Privacy in Connected Vehicles: Perspectives of Drivers and Car Manufacturers

Summer SOC 2023

Andrea Fieschi

28.06.2023

Mercedes-Benz AG, Universität Stuttgart

A. Fieschi, Y. Li, P. Hirmer, C. Stach, B. Mitschang

Known potential of collecting data from cars

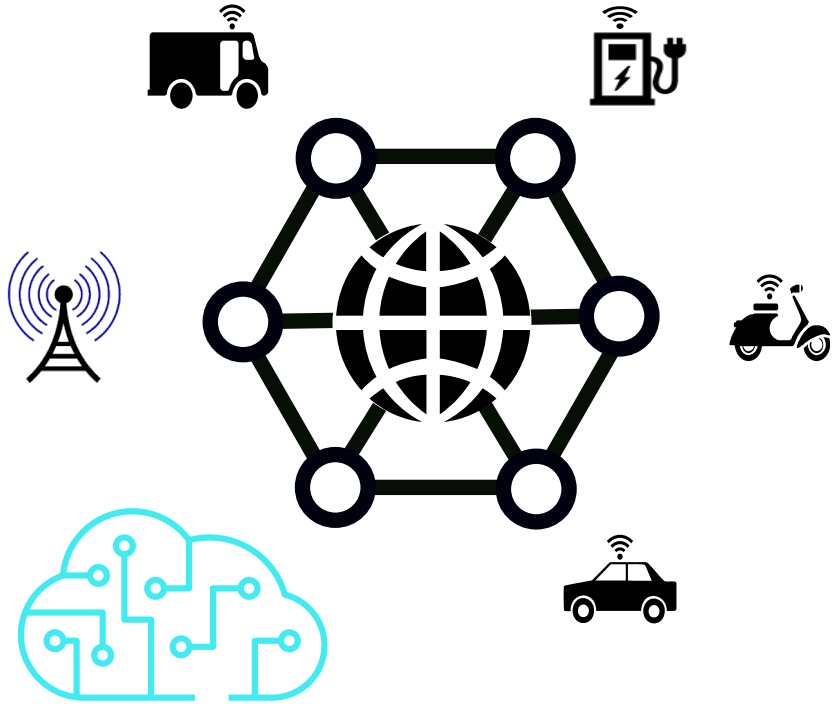
- Autonomous driving
- Diagnostic
- Real world experience
- Infotainment services
- Etc.

Data and the Connected Vehicle Environment (CVE)

A network of possibilities

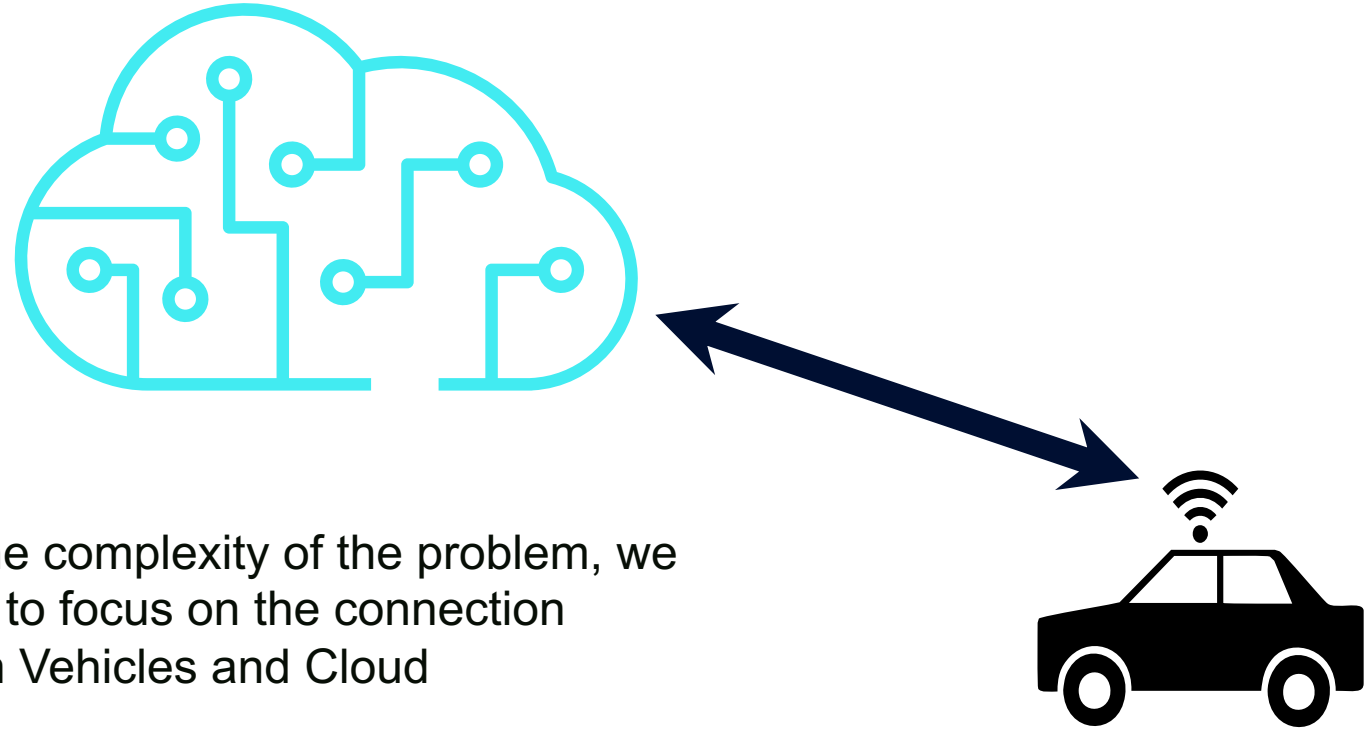
The full connected vehicle environment includes:

- Vehicles
- Road Side Units (RSUs)
- Cloud



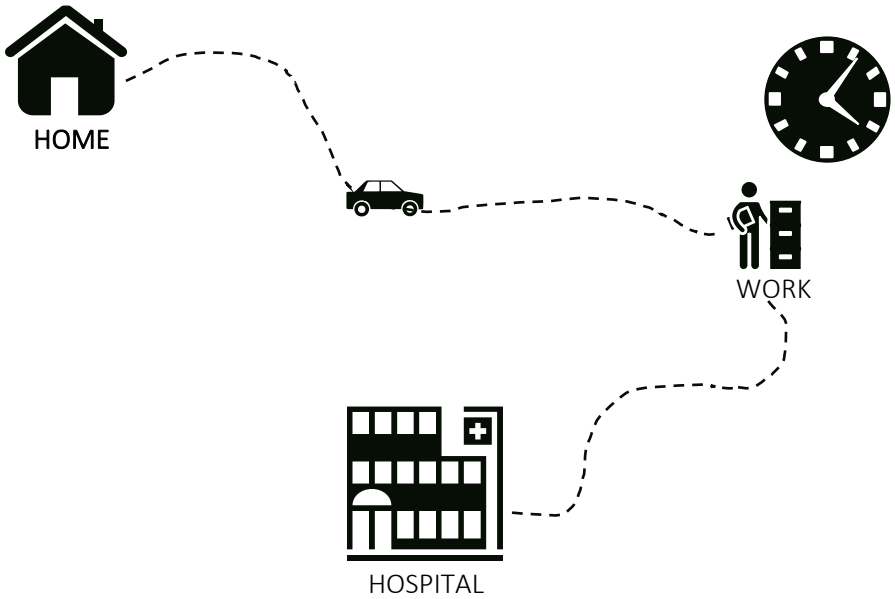
Connected Vehicles

Focus of this work



Given the complexity of the problem, we decided to focus on the connection between Vehicles and Cloud

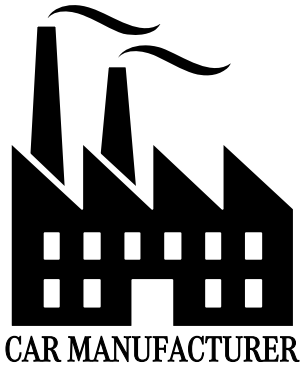
Cars are strongly connected to Driver's actions and habits



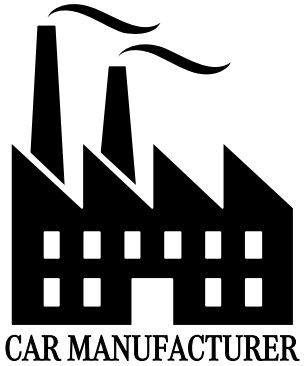
PRIVACY ISSUES

Car Manufacturer, Drivers, and Privacy

Or Service Provider, User, and Privacy

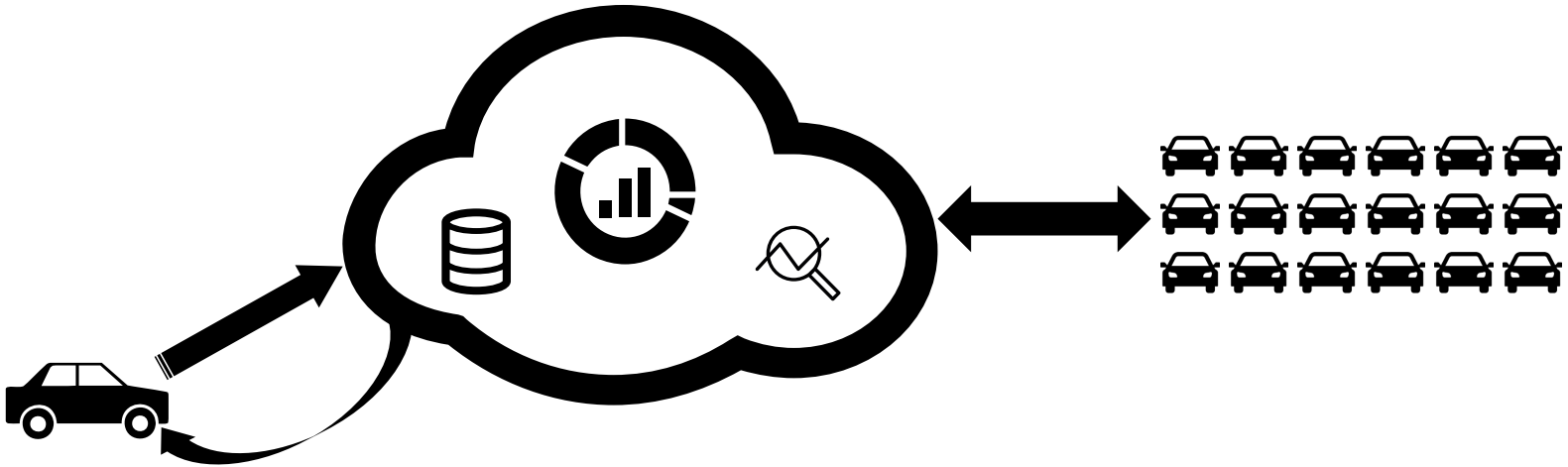


Car Manufacturer‘s Perspective



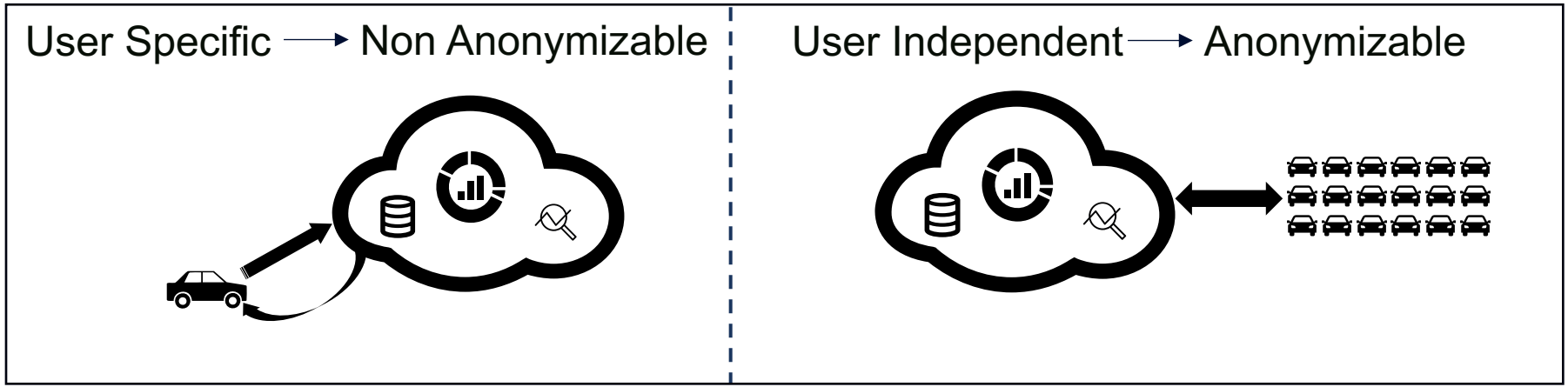
Car Manufacturer‘s Perspective

Data Flow and Services



Car Manufacturer‘s Perspective

Challenges



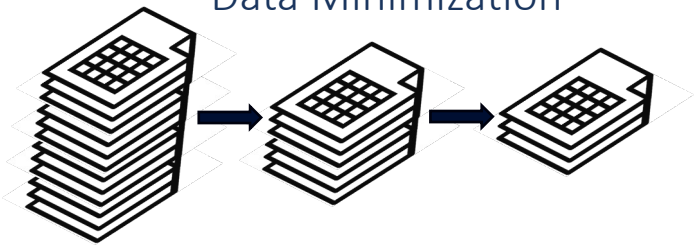
- Privacy needs specific to every use case (no one-rule-fit-all)

- Privacy concerns also extend to individuals near the vehicle

Car Manufacturer‘s Perspective

Possible Data Protection Approaches

Data Minimization

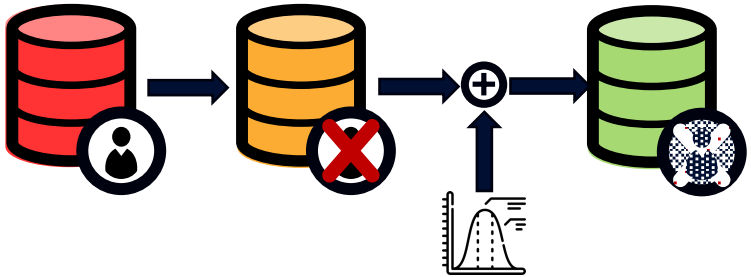


Data Suppression

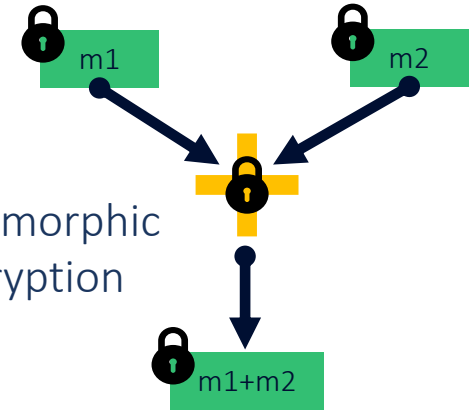
Location
Paris
Nice
Munich
Munich

Location
France
France
Germany
Germany

Differential Privacy



Homomorphic Encryption

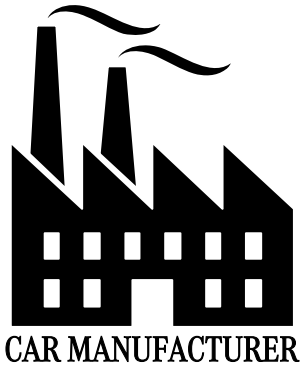


Car Manufacturer‘s Perspective

Approaches

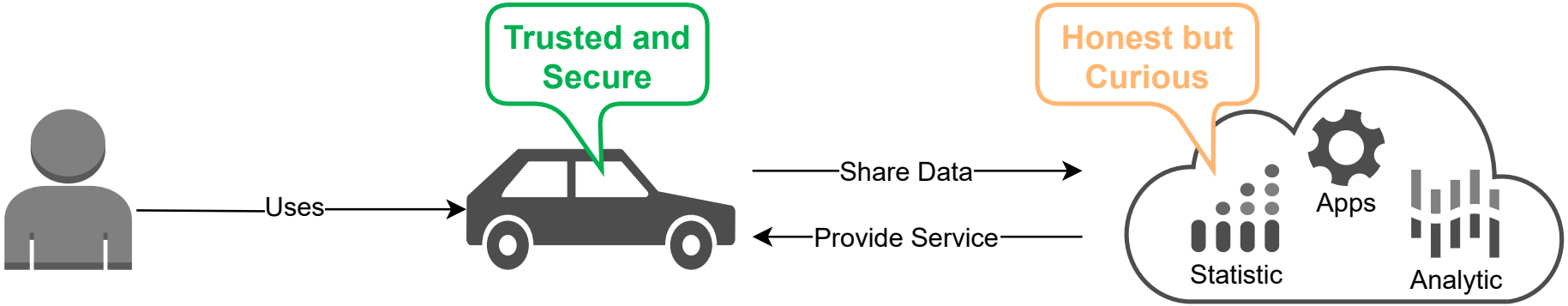
- Prioritize privacy protection given its importance with
  - Transparent data collection
  - Secure communication channels
  - Data minimization
  - Various *Privacy Enhancing Technologies (*PETs)
- While prioritizing privacy, the trade-off between privacy protection and kind of service provided need to be kept in mind

Driver's Perspective



Driver's Perspective

Perception of the Car-to-Cloud Environment



- The underlying CV is ***trusted-and-secure***
  - any personal data stored in the CV cannot be accessed or shared without the driver's consent
  - all computations performed within the CV are secure and resilient to attempts at compromising them
- Remote services are ***honest-but-curious***
  - services comply with legal and driver-consented policies
  - drivers still have concerns that remote services would collect other available personal data out of their inquisitive nature

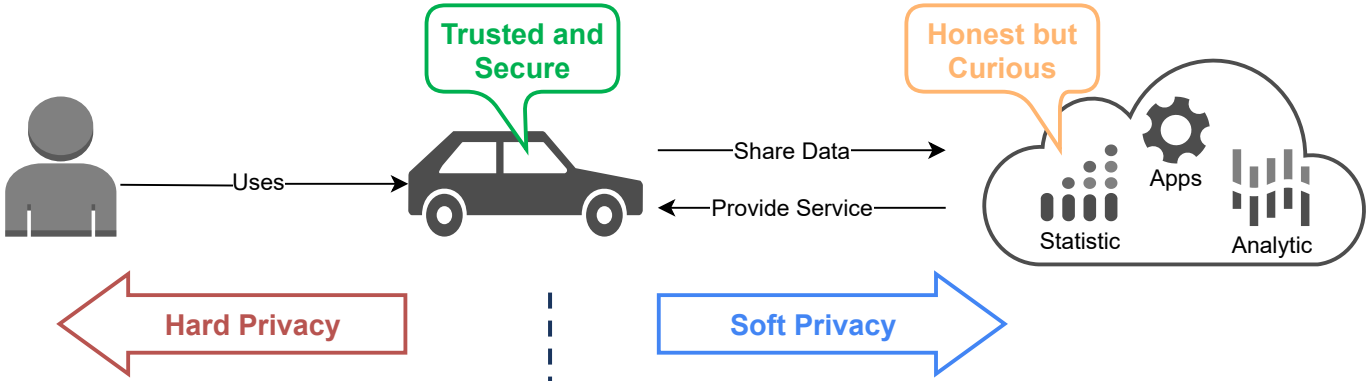
Driver's Perspective

General Privacy Protection Challenges and Approaches

- Balance the **trade-off** between **privacy protection** and **service quality**
  - deploy different PETs and tuning their parameters properly
- Must consider the **dynamic and context-dependent nature** of drivers' privacy needs
  - enable drivers to create privacy policies for individual services and specific situations
  - the data processing in CVs should support live adaptation
- Managing the fine-grained and situation-aware privacy policy for a CV can easily create **information and choice overhead** for drivers
  - develop user-friendly privacy management mechanisms

Driver's Perspective

General Privacy Protection Approaches

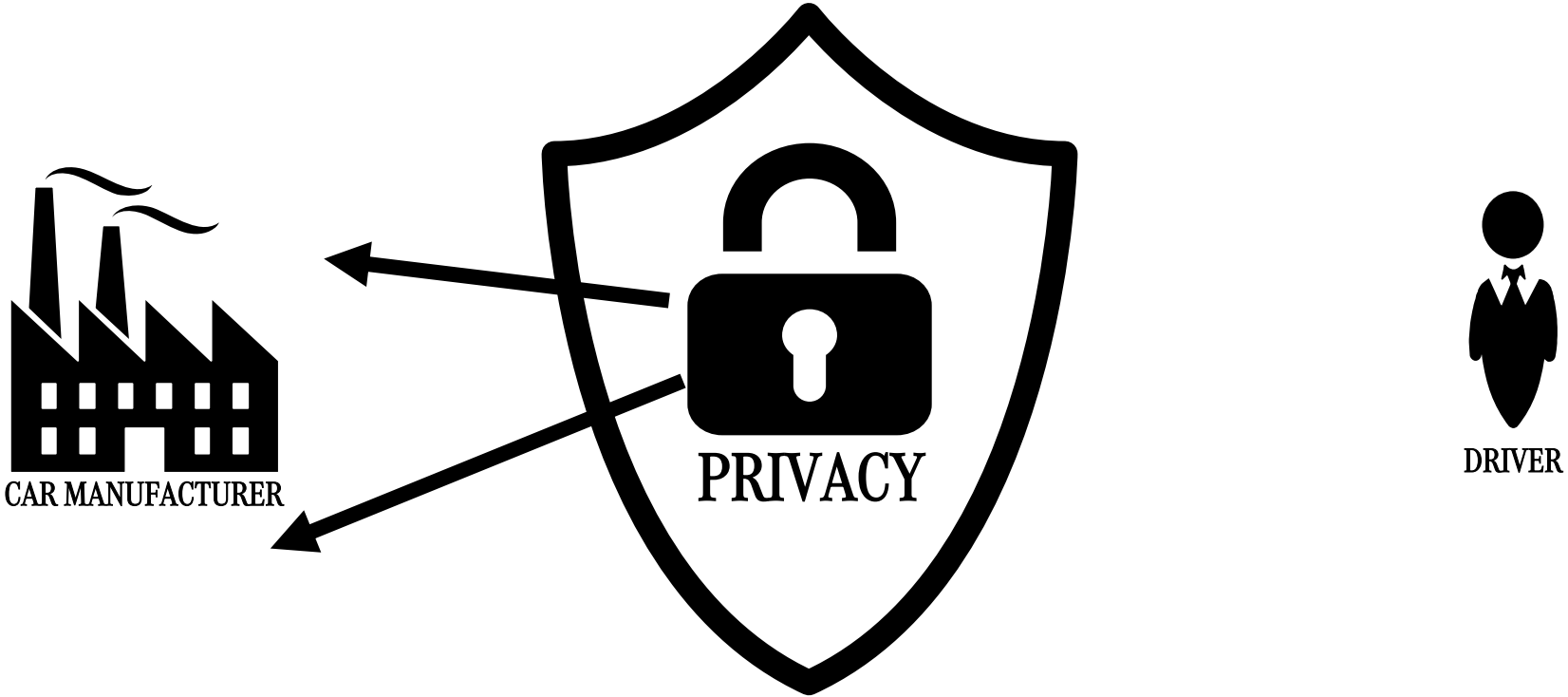


- *Advise drivers to **block unnecessary data sharing** for the desired service functionality*

- *Achieve data minimization through different **PETs** to reduce the accuracy of the vehicle data*
- *Establish a **privacy agreement** between drivers and service providers*

Take Aways

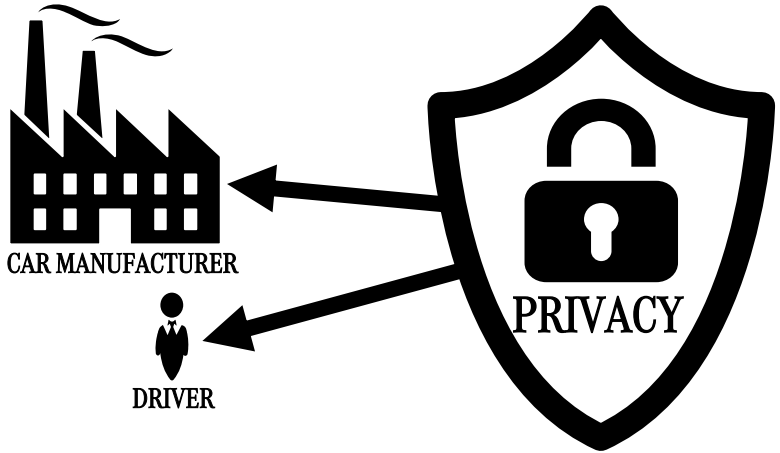
Collaboration and Trust



Take Aways

Collaboration and Trust

- Privacy protection in CVEs is a **shared responsibility**.
- Trust and better privacy can be achieved through driver-manufacturer collaboration, **cooperation**, and **transparent data communication**.



- CVEs' privacy challenges require a balanced approach, addressing both driver and manufacturer perspectives.

Future Work

- User study to thoroughly understand the privacy awareness and requirements of drivers
- Interviews with experts concerning manufacturers' privacy strategies and legal restrictions
- Explore the PETs present in the literature and analyse their feasibility and transferability to the Connected Vehicle domain
- Given the difficulty of finding a general rule for all data collection use cases, privacy by design has a higher chance of succeeding

Andrea Fieschi

Email:
andrea.fieschi@mercedes-benz.com

Thank you