Data-sharing in IoT Ecosystems and Competition Law: The Example of Connected Cars

Wolfgang Kerber

(University of Marburg)

(forthcoming in: Journal of Competition Law and Economics)

DG Competition Lunch Talk

Brussels, 14 November 2019

1. Introduction: Data access problems in IoT ecosystems

Philipps Universität Marburg

"Internet of Things" (IoT): connected smart devices collecting data

Manufacturer of a connected device often has exclusive control of the

(1) data produced with the device and

(2) technical access to the device (closed system / no interoperability)

Problem: this can lead to

+ a monopolistic gatekeeper position in an IoT ecosystem
+ data access / interoperability problems for users/firms in the ecosystem,
+ danger of leveraging market power to all markets for aftermarket and complementary services that need access to data and/or device,
+ and less competition, innovation, and consumer choice

- Example: "access to in-vehicle data and resources" in connected cars

1. Introduction: Data access problems in IoT ecosystems

Philipps Universität Marburg

Research question of the paper:

How and to what extent can competition law help to solve these problems of data access/sharing and interoperability in IoT ecosystems?

Analysis:
- from an economic and legal perspective
- IoT ecosystems generally and example of connected cars

Additionally: brief analysis of other solutions outside competition law

1. Introduction: Data access problems in IoT ecosystems

Philipps Universität Marburg

Important background discussions and previous research (1)

- (European) data economy / data ownership / data sharing
  + Comm. "Building a European data economy" (Jan 2017)
  + New exclusive right on data? (or data producer right)? (Kerber 2016, 2017)
    > discussion with direct regard to IoT applications
  + shifting of general discussion to data access and data-sharing

- my previous research on data governance in connected cars:
  + Kerber / Frank (2017): Data Governance Regimes in the Digital Economy: The Example of Connected Cars, available at: https://ssrn.com/abstract=3064794
  + Kerber (2018): Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, JIPITEC 9(3), 310-331.
  + Kerber / Gill (2019): Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 10(2), 244-256.

1. Introduction: Data access problems in IoT ecosystems

Philipps Universität Marburg

Important background discussions and previous research (2)

- Current discussion on challenges of digital economy for competition law
  - + Various reports:
    - > Schweitzer/Haucap/Kerber/Welker (2018): Modernising the law on abuse of market power (German report)
    - > Crémer/de Montjoye/Schweitzer (2019): Competition policy for the digital era (EU report)
    - > Furman et al (2019): Unlocking digital competition (UK report)
  - + German and EU report:

    digital IoT ecosystems as an own group of cases with competition / innovation problems through exclusive control of access to data, esp. also in IoT contexts (aftermarket / complementary services)
  - + First legislative reaction: Draft proposal for amending German competition law with proposals for facilitating access to data

2. Economics of IoT ecosystems: Data access and interoperability problems

(1) Economics of data
- non-rivalry of use of data => benefits of data sharing
- costs of data production can be very low or high

(2) Economics of interoperability (closed vs. open systems)
- benefits and costs of interoperability
- market failure: often too closed systems / not enough interop /standardis.

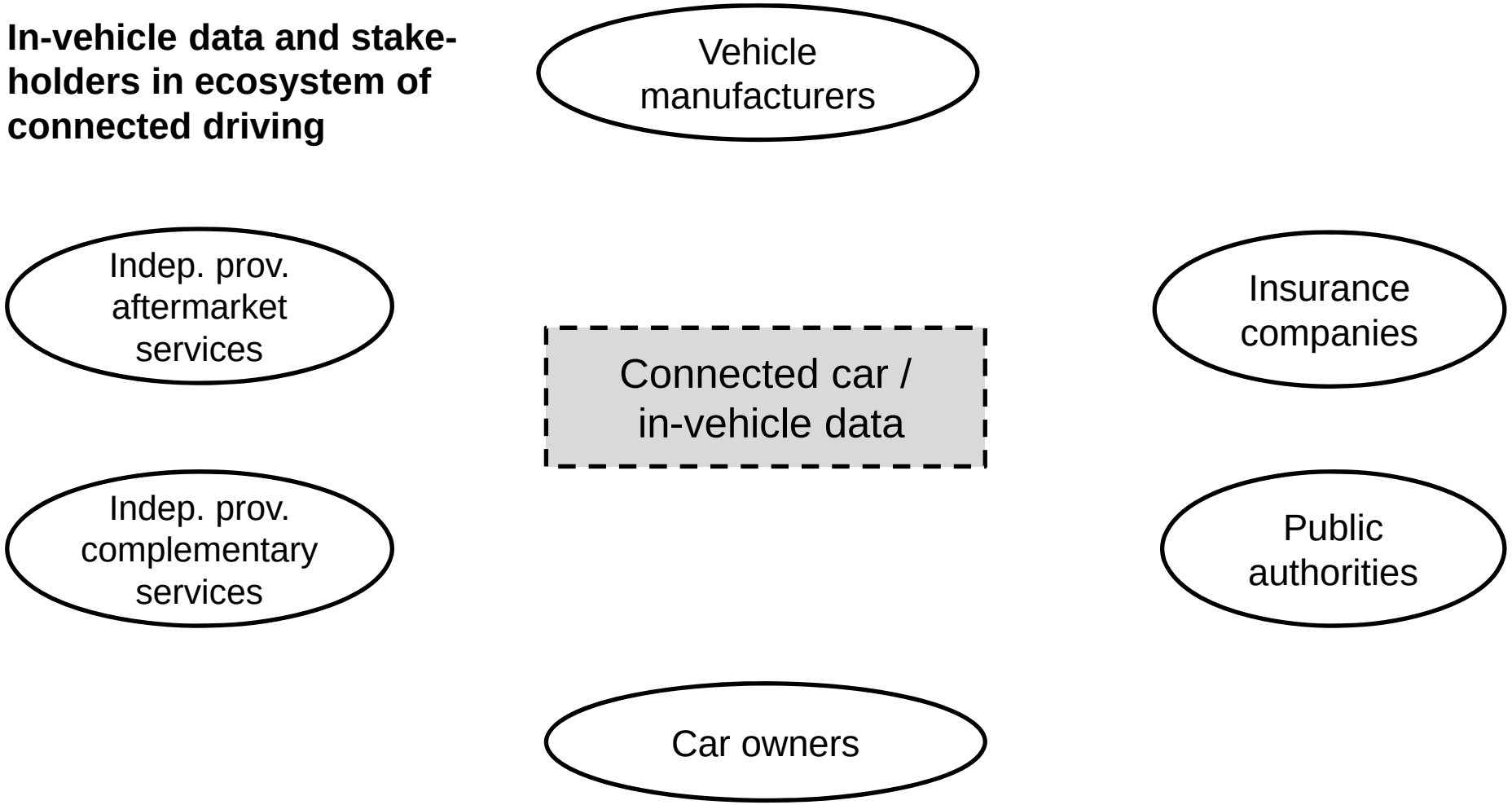
(3) Economics of ecosystems, lock-in, and bundling:
- lock-in of users of connected devices (switching costs)
- leveraging of market power to aftermarket and complementary services in ecosystem that need access to data or the device
- aftermarket theory / systems competition / effects of bundling

=> necessity of balancing manifold positive and negative effects

3. The example of connected cars

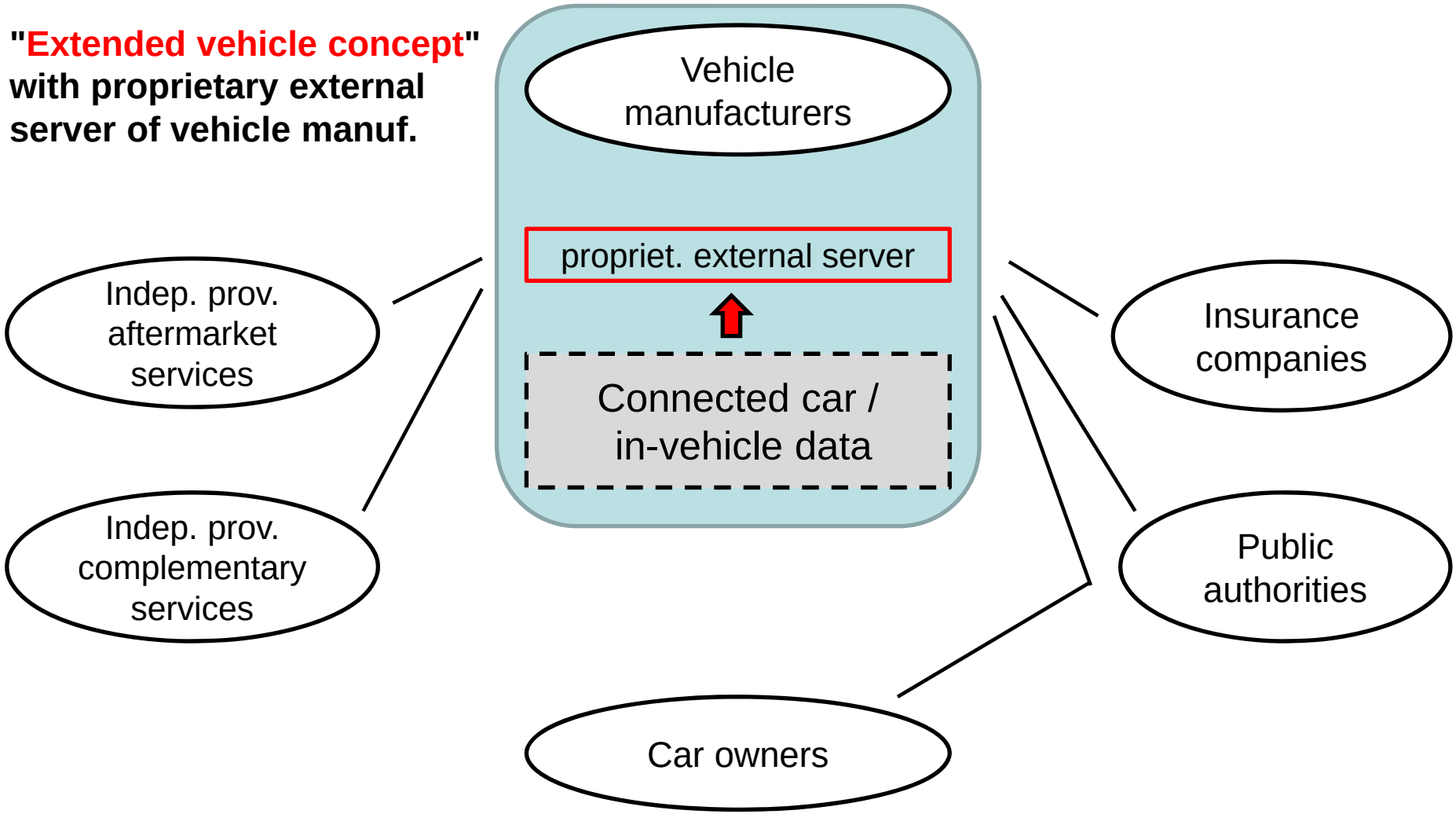
3.1 The problem of „access to in-vehicle data and resources" (1)

In-vehicle data and stake-holders in ecosystem of connected driving

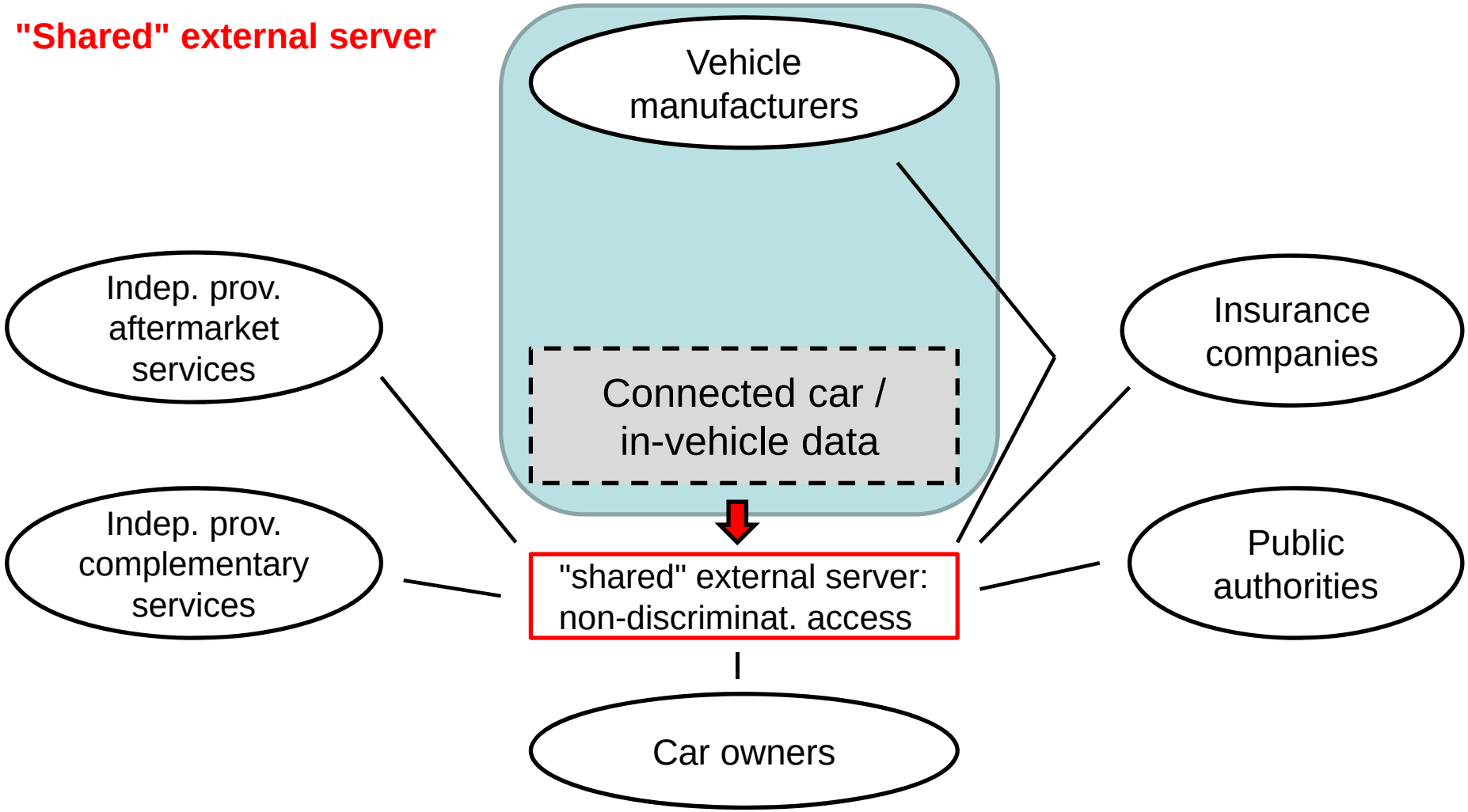


3.1 The problem of „access to in-vehicle data and resources" (2)

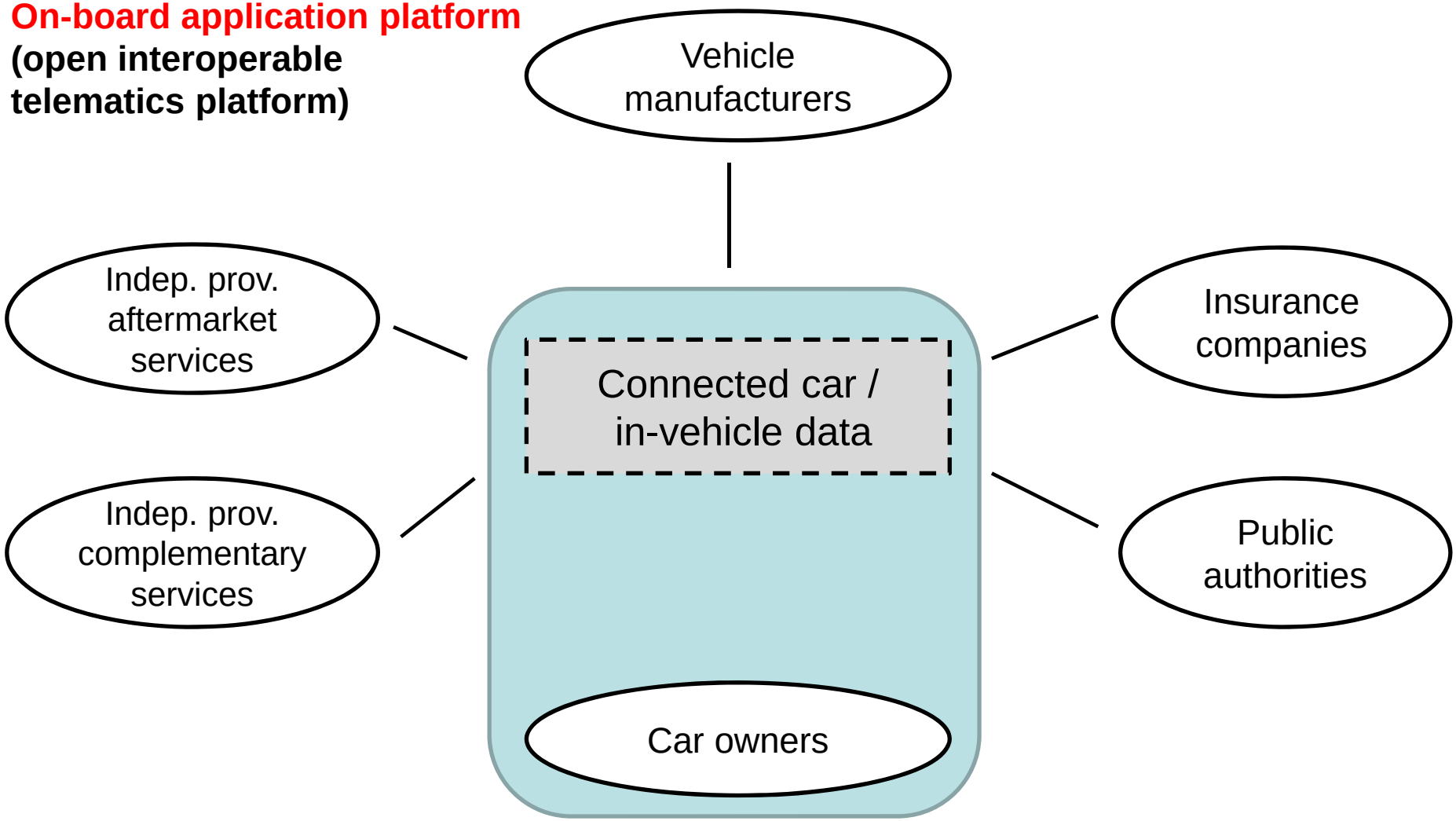
"Extended vehicle concept" with proprietary external server of vehicle manuf.



3.1 The problem of „access to in-vehicle data and resources" (3)



3.1 The problem of „access to in-vehicle data and resources" (4)



3.1 The problem of „access to in-vehicle data and resources" (5)

Controversial policy discussion about „extended vehicle" concept in EU (1)

- Independent service providers (ISPs) / consumers: call for regulatory action
  - + complain „privileged access" to (or monopolisation) of in-vehicle data of OEMs that allows them to control all automotive aftermarkets and new complementary services for which access to these data and/or the car is necessary
  - + large concerns about foreclosing ISPs from these markets, which might lead to less competition, innovation, and consumer choice
- Background: old struggle betw. OEMs / dealers and independent repair / maintenance service providers for market shares on automobile aftermarkets
  - + old topic in competition policy: fighting against foreclosure strategies of OEMs
  - + for a long time: **regulated access regime to essential technical information for repair/maintenance services** (motor vehicle type approval Reg. 715/2007) for protecting competition against foreclosure strategies
  - + FRAND-like access regime but only for info necessary to tradit. R/M services, not for innovative remote aftermarket services or other complementary services in connected cars (new Reg. 2018/858 does not solve the problems)

Controversial policy discussion about „extended vehicle“ concept in EU (2)

- Vehicle manufacturers: defend "extended vehicle" concept
  + exclusive control necessary for safety/security => no regulatory action needed
- EU initiative: C-ITS platform (2016) with 5 principles of access to in-vehicle data, e.g., "fair and undistorted competition"
- comprehensive TRL study (2017): confirms problems, rejects "extended vehicle" concept, esp. due to impediment of fair and undistorted competition, and suggests either, in the medium-term, a "shared server" solution, or, in the long-term, the transition to on-board application platform
- European Parliament (Feb. 2018): wants „levelling the playing field“ with regard to „access to in-vehicle data"
- EU Commission ["On the road to automated mobility", May 2018] acknowledges the problem but has been so far very reluctant about a legislative initiative

=> unresolved open policy question in the EU !

3.2 Market failure problems in the ecosystem of connected driving: An economic analysis (1)

Questions: Assessment of the extended vehicle concept of the VMs?

Can we rely on market competition for finding the best solution for the governance of in-vehicle data and interoperability?

Technological choice and de facto control / "ownership" of data

- Extended vehicle concept leads to
  - (1) exclusive ("monopolistic") control of the in-vehicle data by the VMs, i.e. de facto "appropriation" of in-vehicle data
  - (2) "closed" systems because VMs control the technical access to the car

  => closed ecosystems of connected driving

- On-board application platform: here the car owners have control about the access to the data and the car, i.e. car owners are the de facto data "owners"

=> choice of technology decides about initial allocation of de facto control of data and access to the car

3.2 Market failure problems in the ecosystem of connected driving: An economic analysis (2)

Safety / security problems

- Can extended vehicle concept be justified through safety / security reasons?
- Counterargument I: very unclear whether less safety/security risks through
  - \+ exclusive control of access to cars by VM or
  - \+ an open interoperable telematics platform with a multi-layered safety/security system (with mandatory certification of service providers)
- Counterargument II:

  even if exclusive technical control of VM about access to car necessary, this does not justify the exclusive commercial control of in-vehicle data

  => separability of technical access and commercial control of data

=> safety/security reasons do not justify exclusive control of in-vehicle data

=> no trade off between safety/security and competition !

3.2 Market failure problems in the ecosystem of connected driving: An economic analysis (3)

Market failure I: Competition problems in markets for aftermarket / complementary services

- Effects of exclusive control of VMs of access to data and the car:
  - + VM can monopolize aftermarket / complementary services directly or "sell" the access to these markets (with too high "monopolistic" prices)
  - + concerns about foreclosure of independent service providers are justified!
  - + no fair and undistorted competition and innovation possible ! (outside regulated access regime of type approval regulation)
- Can systems competition between VMs solve this problem?
  - + competition betw. bundles of cars and aftermarket/complementary services?
  - + competition can induce VM to more „open“ strategies and lead to more competition/innovation in aftermarket/complementary services
  - + however very doubtful whether consumers can assess the entire bundle of car and (future) services well for enabling effective systems competition

3.2 Market failure problems in the ecosystem of connected driving: An economic analysis (4)

Market failure II: Information / privacy problems of car owners

- No simple sale contract betw. VM and car owner but
  - + de facto (long-term) bundle of contracts about car and services/updates for connected / automated driving ("Lock-in" problem)
  - + includes "consent" to VM to use personal data
- Information/behavioral problems of car users with regard to decisions about privacy and data provision:
  - + Can car owners make rational „informed“ choices about privacy and data provision decisions (privacy paradox, intransparency of privacy policies etc.)?
  - + Do "notice and consent" solutions really work?
  - + Do car users have a "genuine" choice? Do VM offer enough granular privacy options for different privacy preferences?

3.2 Market failure problems in the ecosystem of connected driving: An economic analysis (5)

Market failure III: Choice of inefficient technologies (interoperability / standardization problems)

- Is "extended vehicle" a superior technology or result of a market failure problem?
  (economics: interoperability and standardisation can suffer from market failures)
- problem I: OEMs might have chosen too closed proprietary systems (with too large lock-in effects for car users) that impede competition / innovation on secondary markets (foregoing benefits of interoperability)
- problem II: long-term architecture of integrated systems of connected and automated mobility will require anyway interoperable interfaces / standards (V2I, V2V, ...)

=> open interoperable telematic platforms might be superior to proprietary closed systems due to more interoperability and standardisation

3.2 Market failure problems in the ecosystem of connected driving: An economic analysis (6)

Summary: Three potential market failure problems (needs more investigation):

(1) competition problems for aftermarket and complementary services with potentially negative effects also on innovation

(2) information / privacy problems for car owners with the problems of "notice and consent" solutions in regard to (personal) data

(3) problems in regard to optimal technological choice (standardisation / interoperability)

=> serious concerns about "extended vehicle" concept as current market solution

Important conclusion: in multi-stakeholder situations as IoT ecosystems exclusive control of data by one firm might not be an efficient solution for the data governance problem

=> still unclear what an appropriate solution for the problem of governance of the ecosystem of connected driving with respect to data / interoperability is

=> important: thinking in terms of "governance of the entire ecosystem" ...

4. Overview about solutions for data access and interoperability problems in IoT ecosystems

In the discussion many different legal / policy instruments have emerged:

- **sector-specific regulatory solutions** (e.g., PSD2, motor veh. type approval reg)
- **data portability right** (Art. 20 GDPR) and other data portability solutions
  - + unclear scope, no real-time data, large transaction costs => not effective
  - + would not be effective in connected car case (Gill/Kerber 2019)
- introduction of **direct data access rights** (e.g., Drexl 2018, Australia: CDRs)
- **contract law / unfair trading law** (unequal bargaining power)
- **standardisation policy** (for interoperability / data portability)
- **competition law:**
  - + particularly: refusal to grant access to data of an exclusive data holder as abusive behavior of firms with market power
  - + but also other provisions as, e.g., prohibition of collusive agreements (Art. 101 TFEU)

5. Competition law solutions

5.1 Abusive behavior I: Dominant firms (Art. 102 TFEU)

Analysis of dominance of firms with exclusive control of IoT ecosystems

+ important: systems competition? separate markets?
+ (Connected cars: here good arguments for separate markets)

Two options for reasonings about refusal to data as abusive behavior:

- Essential facility doctrine (EFD):
  + indispensability, elimination of competition, (new product test) obj. justification
  + very important: can be applied much more flexibly than in traditional EFD (Schweitzer/Haucap/Kerber/Welker 2018)
- Leveraging of market power / foreclosing ISPs on secondary markets of ecosystems (see Crémer et al 2019)
  + refusal is abusive due to negative effects on competition, innovation etc.
- in both options: comprehensive balancing of effects necessary

5.1 Abusive behavior I: Dominant firms (Art. 102 TFEU)

Criteria for balancing of effects (for qualifying refusal of data access as abusive)

- importance of heterogeneity of data (also in CC), (raw/processed data, personal/ non-personal, individual / aggregated data etc., see Cremer et al 2019)
- compliance with GDPR, protection of business secrets / IP / database
- benefits of data access for competition / innovation on secondary markets within IoT ecosystem (=> value creation)
- costs of data production: can be high or low (=> incentive problem?)
- have other stakeholders in the IoT ecosystems participated in data production?
- compensation solutions for giving access to data

  => different solutions for different data and types of stakeholders in ecosystem!

Problems: - not easy to apply in IoT contexts, problem of proving dominance etc.
- (in CC certainly possible but also difficult in practice)

Interoperability problems: refusal of interoperability can also be abusive behavior (Kerber/Schweitzer 2017)

5.1 Abusive behavior II: Firms with "relative market power" (§ 20 (1) GWB)

But: Many doubts whether Art. 102 can be applied flexibly enough for solving these data access problems

Other option: **"Relative market power"** instead of "market dominance"

- "unequal bargaining power" betw. firms / bilateral dependence
- exists in number of countries, as, e.g., Germany, Japan, France
- economically a difficult concept, but also solid economic reasonings

§ 20 (1) GWB in German competition law

- prohibition of abusive behavior is extended to firms with "relative market power":
- firms from which other small or medium-sized firms are dependent, because they have not sufficient and reasonable possibilities of switching to other firms
- old provision of German competition law used for solving specific case groups:
  + "firm-specific" dependency, e.g. authorised dealers
  + buying power situations

5.1 Abusive behavior II: Firms with "relative market power" (§ 20 (1) GWB

German report (Schweitzer/Haucap/Kerber/Welker 2018): proposal of "activating" this provision for solving data access problems in IoT / aftermarket situations:

+ extending this provision to all firms, not only SMEs
+ extending § 20 (1) GWB also to situations of "data dependency"

How to apply (amended) § 20 (1) GWB to data access problems in IoT ecosystems?

- basic idea:
  + ISPs within the IoT ecosystems can be bilaterally dependent on manufacturer of connected device (as VMs in CC example)
  + refusal to grant access to data can be an abusive behavior of this firm with "relative market power"
- important: also balancing analysis necessary with similar criteria as in Art. 102
- advantages: no proof of dominance etc., direct analysis of bilateral dependency
- problems: not easy to develop new case groups but might work to some extent, esp. if competition authority applies it actively (e.g., also by guidelines)
- Connected car example: ISPs can use this provision

5.1 Abusive behavior III: Proposal for amending German competition law

Draft proposal for 10th amendment of German competition law (7 Oct 2019)

- Facilitating data access in § 20 (1) GWB / relative market power:
  + abolishment of limitation to SMEs in § 20 (1) GWB
  + new § 20 (1a) GWB: data dependency

    "(1a) A dependency according to paragraph 1 can also exist if an undertaking for its own business activities needs access to data, which are controlled by another undertaking. A refusal of access to those data can be also an unreasonable exclusionary behavior, if so far no market for these data exists."

- § 19 (2) No.4 GWB: essential facility doctrine explicitly extended also to data

- § 19 a GWB: new type of control of abusive behavior for undertakings with a paramount significance for competition across markets ("überragende marktübergreifende Bedeutung für den Wettbewerb")
  + German competition authority could prohibit measures that would impede competition by making interoperability and data portability more difficult (§ 19 (2) No. 4 GWB).

5.2 Other provisions of competition law

- Intermediate result:

  Competition law rules on abusive behavior might be able to solve data access and interoperability problems in IoT ecosystems but only to some extent and with many problems

- Other options: to prevent the emergence of positions of exclusive control of access to data and the device through competition law
  + merger control
  + prohibition of foreclosing behavior of acquiring data / impeding interoperability
  + prohibition of collusive agreements on technology / data governance (Art. 101)

- Example connected car:
  + Is "extended vehicle concept" itself an anticompetitive horizontal agreement on technology and data governance for establishing exclusive control of in-vehicle data and closed ecosystems of connected driving?
  + good reasons for a deeper investigation

6. Solutions for data governance problems in IoT ecosystems: Broadening the discussion (1)

Summarizing some results:

- in IoT ecosystems there might be serious (market failure) problems regarding exclusive control of access to data and to the connected device (interoperability)
  + Connected cars: ecosystems of connected driving is a good example
- but the problems are complex and different for different IoT ecosystems, which also requires different solutions for data access and interoperability
- competition law can help to some extent to solve these problems, but this might be difficult and often will not be sufficient
- although competition law solutions are important as general (and fallback) solutions, often also other solutions might be necessary and more appropriate,
  + data portability, data acccess rights, contract law, unfair trading law
  + new innovative forms of governance solutions for ecosystems (e.g. data spaces, data sandboxes, data trustee solutions ...)
  + sector-specific regulatory solutions

6. Solutions for data governance problems in IoT ecosystems: Broadening the discussion (2)

Sector-specific regulatory solutions (connected car example)

- complexity of ecosystem of connected driving with many stakeholders and market failure problems => specifically tailored sector-specific solution consisting of
  + technological dimension (e.g., standardisation for interoperable telematic platforms and safety/security)
  + data governance dimension (who controls what kinds of data, protection of privacy, data portability, data access/sharing, data markets)
- learning from other sector-specific solutions:
  + Old/new motor vehicle type approval regulation (Kerber/Gill 2019)
    > FRAND-like solution for access to essential technical information combined with technological and safety/security regulation
    > new regulation (2018/858) is much too narrow for solving problems of connected cars
    > but it can be extended to much more data and services (beyond RMI)
  + PSD2 (second payment service directive) etc.

Literature

C-ITS Platform (2016): Final Report.

Crémer, J./Y-A. de Montjoye/ H. Schweitzer: Competition policy for the digital era, available at: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

Drexl, J. (2018): Data Access and Control in the Era of Connected Devices, Brussels.

Furman, J./D. Coyle/A. Fletcher/ P. Marsden/ D. McAuley (2019): Unlocking digital competition. Report of the Digital Competition Expert Panel

Gill, D. / Kerber, W. (2019): The GDPR's Right to Data Portability, A Solution for Data Access Problems in the Connected Car?, mimeo.

Kerber, W. / S. Frank (2017): Data Governance Regimes in the Digital Economy: The Example of Connected Cars, available at: https://ssrn.com/abstract=3064794

Kerber, W. (2018): Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, JIPITEC 9(3), 310-331.

Kerber, W. (2019): Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars, 2019, forthcoming in: Journal of Competition Law and Economics; available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3445422.

Kerber, W. / D. Gill (2019): Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 10(2), 2019, 244-256.

Kerber, W. / H. Schweitzer (2017): Interoperability in the Digital Economy, in: JIPITEC 8(1), 2017, 39 - 58.

TRL (2017): Access to In-Vehicle Data and Resources – Final Report (18.05.2017).

Schweitzer, H./Haucap, J./Kerber, W./Welker, R. (2018): Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Nomos: Baden-Baden.

Additional slide: Motor Vehicle Type Approval Reg. 2018/858

- Old regime for access to essential technical information for repair/maintenance services (RMI): Reg. 715/2007
  + for protecting competition betw. OEMs and independent repair/mainten. prov.
- Design of this sector-specific access regulation:
  + FRAND-like solution for access to essential technical information for RMI
  + non-discriminatory, reasonable fees, standardized format etc.
  + also technological regulation: OBD-Adapter w. certain sets of diagnostic data
  + solutions for repairs on security-relevant parts of the car: certification of independent repairers (see also certification / independ. spare part producers)
- Analysis of the reform of type approval reg. (2018/858) (Kerber/Gill 2019)
  + reform not sufficient for transition to connected cars
  + what is missing: access to data and interoperability for new R/M services (esp. remote services)
- Option: Extending this sector-specific access regime for RMI to all data that are necessary for ISPs and standardization of interfaces and security solutions
  + one option for a sector-specific regulatory solution (data + interoperability)