UMBC
Dr. Roberto Yus
https://robertoyus.com/

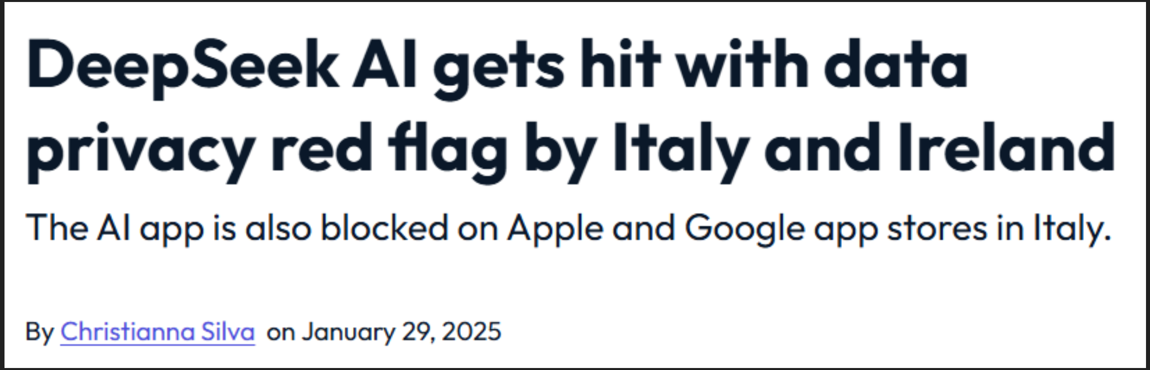
Data Privacy

CMSC 463/663

L02 – Privacy by Design

Previously on…

- Privacy, private information / personal data / PII, privacy principles
- Data Privacy regulations, GDPR



DeepSeek AI gets hit with data privacy red flag by Italy and Ireland

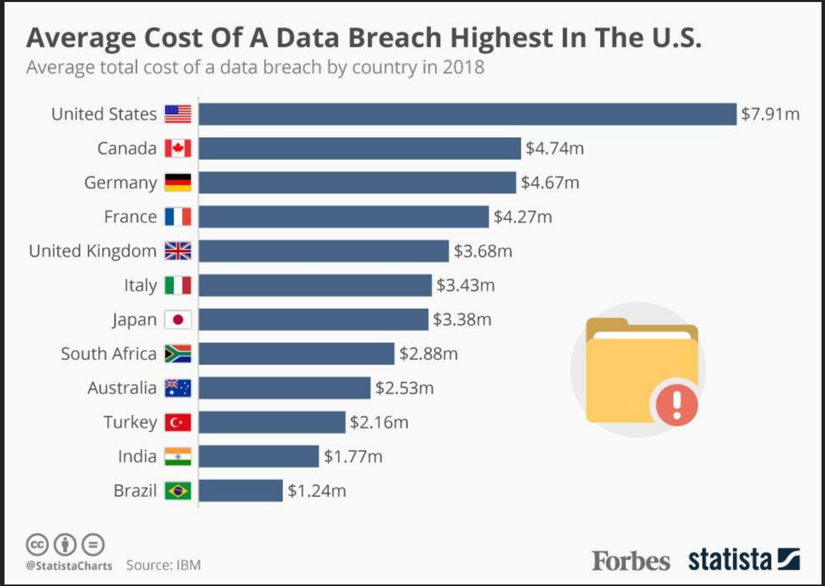
The AI app is also blocked on Apple and Google app stores in Italy.

By Christianna Silva on January 29, 2025

In the news!

Motivation for Adopting Privacy Principles

- Regulations
- **Costs!**
  - Proactive – Reactive
  - Legal liabilities, class action suits
  - Loss of client confidentially and trust
  - Damage to brand’s reputation
  - Loss of costumers and/or competitive edge
  - …



Average Cost Of A Data Breach Highest In The U.S.

Average total cost of a data breach by country in 2018

Source: IBM

Icons from https://thenounproject.com/

Privacy by Design (PbD)

- Approach to systems engineering
- Developed by Ann Cavoukian
- Framework published in 2009
- Calls for **privacy to be taken into account throughout the whole engineering process**.
- The GDPR incorporates Privacy by Design

Foundational Principles

1. **Proactive not reactive**; preventive 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

*"[…] these principles remain **vague** and leave many open questions about their application when engineering systems."* - Gurses et al (2011)

But how?!

The 7 Principles: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

Gürses, Seda, Carmela Troncoso, and Claudia Diaz. "Engineering privacy by design." *Computers, Privacy & Data Protection* 14 (2011).

Case Study: Electronic Toll Pricing

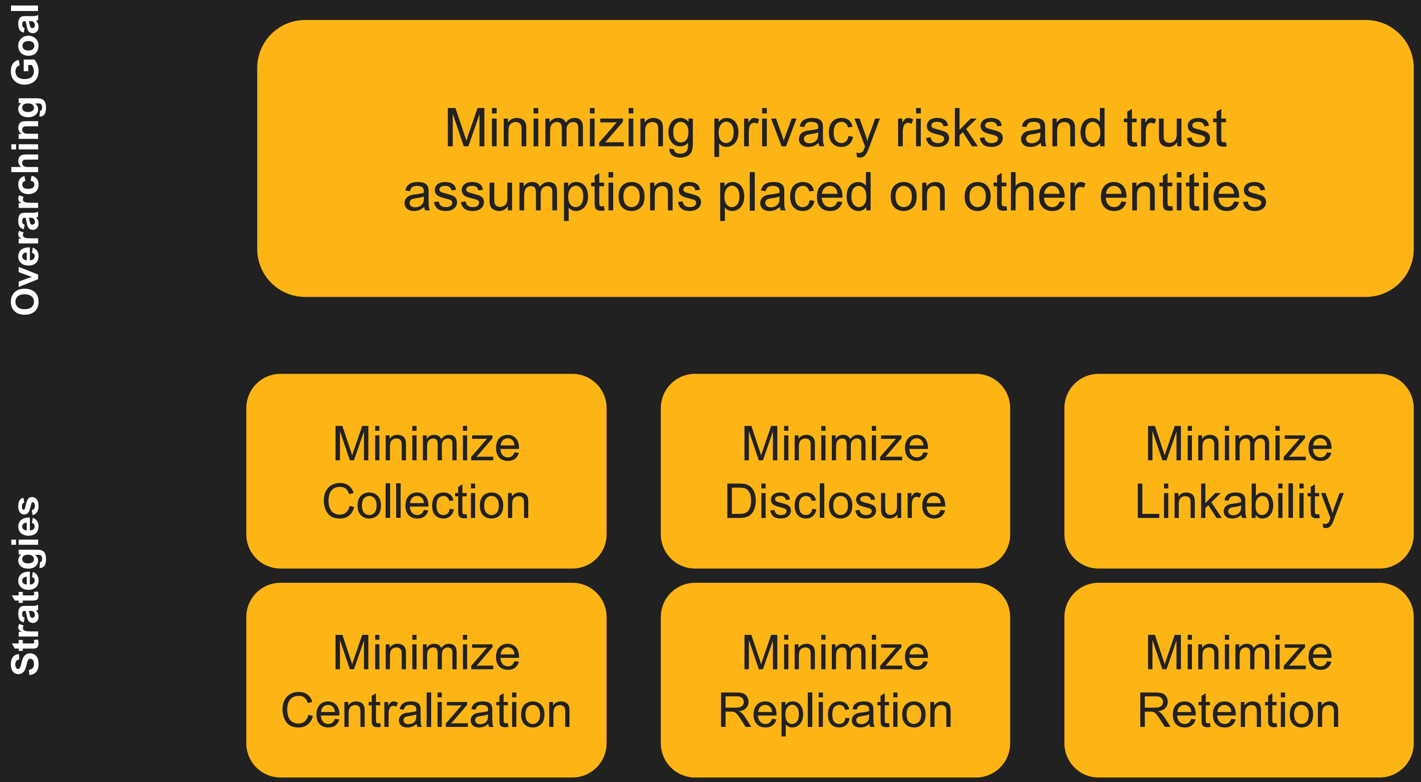
- Pay according to road use: time, distance, type or road, congestion.

- Requirements:
  - “the provider needs to know the final fee to charge;”
  - “the provider must be reassured that this fee is correctly computed and users cannot commit fraud”
  - Note: location as a means to the above -> not intrinsic.

- Privacy risks:
  (1) Third party access to traffic / location data of driver.
  (2) Abuse of traffic data by authority performing the billing.
  (location data cannot be easily anonymized)

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Data Minimization Strategies



Overarching Goal

Minimizing privacy risks and trust assumptions placed on other entities

Strategies

Minimize Collection

Minimize Disclosure

Minimize Linkability

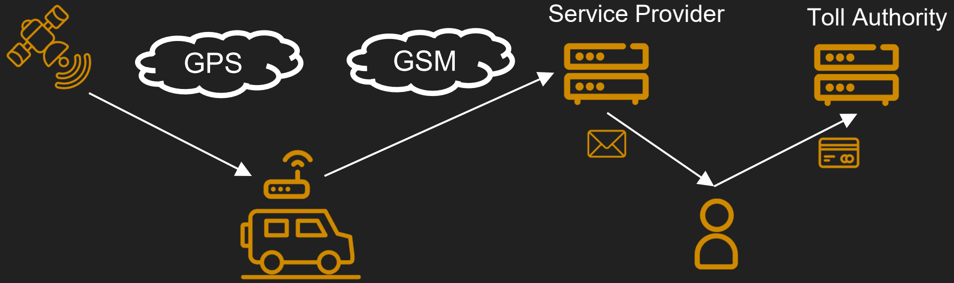
Minimize Centralization

Minimize Replication

Minimize Retention

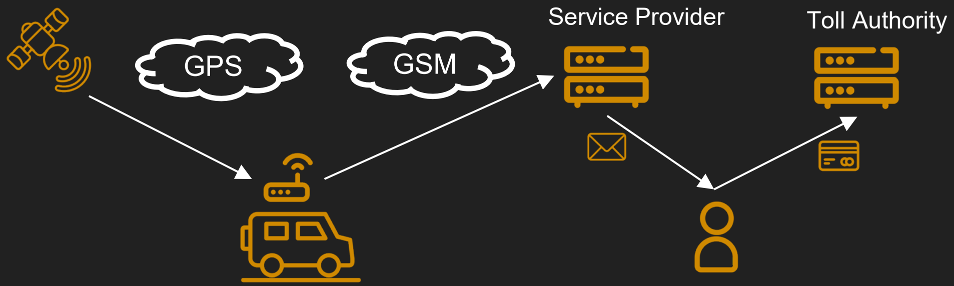
J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing



J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing

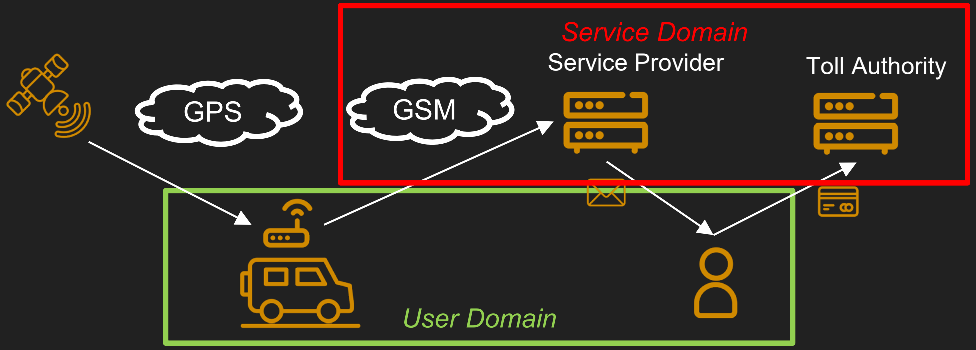


Activity 1: **Classify Entities in Domains**

- User Domain: components under user control (e.g., user devices)
  Service Domain: components outside of user control (e.g., backend server at service provider)

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing

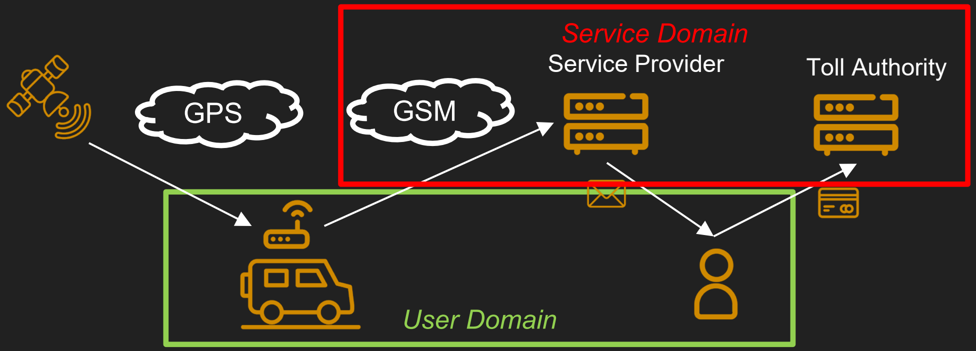


Activity 1: **Classify Entities in Domains**

- User Domain: components under user control (e.g., user devices)
  Service Domain: components outside of user control (e.g., backend server at service provider)

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing



Activity 1: **Classify Entities in Domains**

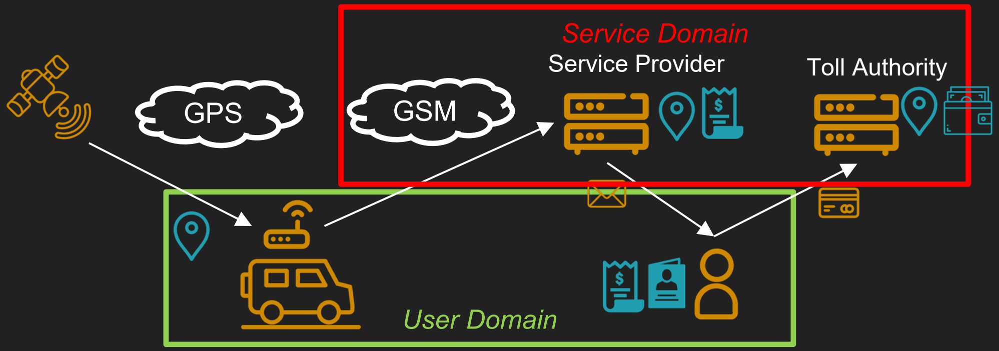
- User Domain: components under user control (e.g., user devices)
  Service Domain: components outside of user control (e.g., backend server at service provider)

Activity 2: **Identify Necessary Data to Provide Service**

- Location Data → Compute Bill
- Billing Data → Charge User
- Personal Data → Send Bill
- Payment Data → Perform Payment

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing



Activity 1: **Classify Entities in Domains**

- User Domain: components under user control (e.g., user devices)
  Service Domain: components outside of user control (e.g., backend server at service provider)

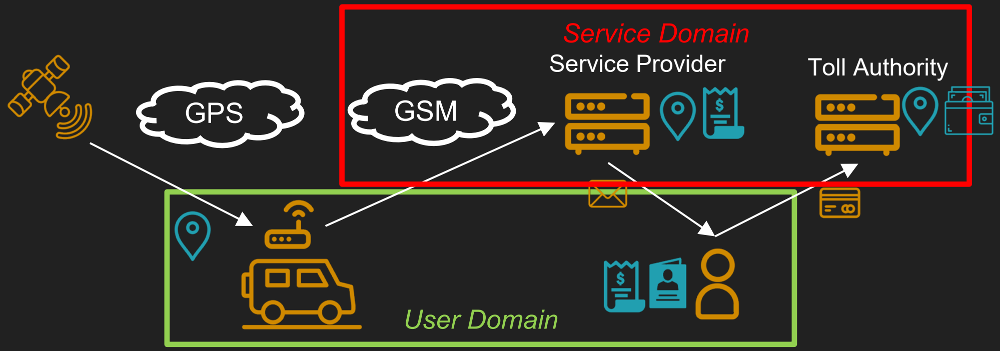
Activity 2: **Identify Necessary Data to Provide Service**

- Location Data → Compute Bill
- Billing Data → Charge User
- Personal Data → Send Bill
- Payment Data → Perform Payment

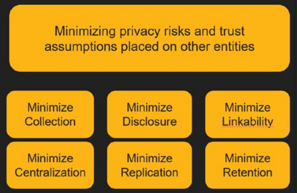
Activity 3: **Distribute Data in Architecture**

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing



Activity 4: **Select Technological Solutions following** →

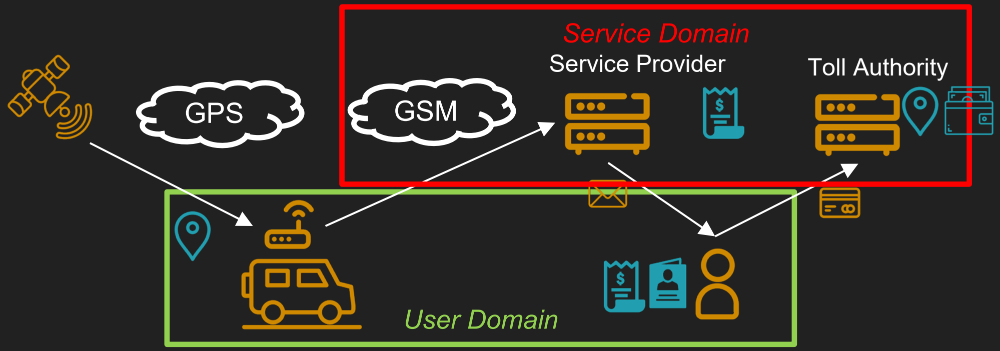


Minimizing privacy risks and trust assumptions placed on other entities

Minimize Collection	Minimize Disclosure	Minimize Linkability
Minimize Centralization	Minimize Replication	Minimize Retention

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Case Study: Electronic Toll Pricing



Activity 4: **Select Technological Solutions following** →

- Not sending the data (local computations)
- Encrypting the data
- Advanced privacy preserving protocols
- Obfuscate the data
- Anonymize the data

Minimizing privacy risks and trust assumptions placed on other entities

Minimize Collection

Minimize Disclosure

Minimize Linkability

Minimize Centralization

Minimize Replication

Minimize Retention

Requires deep knowledge of PETs!

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede. PrETP: Privacy-preserving electronic toll pricing. In 19th USENIX Security Symposium, 2010.

Privacy Engineering (Gurses et al, 2011)

- Process:
  - **Functional Requirements Analysis**:
    (Vague requirements lead to privacy problems.)
  - **Data Minimization:**
    (Identity or data not always necessary)
  - **Modelling Attackers, Threats and Risks**
    (Which parties have incentives to be hostile to the requirements)
  - **Multilateral Security Requirements Analysis**
    (Conflicting / contradicting security requirements of all parties)
  - **Implementation and Testing of the Design**

Crucial

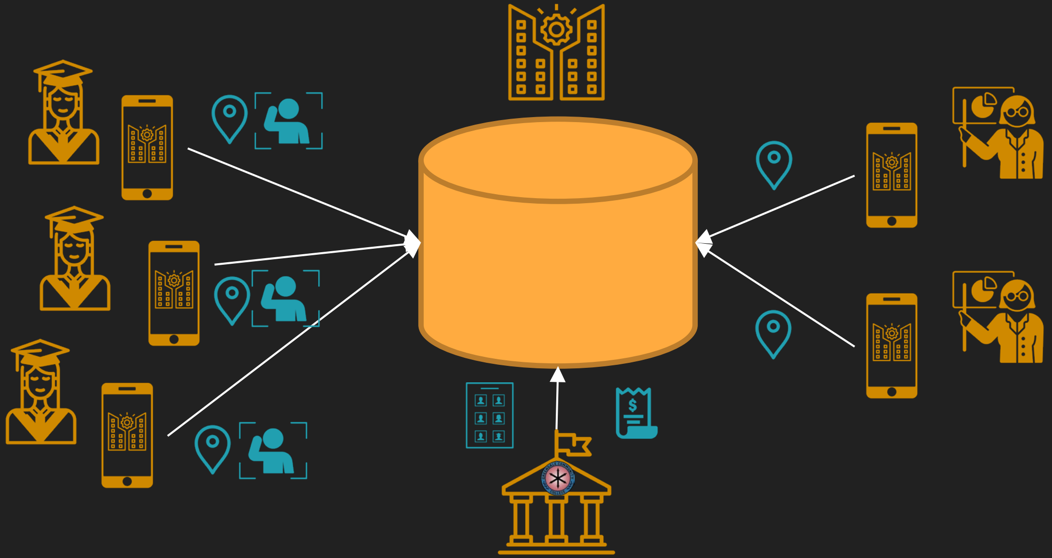
Iterate all

"If the functionality was not properly delimited in our case studies, even following our methodology, we would be forced to go for a centralized approach collecting all the data" -- Gurses et al 2009.

Discussion

Case Study: Pay and earn what is fair

- Greendale Community College (GCC) wants to implement a new system:
  - Students pay only for the classes they attend
  - Faculty salary depends on how many students attend their classes
  - Nobody can commit fraud!
  - ….



Unlimited Data Analytics!
(pose any SQL query)
Encryption
User Authentication
…