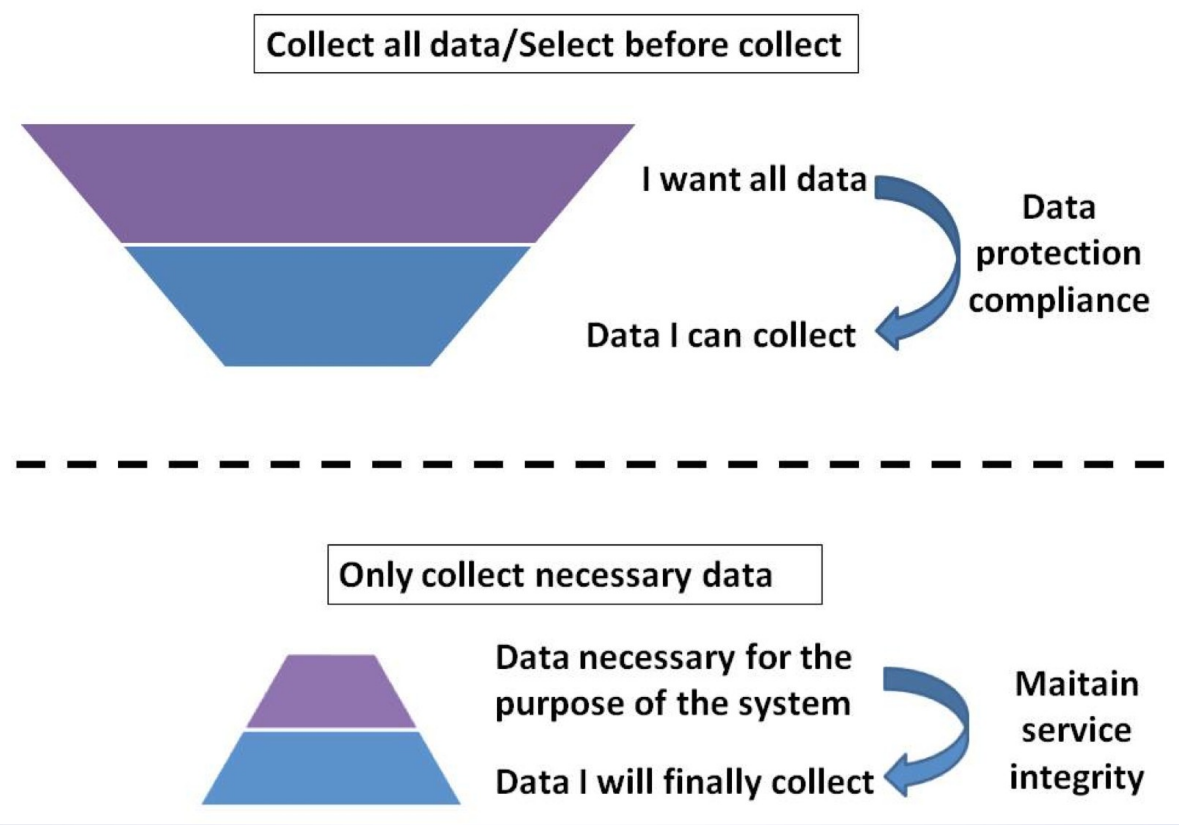
Activity 1: Classify Entities in domains

User domain: components under the control of the user, eg, user devices

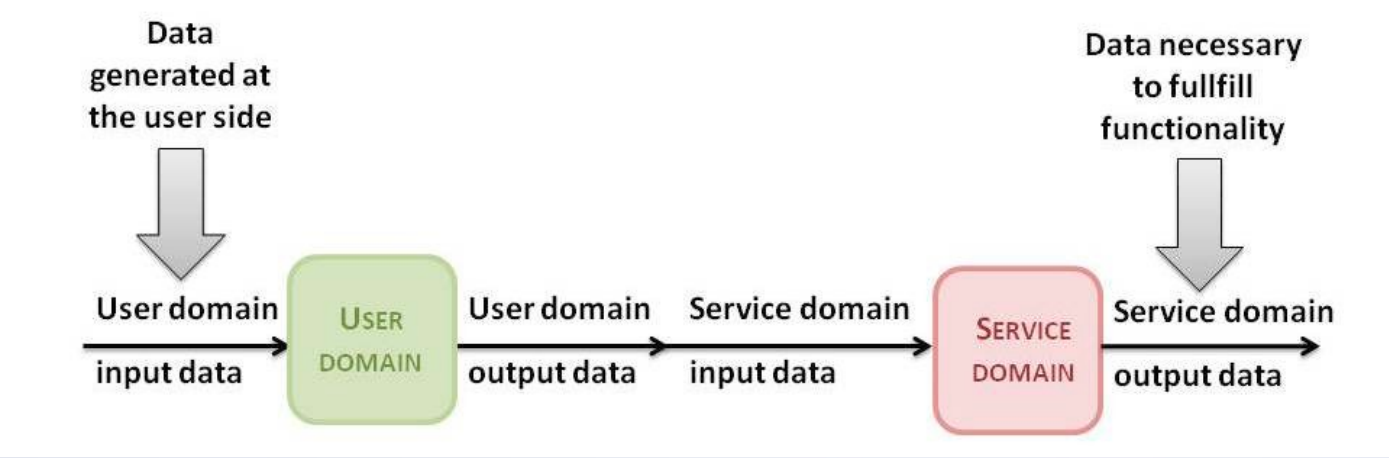
Service domain: components outside the control of the user, eg, backend system at provider



Activity 2: Identification of Necessary data



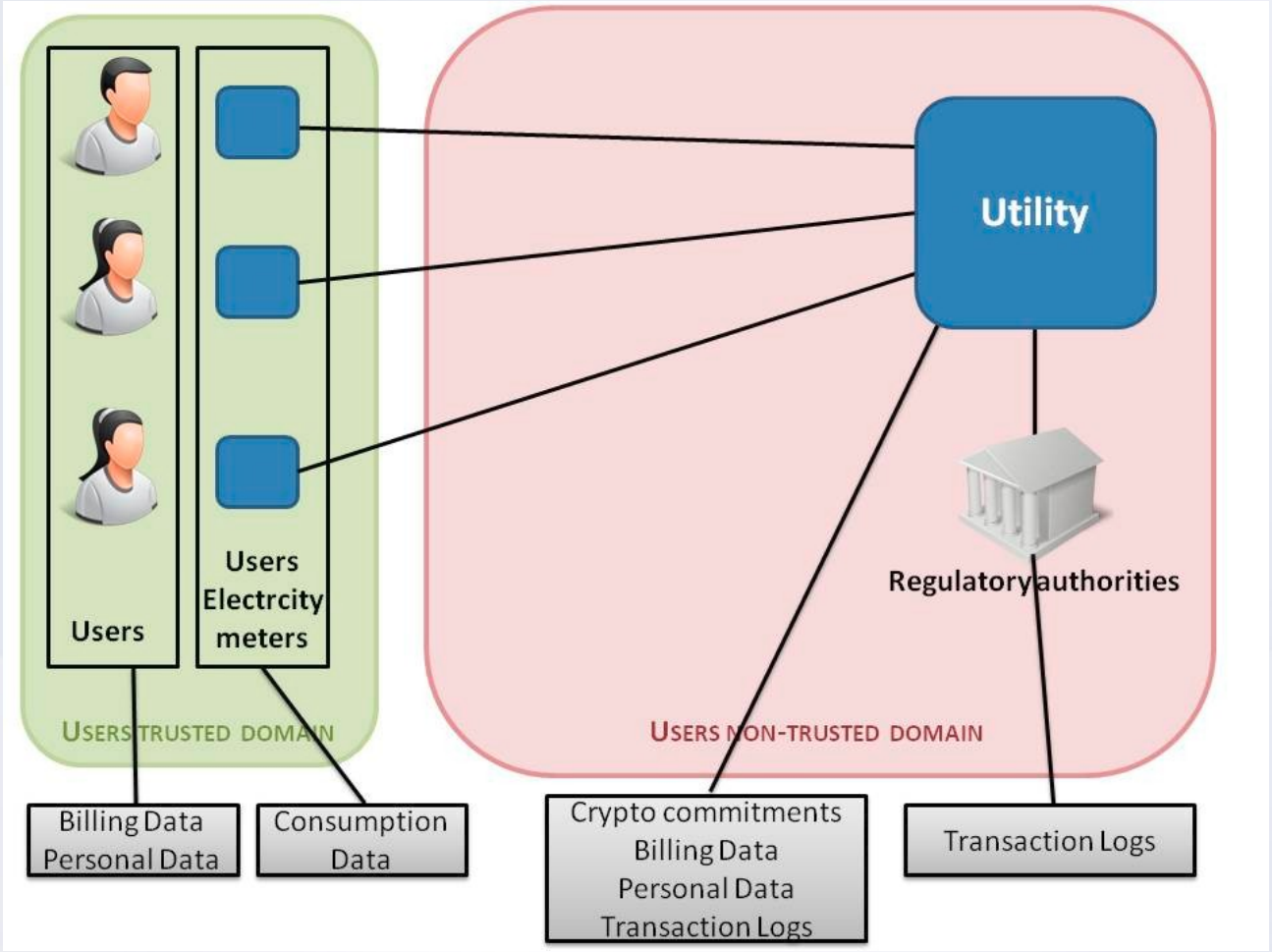
Activity 3: Distribution of data in the architecture



Data necessary at the User Domain: data that needs to exist so that the entities in this domain can produce adequate inputs to the Service domain

Data necessary at the Service Domain: data that must flow in order for the entities in this domain to be able to carry out operations for achieving the functionality of the system.

Activity 3: Distribution of data in the architecture

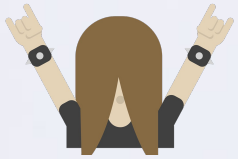


Activity 4: Select technological solutions (Patterns)

- ... that keep as much data as possible out of the service domain while satisfying service integrity requirements
  - not sending the data (local computations)
  - encrypting the data
  - advanced privacy-preserving protocols
  - obfuscate the data
  - anonymize the data

In summary

Privacy by design rocks!



But it is not clear how we make it a reality...

Introspection on privacy engineers activities → Explicit activities

A long, long way to go:

Who establishes requirements?

How do we evaluate privacy?

How do we turn activities into a fully fledged methodology?

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J. H., Metayer, D. L., Tirtea, R., & Schiffner, S. (2015). Privacy and Data Protection by Design-from policy to engineering. arXiv preprint arXiv:1501.03726.

institute imdea software

NEXTLEAP
H2020-ICT-15 GA 688722

THANKS!

ANY QUESTIONS?

More about privacy: https://www.petsymposium.org/

carmela.troncoso@imdea.org
https://software.imdea.org/~carmela.troncoso/
(these slides will be there soon)

Template: http://www.brainybetty.com/
Figures: SlidesCarnival