Privacy Self-Protection for Connected Cars

Harald Zwingelberg
ULD
at the meeting of the International Working Group on Data Protection in Telecommunications
Berlin, 22 November 2017

Partly based on research results of the projects:

- SeDaFa
- iKoPA
- Privacy & Us
- ULD
Overview

- challenges of connected cars identified
- methodology used
- requirements derived
Data protection is about data, people and their fundamental rights.

To be checked while developing technologies for connected cars:
- impact on persons
- impact on society
Connected cars allow a series of new possible applications, e.g.:

- assistance systems (from finding parking spots to self driving car)
- infotainment (optimizing routes, finding POI)
- value added services (booking of charging stations along route)
  => this may be a enabler for e-mobility!
- business models (e.g. car insurances as “pay how you drive”)
- services by car manufacturers (ongoing quality assurance)

**Challenges**

- data involved are often personal data or allow for indirect identification of persons
- profiles on movements and interests
- profiles about driving habits
- ...

Slide initially by Christoph Krauß (SeDaFa project)
Challenges to Data Protection –
collection and interpretation of data 1

Car:

- communication centre with network connection
- ... using identifier (e.g. MAC address)
- ... collecting broad set of data
  (> 10 GB / h, e.g. sensors)
- ... leaving many data traces (e.g. location data)
- ... combined with further technology (e-Call, navigation unit, infotainment system)
Camera observation inside the car itself used for:
- observing drivers and passengers
- Identification of persons
- identification of items held or used
- identification of passengers’ actions

Source: InCarIn

https://www.springerprofessional.de/fahrerassistenz/interieur/ projekt-incarin-arbeitet-an-kamerabasierter-personenerfassung-fu/10551520
Challenges to Data Protection – collection and processing of data

PAYD – Pay as you drive
PHYD – Pay how you drive

First minor step done: Separating the storage of information on driving behaviour (ext. service provider) and customer / contract data (insurance company).

Philipp Benkler: PAYD: Generali testet Mobility-App in der Praxis - Bessere Smartphone-Software mithilfe der Crowd
According to the press, China has plans that e-cars must share data every second including current location and identifiers allowing the identification and tracking of cars and persons.
German minister for transport and infrastructure asking for bringing individual rights and data protection in line with the value chain of the economy.

Anonymisation and pseudonymisation seen as business enabler.
Research papers related to tracking

Tracking- und identification possibilities:

- **location data not anonymous**
  
  Zang, Bolot: Anonymization of Location Data Does Not Work: A Large-Scale Measurement Study, MobiCom 2011

- **inferring trip dentitions from driving habits**
  
  Dewri et al.: Inferring Trip Destinations from Driving Habits Data, WPES 2013

- **tracking by knowing one location and speed across route**
  
  Gao et al.: Elastic Pathing: Your Speed is Enough to Track You, UbiComp 2014
Driver Analytics

http://cloudmade.com/solutions/car-driver-analytics
Driver Analytics und Big Data

Connected Cars Can Build A Better Map

Use your connected vehicles to maintain, improve and augment the navigation map and content layers

Personal Navigation Devices
Social Graph included

Connected PNDs Without The Costs

Deliver rich content from global providers using WiFi or Bluetooth connections
Add advanced features like predictive destinations, customized search and analytics

http://cloudmade.com/solutions/connected-pnd
Challenges to Data Protection – new global players

Consumers Are in the Connected Car Seat in 2015
BY TIM KELLY, ZUBIE 01.28.15 | 1:45 PM | PERMALINK

... This year alone, three giants – Microsoft, Google and Apple – have announced their forthcoming “connected car” platforms. Apple already has CarPlay, Google seems to have something in the works with its Open Automotive Alliance, and Microsoft revealed its “Windows for the car.” They all aim to bring the functionality of your mobile device right to your vehicles center consul and we’ll soon find out who takes the cake.
Challenges to Data Protection – remote “kill switch”

Terrified driver almost crashes car when loan company hit ‘kill switch’ for missing repayments

Heartless creditors LOCKED T. Candice Smith’s steering wheel and stopped her engine as she drove down a busy Las Vegas highway.

A terrified driver nearly crashed her car when it suddenly shut down on a motorway – only to find her LOAN COMPANY had used a remote kill switch after she missed a payment.

T. Candice Smith was driving with her friend down a three-lane Las Vegas interstate when her steering wheel began to lock up.

The car’s engine then stopped causing the vehicle to come to a stop.

“used a remote kill switch after she missed a payment”

http://www.mirror.co.uk/news/technology-science/terrified-driver-crashes-car-loan-4325955
www.datenschutzzentrum.de

Challenges to Data Protection: remotely disabling vehicles

Desire of police institutions: “remotely disable people’s cars”

I want to remotely disable Londoners’ cars, says Met’s top cop
Psst, chief. You’ve probably not heard of backdoors – this is a seriously bad idea

22 Sep 2016 at 15:04, Gareth Corfield

Metropolitan Police commissioner Sir Bernard Hogan-Howe wants the capital's cops to be able to remotely disable people's cars, he told the London Assembly's police and crime committee today.

http://www.theregister.co.uk/2016/09/22/met_police_commissioner_i_want_remotely_kill_car_electronics/
SeDaFa project goals

- data minimizing access on car generated data
- enabling self-protection for data subjects
- due consideration of technological, legal and user aspects

SeDaFa research questions

1. How can the risk of privacy breaches of car users be determined?
2. How can car users be informed about data protection aspects in an appropriate manner?
3. How can car users gain self-determined control over the access to their data?

Slide initially by Christoph Krauß (SeDaFa project)
Research Approach

Chosen approach for interdisciplinary research

- list data types processed by smart cars and infrastructure
- collect list of involved entities (data subjects, controllers,...)
- define use cases to guide evaluation e.g.
  - car sharing services, garage accessing OBD data, LBS, Android Auto, distributed search for parking space
- describe legal setting, focus on upcoming GDPR
- assess necessary protection level and derive data protection requirements deploying the Standard Data Protection Model (SDM)
- propose methods to fulfil the requirements
**Connected Cars: involved entities**

- car manufacturer
- car dealer, garage
- provider of hard- and software for cars and service provider
- network provider (e.g. 3G, 4G, 5G networks)
- app programmer
- car owners:  
  - private person  
  - employers  
  - lessor (e.g. leasing banks)  
  - rental services  
  - shipping companies
- insurance companies
- other contractual parties (e.g. advertising clients)
- security authorities
- other public authorities
- data subjects according to GDPR definition:  
  - car owner (private person)  
  - drivers  
  - previous car owner  
  - car passenger  
  - pedestrians & other persons
Data Protection Goals & Standard Data Protection Model (SDM)

- Confidentiality
- Data Minimisation & Unlinkability
- Integrity
- Intervenability
- Transparency
- Availability
More about the Standard Data Protection Model

- Content
  - Methodology
  - Data Protection Goals
  - In progress: catalogues with measures

- V.1.0 recommended for intensified testing by the conference of German data protection authorities on federal and state level, November 10th, 2016.

- English translation: planned

German version:
https://www.saechsdsb.de/images/stories/sdb_inhalt/schwerpunkt/SDM-Methode_V_1_0.pdf
• The catalogue of high level requirements is under current refinement and internal discussion within the project.

• The following requirements reflect ULD’s positions.

• Many requirements directly rephrase legal necessities (legal ground needed, possibility to withdraw consent at any time and data controller must have process in place to deal with withdrawal, ...).

• The focus for this presentation resides on privacy-related requirements.
• Documentation MUST exist – appropriately understandable for users and sufficiently informative for experts

• Where other entities act as controllers, the documentation MUST suffice their needs to ensure compliant processing and documentation towards data subjects (e.g. car rental services, employers providing cars to employees, ...)

Zwingelberg - Connected Cars 23
Transparency 2

accessing documentation

- Information necessary to fulfil transparency MUST be available in the car

- Interfaces of the car SHOULD enable users to access the information

- Where data protection impact assessment is necessary due to specific processing a summary SHOULD be available
Intervenability 1
general principle

• Procedures MUST be in place to influence / correct / update the personal data itself and the process of processing of personal data (change management)

• It MUST be possible to follow requests for deletion or rectification

• Requests for deletion MUST be followed in appropriate time and where data has been transferred to other entities these entities must be notified about the request, Art. 17 GDPR
Intervenability 2
right to access

- Procedures MUST be in place to ensure that requests for right of access / deletion can be handled appropriately.

- Where processing is done under pseudonym right of access / deletion SHOULD be possible under pseudonym.

- Systems SHOULD support privacy rights e.g. where data is manually deleted locally in the car and data is typically mirrored to a third parties' server as standard option data should be deleted on the server as well (privacy by default).

- Interfaces of the car SHOULD enable users to access and manage their personal data.
Intervenability 3
influencing the system

- The data subject MUST have possibilities to influence the processing of personal data.

- The data subject SHOULD have the possibility to deactivate the collection and processing of personal data without losing core functionalities of the system.

- Where options to configure the processing of personal data exist, the default settings MUST foresee that only personal data which are necessary for each specific purpose of the processing are processed, Art. 25 (2) GDPR (privacy by default).
Data Minimisation & Unlinkability

- Unlinkability includes aspects of purpose limitation: These are MUST-requirements under the GDPR

- Storing data at central entities SHOULD be avoided to prevent profiling and purpose creep, e.g. rather allow driver to select data transfers locally in the car than routing all data via servers and services of the manufacturer by default

- Separate processing for separate purposes SHOULD be preferred to allow for individual treatment of data, e.g. individual deletion periods by purpose
Data Minimisation & Unlinkability 2

- System SHOULD allow for anonymisation and pseudonymisation of data – design processes and data structure appropriately (privacy by design)

- Anonymisation SHOULD be preferred over pseudonymisation
IT Security: Confidentiality, Integrity, Availability

- Deploy appropriate IT security measures and treat personal data as assets to protect, e.g.
  - role and access management,
  - encrypted transfer and storage.

- Data protection specific aspects may include
  - data portability – allow import and export of personal data and to mitigate them to another provider, Art. 20 GDPR
  - balance integrity requirements with intervenability, e.g. between backups and the right to deletion / rectification
Support by IT security experts for some Protection Goals

- Connected cars are part of the internet of things (IoT)

- Security requirements for IoT meet many of the privacy aspects

- Even a paper from typical security authorities stress
  - consideration of confidentiality and security in design phase
  - transparency – also along the supply chain of IoT products

(Whenever one needs a supporting paper from an entity known for not being run by privacy activists.)
Disclaimer

- All statements reflect the position of the ULD or the personal opinion of the author where the author takes the position in favour of data protection and informational self-determination.

- Statements and positions are not made on behalf of the research projects SeDaFa, iKoPA or Privacy&Us or on behalf of the respective project partners.
Funding Notice

The results presented are based on research from these projects:

**SeDaFa**
Selbstdatenschutz im vernetzten Fahrzeug

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

funded by the German Federal Ministry of Education and Research

[www.sedafa-projekt.de](http://www.sedafa-projekt.de)

---

**iKoPA**
integrierte Kommunikationsplattform für automatisierte Elektrofahrzeuge

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

funded by the German Federal Ministry of Education and Research


---

**Privacy & Us**

funded by MSCA-ITN-2015-ETN – Marie Skłodowska-Curie Innovative Training Networks
Project Number: 675730

[www.privacyus.eu](http://www.privacyus.eu)
Thank you for your attention

Questions? Comments?

Harald Zwingelberg
Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein (ULD)
https://www.datenschutzzentrum.de/

E-Mail: uld6@datenschutzzentrum.de
Phone: +49 431 988-1222