Kerber, Wolfgang

Working Paper

Data governance in connected cars: The problem of access to in-vehicle data

MAGKS Joint Discussion Paper Series in Economics, No. 40-2018

Provided in Cooperation with:
Faculty of Business Administration and Economics, University of Marburg

Suggested Citation: Kerber, Wolfgang (2018) : Data governance in connected cars: The problem of access to in-vehicle data, MAGKS Joint Discussion Paper Series in Economics, No. 40-2018, Philipps-University Marburg, School of Business and Economics, Marburg

This Version is available at:
https://hdl.handle.net/10419/200696

Joint Discussion Paper Series in Economics

by the Universities of

Aachen · Gießen · Göttingen
Kassel · Marburg · Siegen

ISSN 1867-3678

No. 40-2018

Wolfgang Kerber

Data Governance in Connected Cars: The Problem of Access to In-vehicle Data

This paper can be downloaded from
http://www.uni-marburg.de/fb02/makro/forschung/magkspapers

Coordination: Bernd Hayo • Philipps-University Marburg
School of Business and Economics • Universitätsstraße 24, D-35032 Marburg
Tel: +49-6421-2823091, Fax: +49-6421-2823088, e-mail: hayo@wiwi.uni-marburg.de

Version: November 14, 2018

Data Governance in Connected Cars: The Problem of Access to In-vehicle Data

Wolfgang Kerber*

Abstract: Through the application of the technological solution of the "extended vehicle" concept the car manufacturers can capture exclusive control of the data of connected cars leading to serious concerns about negative effects on competition, innovation and consumer choice on the markets for aftermarket and other complementary services in the ecosystem of connected and automated driving. Therefore a controversial policy discussion has emerged in the EU about access to in-vehicle data and the connected car for independent service providers in the automotive industry. This paper claims that this problem should be seen as part of the general question of the optimal governance of data in the ecosystem of connected and automated mobility. The paper offers an overview about this policy discussion and analyzes this problem from an economic perspective by using a market failure analysis. Besides competition problems (esp. on markets for aftermarket and other services in the connected car) also market failures in regard to technological choice (extended vehicle vs. interoperable onboard application platform) and information and privacy problems ("notice and consent" solutions) can emerge, leading to the question of appropriate regulatory solutions. The paper discusses solutions through data portability, data rights, competition law, and recommends a sector-specific regulatory approach.

Key words: data governance, connected cars, data economy, data access

JEL classification: K23, K24, L62, L86, O33

---

* Professor of Economics, Marburg Centre of Institutional Economics, School of Business & Economics, University of Marburg, Germany; Email: kerber@wiwi.uni-marburg.de. I thank the participants of the Ascola conference on June 22, 2018 (NYU Law School, New York) and the EPIP conference on September 6, 2018 (ESMT, Berlin) as well as Daniel Möller for valuable comments. The research for this paper has been funded by University of Marburg leading to no conflict of interest. Other research for studies related to this topic have been funded by Bundesministerium für Bildung und Forschung [Specht/Kerber: Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, 2018, as part of the ABIDA (Assessing Big Data) project, University Münster] and Bundesministerium für Wirtschaft und Energie [Schweitzer/Haucap/Kerber/Welker: Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018].

A. Introduction

Connected, automated (and later autonomous) cars can lead to large benefits both to users of cars and to society (such as more convenience, reduction of accidents, congestion and emissions). Connected and automated driving is a technological revolution not only for the automotive industry (and their business models) but also for the mobility in society. Therefore in the EU and the Member States a policy discussion has emerged on how to enable connected and automated driving. The recent EU Communication "On the road to automated mobility: An EU strategy for mobility of the future" offers a broad overview about the challenges and problems that have to be solved.[1] There are many open regulatory questions about safety and cybersecurity risks, liability problems, ethical questions, standardization and interoperability problems, privacy concerns, and the governance of data (esp. data access).

This article focuses on the question of the governance of the huge mass of data produced in connected cars. An important part of this data governance problem is the current controversial policy discussion about "access to in-vehicle data and resources" for independent providers of services within the ecosystem of connected and automated mobility.[2] The car manufacturers (OEMs: original equipment manufacturers) use the so called "extended vehicle concept" that implies transmitting all data produced in the car directly to proprietary servers of the OEMs granting them an exclusive ("monopolistic") control of these data. Many firms within the ecosystem of connected and automated mobility could provide a wide range of services to the cars owners and drivers if they also have access to the in-vehicle data. These independent service providers (and also consumer associations) are concerned that this "privileged" position of the OEMs allows them to control the automotive aftermarkets and adjacent services leading to less competition, less consumer choice and less innovation. Therefore the current policy discussion focuses on this conflict between the OEMs, who defend their extended vehicle concept with safety and security arguments, and the many independent service providers, who demand regulatory solutions about the access to in-vehicle data and connected cars for ensuring a fair and undistorted competition in regard to the provision of services in the ecosystem of connected driving. The most important proposals are either – in short-term - a non-discriminatory governance solution for the in-vehicle data (e.g., a "shared server") or – in long-term - the transition to another technological solution (on-board application platform), which would allow the car owners to control access to in-vehicle data and the car. Although the EU Commission has acknowledged the problem that the "centralisation of in-vehicle" data in the extended vehicle concept might cause a competition

[1] See EU Commission, A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, 30.11.2016, COM(2016) 766 fin.; EU Commission, On the road to automated mobility: An EU strategy for mobility of the future, 17.5.2018, COM(2018) 283 fin.; Bundesregierung, Strategy for Automated and Connected Driving, 2015.

[2] See C-ITS Platform, Final Report, 2016; TRL, Access to In-Vehicle Data and Resources – Final Report, 18.05.2017; and as overview Specht/Kerber, Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, 2018, available at: http://www.abida.de/de/blogitem/gutachten-datenrechte-eine-rechts-und-sozialwissenschaftliche-analyse-im-vergleich, 169-192.

problem and want to improve access to these data, so far only a recommendation with guidance on non-binding principles for access to in-vehicle data is planned.[3]

Although the current policy discussion is primarily about access to in-vehicle data and resources for independent service providers, the problem of finding an appropriate governance solution for data in the ecosystem of connected and automated mobility is a much more complex problem. One important problem is the fact that most in-vehicle data are also personal data that are subject to the requirements of EU data protection law. Due to non-rivalry in the use of data, i.e. that many firms can use the same data for their services and innovations, the question arises whether an exclusive control of in-vehicle data through one stakeholder in such a complex ecosystem of connected driving with so many different stakeholders is an economically efficient governance solution for these data. Or should a more sophisticated data governance solution be chosen that allows more stakeholders to get access to these data as a valuable input for their services and innovations? This economics of data perspective is directly linked to the recent discussion about data rights and the efforts of the EU Commission for better data access and reuse.[4] Any solution however also has to comply with EU data protection law for protecting the privacy of the car users. This article claims that the problem of access to in-vehicle data should be seen as part of the more general question how a comprehensive governance solution for the data that are produced in the ecosystem of connected and automated mobility should look like.

The objective of this article is to provide (1) an overview about the current discussion about access to data in the connected car (section B), (2) an economic analysis of the data governance problem that asks for potential market failure problems (section C), and (3) a discussion about possible policy approaches for dealing with the data governance problems (section D).

The analytical approach used in this article is an economic analysis of potential market failures that can arise in the ecosystem of connected driving and which might make regulatory activities necessary for solving the data governance problems. One of the potential market failure problems are certainly the competition problems that might be caused by the exclusive control of in-vehicle data in the extended vehicle concept on the markets for aftermarket and complementary services. In that respect also an analysis of competition between OEMs is necessary. A second potential market failure refers to the question whether it can be expected that OEMs choose technological solutions that are optimal in regard to the entire ecosystem of connected and automated driving (such as the extended vehicle concept or the onboard application platform). Based upon the insights of the economics of interoperability and standardization serious doubts arise whether OEMs have the right incentives for making optimal technological decisions. An additional third concern is that car users as consumers

[3] EU Commission 2018 (n 1) 13.

[4] See EU Commission, Building a European data economy, 10.1.2017, COM(2017) 9 fin.; EU Commission, Towards a common European data space, 25.4.2018, COM(2018) 232 fin.; and as overview Kerber, Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective, in: Lohsse/Schulze/Staudenmayer, Trading Data in the Digital Economy: Legal Concepts and Tools, 2017, 109-133.

might run into similar problems of protecting and dealing properly with their personal data and their privacy as they are well-known in regard to other internet service providers, where it is doubtful whether and to what extent consumers can make well-informed rational decisions about the provision of data to digital companies. In all three cases the preliminary assessment in this paper suggests that serious market failures can exist, although much more research is necessary. Therefore, the results of this analysis raise serious doubts about the currently used extended vehicle concept of the OEMs, which might be both a wrong technological solution, esp. in the long term, and lead to negative effects regarding competition on markets for aftermarket and complementary services. It will also be shown that safety and security concerns cannot justify the exclusive control of data of OEMs and their power to appropriate the value of in-vehicle data through this monopolistic gatekeeper position. The development of an on-board application platform (as an open interoperable telematics platform) would avoid many of the disadvantages of the extended vehicle concept and might be also more compatible with the needs of the long-term architecture of an integrated ecosystem of connected and automated mobility.

Due to the complexity of the technological and data governance problem in regard to connected driving this article cannot offer a clear-cut policy proposal. However, in an overview about recent discussions of possible policy approaches to solve data access and data governance solutions, section D discusses the right to data portability (Art. 20 GDPR), the general introduction of explicit data rights in civil law, as well as possible solutions in competition law, e.g., data access rights as remedies for the refusal to grant access to data as abusive behavior of firms with market power (as, e.g., Art. 102 TFEU). However, it will conclude with the suggestion that due to the large complexity of this problem, looking for a sector-specific regulatory solution might be the most suitable path for solving the data governance problem in the ecosystem of connected and automated driving.

B. Access to in-vehicle data and resources: A policy discussion in the EU

In the connected and automated car many different kinds of data are produced, particularly through sensors. This can be technical data about the car and its components, data about road, weather and traffic conditions, the driving behavior of the car drivers, location data but also data about the use of entertainment, navigation and many other services by the car users. Through the connectivity of the car via mobile communication these data can be transmitted in real-time to external entities, e.g. to an external server of the OEMs, but also a direct exchange of data is possible that allows, e.g., the downloading of software (updates). The connectivity and the in-vehicle data allow for many new (and innovative) services that can be offered to the car users. They can include new forms of repair and maintenance services (as, e.g. remote diagnostics and maintenance), navigation services, parking apps, search services for hotels and restaurants, entertainment, online-shopping, but also new insurance schemes (as used-based insurance), and others.[5] The providers of these services

[5] See generally about connected and automated cars OECD/ITF, Automated and Autonomous Driving. Regulation under uncertainty. Corporate Partnership Report, 2015; Anderson et al., Autonomous Vehicle Technology – A Guide for Policymakers, 2016; Alonso Raposo et al., The revolution of driving:

however often need access to the in-vehicle data and/or to the connected car for providing these services (and for communication with the car users) for being capable to enter the markets for aftermarket and complementary services.[6] A part of these new services would also require real-time access to these data and the car.[7]

As part of its "Cooperative Intelligent Transport Systems" initiative for solving problems of connected and automated driving, the EU Commission has brought together all stakeholders on the C-ITS platform.[8] In this context the problem of access to these data for independent service providers was already discussed very clearly. An important result for the ensuing policy discussion was a consensus about five guiding principles that should apply in regard to access to in-vehicle data. Besides solving safety and security problems ("tamper-proof access and liability"), the compliance with data protection and data privacy, and standardized access / interoperability for facilitating use of same vehicle data, two important principles were also the right of car users to decide if data are provided and to whom (consent), and that "all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services" to the car users ("fair and undistorted competition").[9] Especially in the Working group 6 of the C-ITS platform, which dealt with technological solutions about access to in-vehicle data, the conflict between OEMs and independent service providers became very apparent,[10] because – as we will see later in more detail (section C.II) – technological solutions can deeply influence the governance of data.

---

from Connected Vehicles to Coordinated Automated Road Transport (C-ART), European Commission JRC Science for Policy Report, Part I: Framework for a safe & efficient Coordinated Automated Road Transport (C-ART) system, 2017; for the new business opportunities through the connected car see McKinsey, Competing for the connected customer: Perspectives on the opportunities created by car connectivity and automation, McKinsey & Company, Advanced Industries, September 2015; McKinsey, Car data: Paving the way to value-creating mobility – Perspectives on a new automotive business model, McKinsey & Company, Advanced Industries, March 2016; BVDW, Connected Cars – ein Diskussionspapier zum Thema Services, 2015; BVDW, Connected Cars – Geschäftsmodelle. Diskussionspapier, 23.05.2016; BVDW, Connected Cars – Chancen und Risiken für die künftigen Anbieter im Automobilmarkt, 2016.

6 The data of connected cars are also interesting for public authorities, e.g. for traffic safety and regulation or law enforcement.

7 Access to the connected car means mobile access of independent service providers to (1) the IT system of the car for either downloading data ("read") or also uploading data or providing services in the connected car ("write") as remote diagnosis or software updates, and (2) the Human-Machine-Interface (HMI or dashboard) for direct communication with the car drivers. If OEMs control this access they can block direct interaction between car drivers and independent service providers. See for the technical details TRL (n 2) 75-92; Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, Digital Economy Working Paper 2018-0X, JRC Technical Reports, 2018, 7-10.

8 See EU Commission 2016 (n 1); C-ITS Platform (n 2).

9 See for these five principles C-ITS Platform (n 2) 75.

10 See C-ITS Platform (n 2) 78-89.

On the C-ITS platform three technological solutions were discussed. For the following analysis and discussion it is sufficient to focus on two basic technological solutions.[11] The first one, the "external server" solution implies that all in-vehicle data are transmitted to an external server (outside of the car) and access to these data is only possible via this external server. The "extended vehicle" concept of the OEMs is one variant of this "external server" solution, in which this is a proprietary server of the OEMs that lead to their exclusive control of the data.[12] Another variant of the "external server" solution is the "shared server" concept. It is technologically the same solution but is not under the exclusive control of the OEMs but under the governance of a neutral entity that can give access to these data to all stakeholders on non-discriminatory terms. The second main technological solution is the "on-board application platform". In this solution the car itself would be the platform, on which the data are stored, and the car owners can decide directly whom to grant access to the in-vehicle data and who can get access to the car for providing services to the car users. Since this technological solution leads to a much more "open" version of the connected car, this solution can also be seen as an open interoperable telematic platform. Thus, the technological choice between these two basic options is important (1) for the question who has control of the data, and (2) for the choice between a more interoperable "open" or a more "closed" model of connected cars.[13]

In the following, the positions of the OEMs and the independent service providers in this policy discussion are briefly summarized.[14] The European car manufacturers are mainly using the extended vehicle concept in their connected cars and are claiming via their associations that this model is the only suitable model for access to in-vehicle data and the connected car.[15] The main argument of the OEMs is that the exclusive control of the access to in-vehicle data and the car is necessary, because it is the only way to ensure the very high standard of safety and security that is necessary for connected (and automated) cars. Due to the risks of cyber-attacks, manipulation, compromising the integrity of the functions of the connected cars etc., all technological solutions that would allow a direct exchange of data with independent service providers would be too dangerous for the safety and security of the car. The responsibility of the OEMs for safety and security is also directly linked to their liabil-

---

[11] For an explanation and analysis of the technological solutions see C-ITS Platform (n 2) 72-90; TRL (n 2) 32-49; and Martens/Mueller-Langer (n 7), 7-13. The third solution, the "in-vehicle interface", is the currently existing On-Board Diagnostic (OBD) Adapter, which is used for transmitting data for emissions control and repair and maintenance services. However it is not such a basic solution as the two solutions described in the following.

[12] In recent publications this variant has also been called "central data server platform" (Martens/Mueller-Langer [n 7] 8) or "centralization of in-vehicle data" (EU Commission 2018 [n 1] 13).

[13] For a very detailed analysis of the advantages and problems of an "open" vs. a "closed" model of connected cars see Determann/Perens, Open Cars, Berkeley Technology Law Journal, 2017, 915-988.

[14] For a deeper analysis of the positions and arguments of the different groups of stakeholders in the ecosystem of connected driving see Specht/Kerber (n 2) 49-55.

[15] See, in particular, ACEA, Access to vehicle data for third-party services. ACEA Position Paper, Brussels, December 2016a; ACEA, ACEA Strategy Paper on Connectivity, Brussels, April 2016b; and VDA, Position. Zugang zum Fahrzeug und zu im Fahrzeug generierten Daten. Berlin, 2016.

ity in regard to the connected car. Therefore safety and security concerns are the reason why the connected car has to be a closed system under the exclusive control of the OEMs. The car manufacturers claim that they are willing to grant access to in-vehicle data on their proprietary servers but only on the basis of freely negotiated B2B-contracts with independent service providers, and they will distinguish in that respect different categories of data.[16] The OEMs also claim that the extended vehicle concept allows the car owner to freely choose between all service providers that have contracts with the OEM in regard to necessary data or access to the car. It is less clear how the OEMs defend their exclusive control of the in-vehicle data. In the position papers only rather general remarks about the huge investments into the development and the operating costs of connected cars can be found.[17]

Despite the heterogeneity of the different groups of independent service providers there is a large consensus in regard to their critique of the OEMs and their extended vehicle concept and possible solutions.[18] Especially repair and maintenance service providers have emphasized the importance of access to in-vehicle data and the possibility to use their knowhow directly in the vehicle, i.e. that they can get direct access to the connected car.[19] Particularly important is that independent service providers can develop and offer many new innovative services (as, e.g. remote monitoring and maintenance) in the automotive aftermarkets and in markets for complementary services.[20] They are concerned that the exclusive control of OEMs regarding access to in-vehicle data and the connected car can impede competition and innovation on these markets. Access via an external server can also impede innovation, because certain new services need access in real-time (whereas the external server leads to time lags). Also access to raw data and not only aggregated or already processed data can be important for new innovative services. Another alleged problem is that OEMs can observe the data access of independent service providers and therefore monitor their transactions with the car owners. These data can lead to a competitive advantage of the OEMs in regard

16 See VDA (n 15) 6 et seq.. There are three exceptions about access to data via free B2B-contracts: Personal data only with explicit consent of the car owners, repair and maintenance information according to the regulated access of the type approval regulation (see below in this section), and anonymised data for the improvement of traffic safety for public authorities.

17 See ACEA 2016b (n 16) 7. Very interesting but not clearly elaborated are also hints about the danger of market dominance through large tech companies if data are made as accessible as possible according to the principle of “free flow of data” (ibid, 1).

18 See FIGIEFA, Commission Communication on "Free Flow of Data". Input from the Independent Automotive Aftermarket, 23 December 2016, AFCAR, Insurance, leasing, dealers, vehicle inspection, automotive aftermarket and consumers coalition: Keeping the principles of the Treaty of Rome alive in the automotive digital age, Press Release, Brussels, 23 March 2017, ADPA et al, EC Mobility Package outlines vision for automated mobility but fails to set out a clear plan for access to in-vehicle data. Press statement, 17 May 2018.

19 See for the following FIGIEFA (n 18) 14-17.

20 See FIGIEFA (n 18) 3: “Foreseeable use cases are for example the proactive monitoring of safety-critical vehicle systems, the predictive ... maintenance in the workshop, remote monitoring of operations to prevent defects, remote maintenance through software updates or reconfiguration and automated services in case of a breakdown on the road”.

to their own services to the car users.[21] These arguments are also relevant for many other independent service providers. Therefore nearly all other stakeholders reject the extended vehicle concept and the "privileged" position of the OEMs and demand, in the short term, non-discriminatory access to the data, and, in the long term, the transition to an "open telematics system" (on-board application platform) that would give the car users direct control of the access to the data and the connected car. This is also in line with the position of the consumer associations who insist on fair and undistorted competition in regard to aftermarket and complementary services and the right of car users to choose freely between all service providers (consumer choice).[22] The consumer associations also demand a clarification about the rights of car owners in regard to the data (including the non-personal data).[23]

Parallel to this policy discussion, the EU has enacted in 2018 a reform of the type approval regulation for vehicles.[24] For a long time competition law had to deal with strategies of the OEMs that tried to foreclose independent service providers from the often highly profitable automotive aftermarkets. Since the 1980s the EU competition policy had implemented regulatory provisions, first in a sector-specific block exemption regulation and since 2007 in the type approval regulation of vehicles that should ensure that competition on these automotive aftermarkets between the OEMs and the independent service providers is not distorted or eliminated through a lack of access to necessary technical information for repair and maintenance services.[25] The main regulatory instrument for achieving this objective was the introduction of an obligation of the OEMs to grant the same access about necessary information for repair and maintenance services to independent service providers as to their own service providers. Therefore, in regard to repair and maintenance services independent providers have had already for a long time regulated access rights to essential technical information and diagnostic data via the OBD ("on-board diagnostic") adapter. This solution of a "regulated access" to necessary technical information for safeguarding fair and undistorted competi-

[21] See FIGIEFA (n 18) 14. These and other critical arguments have already been discussed clearly in the Working Group 6 of the C-ITS platform (n 2, 78).

[22] See BEUC, Protecting European Consumers with connected and automated cars. Position paper, Brussels, 11.12.2017; FIA, Policy Position on Car Connectivity, Brussels, 2016a; FIA, What Europeans think about connected cars, Brussels, January 2016b.

[23] See, e.g., BEUC (n 22) 8. In a survey of European car owners about connected cars 90 % of the participants said that the data that are produced in connected cars should be "owned" by the car owners or the car drivers. See FIA 2016b (n 22) 1.

[24] Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

[25] Regulation (EC) 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information. Regulation (EU) 461/2010 of 27 May 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector. See for this regulation also Becker/Simon, GVO Nr. 461/2010 (Kfz-GVO) Vertriebs- und Kundendienstvereinbarungen im Kfz-Sektor, in: Bornkamm/Montag/Säcker, Münchner Kommentar Europäisches und Deutsches Wettbewerbsrecht (Kartellrecht), 2015, 1173-1234.

tion on the aftermarkets for repair and maintenance service providers is a broadly accepted regulation that has fulfilled its task successfully.[26] Although the reform of the type approval regulation was triggered by the emissions scandal in the automotive industry, it also led to some adaptation of the rules about this regulated access of independent service providers. This reform did not take into account all the implications of the transition from traditional to connected cars, but the extent of the regulated access of independent service providers in regard to data and the car under these new technological conditions, e.g. also for providing new services (by using remote access), was also discussed in this context. In the end, the respective changes in the type approval regulation have remained rather limited, but it is clear that this regulatory access solution will be subject to further regulatory discussions in the future with the same conflict between the OEMs and independent service providers.[27]

Since already in the C-ITS platform discussions the conflict between OEMs and independent service providers about access to in-vehicle data and resources could not be resolved between the stakeholders, it was a logical next step that the EU Commission initiated a study with the task to investigate to what extent the different technological solutions are compatible with the above-mentioned five C-ITS guiding principles about access to in-vehicle data and resources (TRL 2017). This (so far still the most comprehensive) study about this access problem led to the following results:[28] All technological solutions are technically and legally feasible (also in regard to safety and security) but they each have different advantages and problems. Although no solution is superior in regard to all five principles, the study comes to the conclusion that the “on-board application platform” is the relatively best solution. Particularly important for this result is that the extended vehicle concept is assessed as being incompatible with the principle of fair and undistorted competition. The study discusses a number of possible policy measures which differ in regard to the time horizon and the depth of policy intervention. This discussion clearly suggests that in the short-term (under the current technological “external server” solution) the variant of the “shared server” would lead to more compatibility with the principle of fair and undistorted competition. However for ensuring a far-reaching compatibility with this principle, the interoperable on-board application platform is recommended in the long-term. The study acknowledges the safety and security challenges of this solution but deems them to be solvable. The study recommends to encourage the development of a single interoperable platform but in the end does not go so far as to recommend making such a platform mandatory for the OEMs.[29]

What is the state of the current policy discussion? Despite the results of the TRL study the conflict between OEMs and the independent service providers could not be resolved. Whereas the independent service providers still demand legislative action, esp. in regard to “shared server” and interoperable platforms solutions, the OEMs reject legislative measures

---

[26] See European Commission, Study on the operation of the system of access to vehicle repair and maintenance information, Final report, 2014.

[27] Important changes of the type approval regulation refer to rules about the support of repair and maintenance services through wireless networks and the access to remote diagnosis services of the OEMs.

[28] See TRL (n 2) 8-16.

[29] See TRL (n 2) 160.

and want to stick to their extended vehicle concept. On February 2018, the European Parliament demanded that the Commission publishes a legislative proposal on access to in-vehicle data and resources with the explicit objectives of maximum security and a level-playing-field for access for all third-parties "… to protect consumer rights, promote innovation and ensure fair, non-discriminatory competition on this market …".[30] In its Communication "On the road to automated mobility" (May 2018) the Commission acknowledged the competition problems and that the "centralisation of in-vehicle" data in the extended vehicle concept might "not be sufficient to ensure fair and undistorted competition between service providers".[31] But the Commission seems to be reluctant addressing this problem, and therefore is not planning legislative actions with binding rules but wants to solve the problems by publishing a recommendation with "guidance on a data governance framework for access to and sharing of data generated by connected vehicles" based upon non-binding principles.[32]

C. Data Governance in Connected Cars: An Economic Analysis of Potential Market Failures

I. Introduction

Can we rely on the market for finding appropriate solutions for the governance of data in the ecosystem of connected and automated mobility or do serious market failure problems exist that require policy solutions? This section C has the task of identifying and discussing potential market failure problems in regard to the data governance problem from an economic perspective.[33] Although the policy discussion about access to data has focused primarily on the conflict between OEMs and independent service providers, the policy problems in regard to the governance of in-vehicle data and connected cars are much more complex.

For the analysis of this complex data governance problem also the law and economics of data have to be taken into account. Important from a legal and normative perspective is first that most of the data in the connected car are personal data that are subject to European data protection law, which grants the data subjects (i.e. the car users) a set of strong rights in regard to these data for helping them to protect their privacy. Therefore OEMs but also other firms that would like to use their data need the consent of the car users[34] for the processing

30 See EP, Report on a European strategy on Cooperative Intelligent Transport Systems (2017/2067(INI)). Committee on Transport and Tourism (PE610.712v02-00), 2018, 10.

31 EU Commission 2018 (n 1) 13.

32 See EU Commission, Roadmap Cooperative, Connected and Automated Mobility (CCAM), Ref. Ares(2018)5386378 – 19/10/2018, 2.

33 Martens/Mueller-Langer (n 7), and Kerber/Frank, Data Governance Regimes in the Digital Economy: The Example of Connected Cars, 2017, available at: https://ssrn.com/abstract=3064794, seem to be the only papers that have analyzed this access to in-vehicle data problem from an economic perspective. The TRL study (n 2)) also takes economic effects into account but does not analyze market failures.

34 For some (mostly legal) issues (e.g., data protection) it is necessary to distinguish between car owners, car drivers, and car passengers. In this paper we cannot go into the details of this problem.

and use of these data.[35] Thus, it is also necessary to discuss whether the car users are capable of making rational and well-informed decisions about permitting the OEMs (or other firms) the use of their personal data, and whether they are offered sufficient privacy options for being able to protect their privacy. Secondly, in regard to non-personal in-vehicle data, which might be certain kinds of technical data and, in particular, the huge mass of anonymized data no clear legal rights exist, esp. no property rights for data.[36] The discussion about data rights however has shown that an exclusive de facto control of non-personal data by a data holder leads from an economic perspective to a de facto (but not legal) "ownership" of these data. But due to the non-rivalry in the use of data, it is unclear whether such an exclusive "ownership" of data is an economically efficient governance solution. Especially in multi-stakeholder situations as the ecosystem of connected and automated driving, in which the same in-vehicle data can be used for the value creation of many service providers, it is very doubtful whether the exclusive (monopolistic) control of these data by one stakeholder leads to an efficient way of using the data.[37] Therefore the specific economic characteristics of the data and the data economy are also an important input for the following analysis about appropriate solutions for the governance of the in-vehicle data of connected cars.[38]

The analysis in this section is structured as follows. In section II we will analyze how the technological decisions of the OEMs, as choosing the extended vehicle concept or the onboard application platform, determine who has de facto control of the in-vehicle data and might therefore be able to appropriate the benefits of these data. Section III offers a critical analysis of the main argument of the OEMs that the extended vehicle concept with its exclusive control of the access to data and the car is necessary for ensuring the necessary high level of safety and security of connected driving. Section IV analyzes the potential negative effects of the extended vehicle on competition and innovation on the markets for aftermarket and complementary services. In section V it will be shown that competition between OEMs does not necessarily lead to optimal technological decisions in regard to interoperability and standardization leading to a potential market failure in regard to technological choice. This is

---

We therefore will mostly use the general term car users and only in some specific contexts use explicitly the terms car owners or car drivers, where this specific role is relevant (e.g. in regard to buying a car).

[35] For the relevance of European data protection law for data in connected cars, see Hornung, Verfügungsrechte an fahrzeugbezogenen Daten. Das vernetzte Automobil zwischen Wertschöpfung und Persönlichkeitsschutz. Datenschutz und Datensicherheit, 2015, 359-366, Hornung/Goeble, "Data Ownership" im vernetzten Automobil. Computer und Recht 2015, 265-273.

[36] These data might be subject to trade secret protection but this does not grant a property-like legal position. See for this discussion Zech, A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. Journal of Intellectual Property Law & Practice, 2016, 460-470, and in more detail section D.II.

[37] See Kerber (n 4)109-133.

[38] See for contributions about the economics of data and the data economy OECD, Data-driven innovation: Big data for growth and well-being, 2015; Kerber, A new (intellectual) property right for non-personal data? An economic analysis. GRURInt, 2016, 989-998; Duch-Brown/Martens/Mueller-Langer, The economics of ownership, access and trade in digital data. EC JRC Technical Reports Working Paper 2017-01, 2017; Kerber (n 4) 109-133; Schweitzer/Peitz, Datenmärkte: Funktionsweise und Regelungsbedarf. Diskussionspapier 17-043, Mannheim: ZEW, 2017.

followed by an analysis of potential market failures due to information and behavioral problems of car users in regard to their consent to the use of their personal data and the protection of their privacy (section VI). Section VII offers a brief analysis to what extent these potential market failures might be mitigated by competition between the manufacturers of connected cars (section VII). The results of section C are summarized in the concluding section VIII.

II. Technological decisions and de facto control of data and access to the car

What are the economic implications of the technological decision of OEMs for the "extended vehicle"? Since all in-vehicle data are transmitted directly to proprietary servers of the OEMs, they are obtaining de facto exclusive control of these data. Neither the car users nor other stakeholders can get access to these data without the consent of the OEMs. In that respect, the OEMs have gotten the de facto (but not legal) "ownership" of these data and might therefore be capable of appropriating the economic value of these data.[39] Additionally, the extended vehicle concept also implies that the OEMs also have the exclusive control of the access to the connected car, i.e. without the consent of the OEMs independent service providers cannot exchange data with the connected car nor communicate with the car drivers via the integrated Human-Machine-Interface (HMI). Therefore, the connected car is a closed system (similar to Apple's IPhone). As far as the OEMs have exclusive control of in-vehicle data and the access to the connected car, all independent service providers who would like to offer services to the car users need the consent (and therefore contracts) with the OEMs for being granted access (1) to in-vehicle data that they need as indispensable input for their services and/or (2) to the connected car, if they need access either to the IT system or the HMI of the car for providing these services and/or communicating with the car users.[40] As far as OEMs have exclusive control, also the consumers can only choose between those service providers who have contracts with the OEMs. Since the connected car is an expensive durable good, the car owners are "locked in" the closed system of the OEMs. Therefore, the OEMs are in a "monopolistic" gatekeeper position in regard to the in-vehicle data[41] and the connected car, and can increase their profits by "selling" access to the users of the connected car to the independent service providers.

Technological alternatives would lead to different data governance solutions. The "on-board application platform" – the technological architecture favored both by the TRL study and in-

39 This de facto exclusive control of these data is only limited by (1) the regulated access for repair and maintenance information (type approval regulation), and (2) by the rights of the car users in regard to their personal data, but these rights do not extend to non-personal data (and therefore the anonymized data sets from these personal data).

40 These distinctions are important, because the exclusivity of the control of the access to the in-vehicle data and the car by the OEMs is limited by alternative channels for getting data and/or for communication with the car users (as, e.g. through smartphones). Therefore, e.g., location data and data about the traffic situation might not be exclusive, because this information might also be gotten from the smartphones of the car users or from connected cars from other brands. The importance of the number of data access channels is emphasized by Kerber/Frank (n 33), 41 and Martens/Mueller-Langer (n 7) 24.

41 See also Martens/Mueller-Langer (n 7) 14.

dependent service providers[42] – would offer the possibility that car users can decide where the data are stored and whom they grant access to the in-vehicle data and/or the connected car. Therefore, it would be the car users who have the exclusive control. In this case they can choose freely between all service providers without the need to have contracts with the OEMs. As a consequence, the car users would be the de facto "owners" of these data and can use them for their own benefit, either through choosing the most attractive offer from service providers and/or by "selling" these data to the highest bidder. With this technological solution the OEMs would have lost their "monopolistic" gatekeeper position in regard to the in-vehicle data. Hence, from an economic perspective the technological solution determines the initial allocation of the de facto exclusive control of data and thus the initial allocation of the de facto "ownership" of data.[43] It also decides to what extent the connected car is a "closed" or an "open" system, i.e. whether the manufacturer of a primary product (here the connected car) does also exclusively control the access to the connected car for aftermarket and complementary service providers, and whether and to what extent the consumers are "locked in" (see below section IV).[44]

III. Justification of the "extended vehicle" through safety and security concerns?

The OEMs defend the extended vehicle concept with the argument that only through this technological solution (with an external server) a maximum standard of safety and security can be ensured.[45] There can be no doubt that in regard to connected and (automated) driving safety and security issues are very important, esp. for the car users. In the current policy discussion the problem of access to in-vehicle data and resources is primarily been seen as a trade-off problem between safety and security on the one hand and fair and undistorted competition on the other hand. However, it can be asked whether and to what extent such a trade-off exists. We will analyze this problem in two steps.

In a first step, we ask whether the external server solution (as part of the extended vehicle concept) and the on-board application platform can solve the safety and security problem. This is a technological question that has to be answered by technical and IT experts. The TRL report came to the conclusion that both the on-board application platform and the external server solution can solve the safety and security problems, although there might be cost advantages for the external server solution.[46] Among IT experts there is a wide-spread opinion that closed proprietary systems need not be more secure than well-designed open systems; on the contrary, the often multi-layered architecture of interoperable open systems

---

[42] See section B.

[43] See Kerber/Frank (n 33) 28. It is however important to take into account that through contractual arrangements between the car owners and the OEMs this position of exclusive control of data and therefore the de facto "ownership" can be traded between the contracting parties; see also section C.VI.

[44] See Determann/Perens (n 13).

[45] Safety and security refer to the safety of the car but also to cybersecurity of the connected car, which also can encompasses the security of the personal data see ACEA 2016b (n 15) 5.

[46] See TRL (n 2) 77.

might even offer better protection against cybersecurity attacks.[47] Since also OEMs offer direct access to their connected cars to some service providers, with whom they have contractual arrangements, ensuring a sufficiently high level of safety and security seems to be possible also for direct access to the connected car. However it is clear that an open interoperable telematics (on-board application) platform need the implementation of a sophisticated safety and cybersecurity system. One part of the solution might be the separation of safety- and security-sensitive functions and data from the vast amount of other data, which are not related to safety and security.[48] Particularly important is however to strictly control whether independent service providers who want to offer their services to the car users fulfill certain standards for safety and security of their services, e.g. in regard to apps and software that are uploaded to the connected car. This can be implemented by requiring a certification of these service providers.[49] In addition to that, the medium- and long-term development of integrated mobility systems with connected, automated, and later autonomous cars would require in any case the development of a comprehensive safety and security architecture with interoperable brand-independent industry-wide interfaces between connected cars and other entities. Therefore, solving the safety and security problems of interoperable telematics platforms, e.g. also by establishing a comprehensive system of certifications for safety and security, is in any case one of the important tasks for achieving the policy objective of a future integrated mobility system of connected and automated driving.[50] [51]

Most important for the governance of the in-vehicle data is, however, that safety and security concerns do not lead to a justification for the exclusive economic control of the in-vehicle data through the OEMs.[52] Even if we assume that it is necessary that all data have to be transmitted to an “external server” and the OEMs must have exclusive control of the access to the IT system of the car due to safety and security reasons, this does not lead to a justification that they also need to be the de facto exclusive “owners” of these data with the right to exploit these data commercially. In regard to connected cars the OEMs can also be seen as service providers of IT security who have the task of keeping the car and its data safe and secure, whereas the car users still retain the right to decide who should get access to the in-vehicle data of the car or to “sell” these data to other firms. Therefore even if safety/security problems make it necessary that the OEMs control exclusively the access to the car and the data, it is not clear at all, why the OEMs also should have the right to decide freely and according to their own interests who can get access to the car and/or the data, and can exploit these decisions about access to increase their profits. The extended vehicle concept thus

47 See in more detail TRL (n 2) 75-79; Determann/Perens (n 13) 939-942, and Martens/Mueller-Langer (n 7) 12.

48 This could be achieved by using so-called hypervisor technologies (TRL [n 2] 8).

49 Certification was also the regulatory solution in regard to solving quality concerns in regard to the products of independent spare part producers in the automotive industry.

50 See EU Commission 2018 (n 1) 9.

51 Particularly important is the solving of liability problems. See also Determann/Perens (n 13) 984-986, in regard to the general problems with liability in the case of open systems. This is however no serious argument against interoperable telematics systems. If the safety and security problems can be solved, then also suitable solutions for the assignment of risks in tort law can be found.

52 See also Kerber/Frank (n 33) 54.

entails a bundling of the task of providing safety and security services with the transfer of de facto ownership rights of the data to the OEMs, which is not necessary and lacks economic justification. These are two different roles that can easily be separated and unbundled.[53] One simple "unbundling" solution in the case of an "external server" solution is the already much discussed "shared server" solution, in which the external server is not under exclusive control of the OEM but under the control of an entity that is independent from the OEMs. This entity then can give access to these data on a non-discriminatory basis according to certain general principles (e.g. FRAND conditions), and would therefore eliminate the privileged position of the OEMs in regard to the data. In the case of the "on-board application platform" it is clear that it is the car user who has de facto "ownership" of the data and the right to decide on the access to the car, and the OEMs are "only" service providers for safety and security of the car.

Therefore this section leads to the following results:
(1) The exclusive ("monopolistic") control of the in-vehicle data in the extended vehicle concept that allows the OEMs to appropriate the economic value of the data cannot be defended through safety and security concerns. Even if exclusive control of the access for solving safety and security problems is necessary, this does not imply that the provider of safety and security also need to have the right to exploit the commercial value of the data. Both roles can be easily unbundled.
(2) But, additionally, it is also very doubtful whether an external server solution and the car as a closed system with the exclusive control of the OEMs about the access to the car is necessary at all for safety and security. There seem to be good reasons to believe that the same (or even a higher) level of safety and security can also be achieved by using an "on-board application platform" with a sophisticated safety and security system.
(3) As a consequence, the basic assumption of the current policy discussion that there is a fundamental trade-off between the objectives of safety/security and fair and undistorted competition is deeply flawed. There is definitely no such trade-off in regard to the access to the in-vehicle data, and it is also very doubtful whether there is such a trade-off in regard to access to the connected car.
(4) Another conclusion is that it is necessary to analyze the safety and security problems as part of the medium- and long-term technological architecture of an integrated ecosystem of connected and automated mobility (see below section C.V).

IV. Competition problems on aftermarket and complementary markets

In section B we have seen that both the independent service providers and the consumers are very concerned that the exclusive control of the OEMs in regard to the data and access to the connected car can impede competition and innovation on the markets for aftermarket

[53] A firm who hires a security service firm for the task to control the access to this firm (either physically or in regard to its IT system) does not give the security firm simultaneously the right to decide freely whom to give access to the firm and whom not, and therefore allowing the security firm to "sell" access to this firm. The right to decide who gets access will remain with the firm. The security firm has only the right (and duty) to deny access in the case of clearly defined safety and security risks.

services and complementary services in the ecosystem of connected driving. The problem how to ensure fair and undistorted competition for independent service providers has been raised in the Working Group 6 of the C-ITS platform, confirmed by the TRL study, and has been acknowledged by the EU Commission as an unsolved problem.[54] From a competition economics perspective, the competition concerns have to be taken very seriously. As far as independent service providers need access to in-vehicle data and/or the access to the connected car, the OEMs can control a necessary ("essential") resource for providing these services. This position allows them to foreclose independent service providers. This is an old well-known competition problem in the automotive industry,[55] and the long-existing regulatory efforts of European competition policy for protecting competition on markets for automotive repair and maintenance services and spare parts, which led to the solution of a "regulated access" to necessary technical information (see section B), have always focused on exactly this problem. Since in regard to connected driving many more new and innovative services are expected to be offered, the problem of foreclosing competition and leveraging market power has gotten much more important than in the traditional case of repair and maintenance services. It is also important that the problem is not limited to automotive aftermarket services but encompasses also the wide range of many other innovative services for the users of connected cars (complementary services),[56] which are also often the result of new data-driven innovation.

The exclusive control of the data and the car allows the OEMs several options for increasing their profits through this gatekeeper position in regard to these markets. One option is to deny access in order to block the entry of service providers for specific kinds of services, which then could be offered exclusively by the OEMs themselves. If these markets promise particularly high profits, then monopolizing these markets can be one strategy for making profits through foreclosure strategies. Another option is to "sell" access to these data and the car to independent service providers who would like to enter these markets. This can be done by concluding B2B-agreements with service providers who, for a certain price, can get access to data and / or the IT system of the car, which can be interpreted as an entry fee into the relevant markets. This can also lead to exclusivity agreements, i.e. that such a "license" to sell services in the connected car is granted only to one service provider (for a high "fee" that allows the OEMs to reap the profits from such an exclusive position of providing a specific service for the cars of a particular brand). But even if the OEMs grant access to a number of service providers, the OEMs via their contractual relationships with these firms remain in control of the aftermarkets and complementary services. Irrespective of the option the OEMs

---

54 See EU Commission 2018 (n 1) 13.

55 For the economics of aftermarkets and its discussion in competition law see Shapiro, Aftermarkets and Consumer Welfare: Making Sense of Kodak, Antitrust Law Journal, 1995, 483-511; Borenstein/MayKie-Mason/Netz, Exercising Market Power in Proprietary Aftermarkets, Journal of Economics & Management Strategy 9, 157; Bauer, Antitrust Implications of Aftermarkets, Antitrust Bulletin 52, 2007, 31, and Bishop/Walker, The Economics of EC Competition Law, 2010, 150-152, 245-249.

56 The term "complementary services" encompasses all services that are useful for the car users only in connection with the connected car, especially during driving. Therefore the car and these services are economically complements. In that respect there is from an economic perspective no difference between aftermarket services and other complementary services.

choose for maximizing their profits,[57] there are no independent markets for aftermarket and complementary services any more, and the OEMs can reap all (or most) of the profits. Also the concern that such market control can lead to less innovation of new services has to be taken very seriously from an innovation economics perspective, because it enables the OEMs to filter which innovative services are offered to the car users. An additional way of monetizing the data is the selling of (anonymized) data sets for all kinds of other uses outside of the automotive industry and the ecosystem of connected and automated driving. Since many of these data sets are unique and not replicable, there is a danger that the ensuing monopolistic prices will lead to welfare losses through an under-utilization of these data in the data economy.[58]

Also other variants of the external server solution have been discussed. One variant is that "neutral servers" (operated by independent entities) might be established that provide in-vehicle data to other stakeholders under non-discriminatory terms. This neutral server solution however suffers from the problem that the in-vehicle data are still first transmitted exclusively to a proprietary server of the OEMs, who are free to decide what data they make available under what conditions in free B2B-agreements to the operators of these neutral servers. Therefore the OEMs can still apply the same strategies as described in the last paragraph. The only difference is that the OEMs cannot make direct contracts with the users of those data that are made available to the neutral servers, which limits their options for controlling the use of these data to some extent.[59] Whereas such a neutral server solution is not a solution for the competition problems, this is different for the already mentioned "shared server" solution. Since in this case the in-vehicle data are transmitted directly to an external server operated by a neutral entity, the OEMs lose their monopolistic gatekeeper position in regard to in-vehicle data. This leads to a level playing field in regard to the access to the data, and therefore removes one important hurdle for ensuring fair and undistorted competition on the markets for aftermarket and complementary services. However, a shared server would not necessarily solve all competition problems on these markets, because the OEMs might still block independent service providers via their exclusive control of the access to the car. A transition to an open on-board application platform might also solve this problem.

---

[57] Please note that the OEMs with their extended vehicle concept insist on freely negotiated B2B agreements (ACEA 2016a [n 15]), i.e. that it is in their discretion what kind of profit-maximizing strategy they use.

[58] See Martens/Mueller-Langer (n 7) 14-17, who also analyze pricing strategies of OEMs for selling access to data (monopoly pricing, price discrimination).

[59] One benefit of this neutral server solution can be that it might help to mitigate the concern of the independent service providers that by monitoring their proprietary server the OEMs can observe the transactions between car users and independent service providers, which might give them an advantage in regard to the offering of their own services. This is a wide-spread concern of independent service providers. See C-ITS Platform (n 2) 79. Please note that the same competition problem is discussed currently in regard to transaction and user data on platforms as Amazon. Here the concern is that those platforms can use these data for favoring their own services (see Schweitzer/Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018, 142) as well as the current Amazon investigation of the EU Commission (see https://www.businessinsider.de/amazon-investigated-by-eu-commissioner-margrethe-vestager-2018-9?r=US&IR=T).

Therefore from a competition economics perspective, there can be no doubt that the OEMs with their exclusive control of the in-vehicle data and the access to the car can eliminate competition on markets for aftermarkets and complementary services. In that respect, the concerns of the independent service providers about the implications of the extended vehicle concept are justified. However from an economic perspective an important counterargument has to be considered. It also has to be asked whether competition between the OEMs is capable of solving the problem of ensuring an efficient provision of aftermarket and complementary services and with prices on a competitive level, even if the OEMs have exclusive control of these markets. Competition between OEMs can also be seen as competition between connected cars as bundles of the car itself and a set of aftermarket and complementary services ("system competition"). It can be argued that if competition between OEMs works very well, then they might be under enough competitive pressure for offering attractive bundles of cars and services at competitive prices. Otherwise car buyers would switch to the connected cars of other brands. This is a standard argument in the economic theory of aftermarkets. This question also has emerged in competition law in respect to defining the relevant markets in the automotive industry. Is the relevant market an aftermarket for a specific brand, because consumers are "locked in" after they bought a particular car? This would lead to the conclusion that an OEM is a monopolistic (dominant) firm in regard to aftermarkets and complementary services, which depend on the access to the data or the car. Or do the car buyers decide between different bundles of cars and services of OEMs leading to the definition of "system markets"?

Can competition between bundles of OEMs and aftermarket and complementary services work well enough for solving the problems of exclusive control of OEMs? This problem has been discussed in competition economics extensively,[60] e.g. for the well-known printer/toner problem. If we assume that the consumers are rational and well-informed about the future costs of the specific toner they need before buying a printer, then the ensuing result that the buyers are getting locked-in in regard to the toner is no problem, because they would already have taken this into account in their buying decision in regard to the printer. However, even in regard to this relatively simple lock-in problem, consumers seem to have considerable problems in dealing with it. In regard to connected and automated mobility these problems are much larger for the car buyers. It is very hard for car buyers to make reliable estimations about the future costs of being locked into such a bundle. The car buyers cannot know what kinds of services with what prices the OEMs will offer during the lifetime of a connected car. In the same way they will not know what kind of choice between different service providers the OEMs will offer them in two, five, or eight years.[61] Therefore it is very doubtful whether the car buyers can appropriately calculate the long-term costs (and benefits) of the aftermarket and complementary services that are part of this bundle. As a consequence, it is very unclear whether system competition between OEMs can work sufficiently for solving the

60 See Shapiro/Teece, Systems Competition and Aftermarkets: An Economic Analysis of Kodak, Antitrust Bulletin, 1994, Shapiro (n 55), Borenstein et al (n 55), Bauer (n 55), Bishop/Walker (n 55) 150 et seq., 249 et seq.

61 Selling the connected car in the case that OEMs later diminish the choice or increase prices for these services is not a solution, because this will lead to lower prices of the used cars.

competition and innovation problems on the markets for aftermarket and complementary services. It should be noted that if system competition between OEMs would have worked effectively in the past, the decades-long efforts in competition law for protecting competition in the markets for repair and maintenance services (as well as spare parts) would not have been necessary. Since connected and automated cars are much more complex in regard to services than traditional cars, we should be very cautious in relying on the effectiveness of systems competition between OEMs in regard to these services.

V. Market failures in regard to technological choice: interoperability and standardization problems

In economics we usually assume that the firms should be free to decide on the technological design of their innovations and that the market is capable of selecting the superior technologies. If the OEMs choose the extended vehicle concept and this solution also prevails in the markets (as it is widely expected without regulatory intervention),[62] the question arises whether it is also the most efficient technological solution or whether there might be a market failure problem about technological choice. The TRL study came to the conclusion that in the long-term the on-board application platform would be superior to the extended vehicle concept (with its external server)[63] and also our analysis will suggest a similar result. Economic research has identified a number of cases, in which profit-maximizing firms can choose inefficient technologies and/or markets are not capable of selecting the best technologies.[64] Since in the future ecosystem of connected and automated mobility, interconnectivity and real-time exchange of data between cars, infrastructure, private firms, and public institutions will be necessary for a well-functioning integrated mobility system, interoperability and standardization are important issues in this mobility ecosystem. Therefore it, can be asked about potential market failure problems in regard to interoperability and standardization.

One interoperability issue refers to the question whether OEMs choose a proprietary and closed technological system for the connected car or an open interoperable system, in which the car users can decide about the access to the connected car. The economics of interoperability shows that both open and closed systems can have benefits and costs, and that a deeper economic analysis is necessary for answering the question which one is superior in a

62 See TRL (n 2) 13.

63 See TRL (n 2) 170.

64 In one group of cases dynamic economies of scale (learning effects) or network effects can lead to path dependencies which might result in the lock-in of old technologies that are hard to be replaced by the market with newer more efficient ones. The famous QWERTY-problem is another example. See, e.g., Katz/Shapiro, Network Externalitites, Competition and Compatibility, American Economic Review 75, 1985, 424; David, Clio and the Economics of QWERTY, American Economic Review 78, 1988, 332.

specific case.[65] Our discussion about the effects of the extended vehicle concept vs. the on-board application platform can be seen as part of such an assessment of the advantages and costs of interoperability in regard to connected driving. Since one of the benefits of interoperability can be more innovation, the question arises whether a closed system would lead to more innovative solutions (e.g., due to synergies between the connected car and other services within the system) or whether it can be expected that, due to open interfaces, an open system that allows for independent innovation activities of service providers would lead to more innovative services within the ecosystem of connected and automated mobility. So far the OEMs have not claimed that their closed systems will lead to more innovation in regard to aftermarket and complementary services, whereas the independent service providers are emphasizing the huge potential of new innovative services. Therefore, it is necessary to carry out a much deeper analysis of the advantages and costs of interoperability to decide which degree of closeness or openness of the connected car would be optimal. If competition between entire systems (bundles of cars and services) does not work well, as we suggested in the last section in regard to connected cars, then it is doubtful whether individual profit-maximizing decisions of the manufacturers of the primary products (here: the connected cars) lead to optimal decisions about interoperability in regard to complementary services. Rather the firms tend to choose too often a proprietary closed system.[66]

However, interoperability is also very relevant at the level of the entire integrated ecosystem of connected and automated mobility. Due to the long-term need for direct communication and data exchange between vehicles, infrastructure, private firms and public institutions far-reaching standardization processes in regard to communication, data formats and categorization, safety and cybersecurity issues and other technological features are necessary, which require industry-wide standardized interfaces between the vehicles and the overall technical architecture of the mobility system. The connected, automated and later autonomous car must be an integral part of this system, i.e. the cars have to fit into the overall architecture and therefore have to comply with standardized technical interfaces for being capable to interoperate with many other parts of this ecosystem. Therefore an (to some extent) open and interoperable on-board application platform has to be developed in any case in the next steps of the automation of the connected cars.[67] The economics of standard-setting has shown that these kinds of uniform standards at the level of the entire mobility system cannot

---

65 On the one hand, more open systems with more interoperability can offer the consumers more choice, innovation and competition between complementary products and services that they can use in combination with this system, on the other hand, closed systems might have advantages in terms of more differentiation and a higher quality of services due to a better integration between the system and these complementary services. See for the economics of interoperability Choi/Whinston, Benefits and requirements for interoperability in the electronic marketplace, Technology in Society 22, 2000, 33; Gasser, Interoperability in the Digital Ecosystem, 2015, 9-17; available at: http://ssrn.com/abstract=2639210, and as overview Kerber/Schweitzer, Interoperability in the Digital Economy, JIPITEC, 2017, 39, 41 et seq.

66 For the general complaint in the digital economy about too many proprietary solutions and not enough interoperability see, e.g., PwC, Cross-cutting Business Models für IoT. Final report (SMART number 2017/0027), Brussels, 2017, 132.

67 See Martens/Mueller-Langer (n 7) 13 about the necessity of on-board application platforms for automated and autonomous driving.

emerge in market competition.[68] Although the decisions of the OEMs for the extended vehicle concept might seem to be profit-maximizing (at least in the short- or medium-term), in such situations their individual incentives might lead them to technological decisions that are not optimal for the entire ecosystem. Therefore it is necessary to find a solution for this market failure problem. This can be done by a collaboration of all relevant stakeholders in this ecosystem in order to develop the most suitable technological standards and interfaces.[69]

VI. Information and privacy problems of consumers

The discussion on the governance of in-vehicle data has been dominated by the conflict between the OEMs and independent service providers about access to in-vehicle data. Much less attention has been paid to potential market failures in regard to the interests of the consumers, i.e. the car users. First it is important to understand that buying a connected and automated car requires not only a traditional sales contract but also contracts about services (and software updates etc.) as well as contractual provisions about the consent of the car users for the processing and the use of personal data in the connected car. Therefore both parties are de facto in a long-term relationship, which implies a much larger "lock-in" problem for the car owners than in regard to traditional cars. This "lock-in" problem does also exist in the solution of the "on-board application platform", but is much more serious in the "extended vehicle" concept, where the OEMs also can control additionally many aftermarket and complementary services and the consumers are "locked-in" in the entire bundle of car and services (see section C.IV). However, in the following, we want to focus on the problem whether there might be a market failure problem in regard to giving consent for using personal data and the protection of privacy. The following reasonings refer again mainly to the extended vehicle concept.

In the discussion about privacy problems in the digital economy and the issue of "data as counterperformance" for "free services" as in regard to the Google search engine or social media (Facebook), serious concerns have been raised, whether the "notice and consent" solutions in standard form contracts for giving digital companies permission to use their personal data work in a satisfactory way.[70] This refers to the problem of transparency about the

---

[68] Due to the advantages of compatibility often only one uniform (and monopolistic) standard can exist. In the economics of standard-setting it has been shown that markets have large problems to find and establish efficient standards in an uncoordinated way. The main problem is that profit-maximizing individual firms often have incentives for choosing technological standards that are not aligned with the overall welfare effects of these standards. Due to these market failure problems, many standards are developed through standard-setting organizations (SSO), in which firms collaborate in regard to new standards. See for an overview about the economics of (the market failure problems of) standard-setting Farrell/Simcoe, Four Paths to Compatibility, in: Peitz/Waldfogel, The Oxford Handbook of the Digital Economy, 2012, 34-58.

[69] Efforts for standardization for improving interoperability are already taking place both at the EU and the international level. See TRL (n 2) 58-67, and EU Commission 2018 (n 1) 4-8.

[70] See, e.g., European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion, 2014; Borgesius, Behavioural Sciences and the Regulation of Privacy

extent of data collection and use of the data, whether users are aware of the value of their data, about the problem whether there is a real choice, if without giving consent these services cannot be used, and related to that, whether enough privacy options are offered, i.e. that users can make granular decisions about providing personal data according to their specific privacy preferences. All of these problems are also relevant in regard to the personal data of the connected cars. In the context of the "privacy paradox" discussion it has been argued that due to information and behavioral problems users might often not be capable for making rational, well-informed decisions about providing personal data and protecting their privacy.[71] Therefore, it is necessary to do more research about the contractual arrangements between car owners and OEMs in regard to the provision of personal data and the possibilities for protecting their privacy, and ask whether also in this context market failure problems and unsolved privacy problems exist.[72]

In the current policy discussion about data governance in connected cars there is a consensus that the privacy of the car users has to be protected. However so far not much specific discussion can be found how this should be achieved. In a recent survey car owners in the EU were very concerned about disclosure and commercial use of personal data in connected cars, and emphasized their wishes for being able to make more granular decisions about the provision of personal data.[73] This can imply that car users do not have to give generally consent to the processing and use of personal data, but that, e.g., car users can decide for each ride whether, e.g., location data are transmitted or not. The experiences with the privacy policies in other digital contexts do not support the belief that competition between OEMs might be enough for leading to privacy-friendly solutions for car users. Therefore a discussion about additional regulatory solutions (perhaps also in the form of self-regulation) might be necessary for supporting privacy-by-default solutions and offering sufficient choice between different privacy options.[74]

Another very interesting question is whether the car users should also have rights in regard to the non-personal data of their cars, esp. also concerning the anonymized sets of (their) data, and to what extent they get a (fair) share of the value of the data of their connected

---

on the Internet, in: Alemanno/Sibony, Nudging and the Law – What can EU Law learn from Behavioural Sciences?, 2015, 179-207.

71 For the privacy paradox, and the (behavioral) economics perspective see Norberg/Horne/Horne, The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 2007, 100-126, Kokolakis, Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. Computers & Security, 2015, 122-134, Hermstrüwer, Contracting around privacy: The (Behavioral) Law and Economics of Consent and Big Data. JIPITEC, 2017, 9-26, and Acquisti/Wagman/Taylor, The Economics of Privacy, Journal of Economic Literature, 2016, 479.

72 For a skeptical view about individual consent in regard to protecting privacy in connected cars, see from an U.S. perspective Akalu, Privacy, consent and vehicular ad hoc networks (VANETs). Computer Law & Security Review, 2018, 37.

73 See FIA 2016b (n 22) 15.

74 In that respect also the discussion about Personal Information Management Systems (PIMS) can be relevant. See European Data Protection Supervisor, EDPS Opinion on Personal Information Management Systems. Opinion 9/2016.

car.[75] This is a very difficult problem that cannot be analyzed here in detail. Therefore only a few remarks can be made. There is a wide-spread opinion that the owner of a car should also "own" the data that are produced in the car ("MyCarMyData" [76]). However, from an economic perspective, it has to be taken into account that providing data to the OEMs can be seen as an example of "data as counterperformance" as part of the contractual arrangements between OEM and the car owners, which from an economic perspective might lead under competitive conditions on the car market to lower prices for the car and its services. In this case the car owners might indirectly participate in the value of the data. However, it also has to be taken into account whether this mechanism really works sufficiently.[77] All of these questions need much more research. They also arise to some extent with the technological solution of the "on-board application platform" solution; however in this case the car users could "sell" their data also directly to other firms than the OEMs.

VII. Can competition between car manufacturers solve the market failure problems?

Competition between OEMs can only have a very limited effect on market failures through information and behavioral problems of consumers in regard to giving their consent to the provision of data and protecting privacy. Competition between OEMs can also not solve the potential market failure problems in regard to choosing the optimal technologies concerning technical standards and interoperability in regard to an optimal technological architecture for an integrated ecosystem of connected and automated mobility. Since there are good reasons to be skeptical about the effectiveness of systems competition between OEMs, it also cannot be expected that this competition would solve the competition problems on the market for aftermarket and complementary services that are caused by the exclusive control of the access to the in-vehicle data and the car in the extended vehicle concept. But from a competition economics perspective the question of the impact of competition between OEMs is very important and needs much more research. In that respect it is also important that competitive pressure on the OEMs can also come from outside the automotive industry. Large digital companies as Google, Apple, and others also want to enter this ecosystem of connected and automated mobility, either with own connected and automated cars or with their huge competence in regard to data analytics and artificial intelligence and the provision of many digital services.[78] Especially strategic alliances between traditional OEMs and large digital companies have the potential to intensify competition between OEMs and might break up the old

[75] See e.g., BEUC (n 23) 8; Specht/Kerber (n 2) 190.

[76] See FIA 2016b (n 22) 1.

[77] See for the problem whether the provision of data to the OEMs would lead to lower prices for connected cars Kerber/Frank (n 23) 28.

[78] Martens/Mueller-Langer (n 7) 20-23 make the important argument that if platforms (as, e.g., media and entertainment platforms) with large network effects offer car versions of their (for the car users very attractive) services (Apple iOSCarPlay or Android Auto), then OEMs might be under competitive pressure to install those media systems in their cars as part of the entire bundle they are offering to their customers. This would allow the large digital companies to enter the markets of aftermarket and complementary services and use their huge competitive advantages in regard to data and data analytics on these markets.

business model of the OEMs. Therefore a careful monitoring of the business strategies of the OEMs is important.

However, there might also be competition problems between OEMs through collusive, cartel-like behavior of the OEMs. It can even be asked whether the extended vehicle concept itself (as it has been developed by OEMs and defended by their associations in Europe) can be seen as an anticompetitive horizontal agreement about decisions on technology and governance of in-vehicle data in connected and automated cars. All OEMs that apply the extended vehicle concept (1) use the same technological solution of a proprietary server to which all in-vehicle data are transmitted (leading to their exclusive control of the in-vehicle data), and (2) design the connected car as a closed system (with exclusive control of the access to the car). Therefore, the monopolistic gatekeeper position of the OEMs is an integral part of the extended vehicle concept. It would also be interesting to investigate to what extent the OEMs with the extended vehicle concept have also agreed upon (3) the categories of data that they are making accessible under certain conditions to other stakeholders, and (4) on contractual provisions in regard to (personal) data and privacy options in their contracts with car owners. As far as the OEMs have de facto agreed on these and perhaps also other aspects of their technological or data governance solutions, competition in regard to these solutions would have been eliminated.[79] There would be, in particular, no competition in regard to other technological solutions as, e.g., the interoperable on-board application platform. Since, however, the business strategies of OEMs also differ to some degree,[80] it would be necessary to investigate the extent to which the extended vehicle concept leads to collusion between the OEMs in regard to the design of technological and data governance solutions in the ecosystem of connected and automated driving.[81]

VIII. Conclusions

In this section we have analyzed what kind of market failure problems might emerge in regard to the data governance in the ecosystem of connected and automated mobility and offered a preliminary assessment of these market failures, which however requires much more (and primarily also empirical) research:

(1) **Competition problems:** By using the extended vehicle concept with its exclusive control of the access to the data and the car the OEMs can foreclose independent service providers and control and monopolize aftermarket and complementary services. This can lead to too high prices, not enough consumer choice, and less innovation. These competition problems cannot be sufficiently mitigated through systems competition between OEMs.

---

79 In that respect also a closer analysis of the effects of the standard-setting process in regard to the "Extended Vehicle Standard" (ISO 20078) might be relevant (see for more information https://www.iso.org/standard/66978.html). In regard to technological collusion between OEMs in the automotive industry see also the current investigation of the EU Commission into possible collusion on clean emission technology (see press release IP/18/5822, 18 September 2018).

80 See TRL (n 2) 67-72.

81 Then the question of a cartel exemption can be discussed (see below section D.III).

(2) **Interoperability and standardization problems:** Within this complex integrated ecosystem of connected and automated mobility it cannot be expected that the individual profit-maximizing decisions of OEMs on technology lead to optimal solutions in regard to interoperability and standardization for the entire system.
(3) **Information and privacy problems of car users:** Especially important is research whether and to what extent there might also be a market failure problem in regard to the decisions of the car users for giving their consent to the processing and use of their personal data. This would also require an analysis of the provisions on data in (standard form) contracts and the options the OEMs offer the car users for granular decisions about protecting their privacy.
(4) **Safety and cybersecurity:** These concerns are very important but do not lead to a justification of the extended vehicle concept, because they also can be solved with the on-board application platform. In any case, safety and cybersecurity concerns cannot justify the exclusive control and therefore de facto ownership of the in-vehicle data by the OEMs.

What are the conclusions for the current discussion between OEMs and the independent service providers about access to in-vehicle data? Although there is still considerable need for further research, the preliminary results of our analyses of potential market failure problems suggest that the concerns of the independent service providers about the impact of the extended vehicle concept on competition and innovation on the markets for services in the ecosystem of connected driving are justified. Since also the extended vehicle concept with its exclusive control of the in-vehicle data cannot be defended by safety and cybersecurity concerns, the trade-off between competition and cybersecurity does not exist in regard to in-vehicle data. Safety and security concerns seem to be solvable also with the on-board application platform that would allow to give the control of the access to the connected car and the in-vehicle data to the car users. In regard to the discussed policy conclusions both the “shared server” in case of the current technological solution of the “external server” and the on-board application platform would allow for a “levelling-the-playing field” in regard to the access to in-vehicle data and can therefore contribute to the protection of competition on the markets for services within the ecosystem of connected and automated mobility.

D. Governance of in-vehicle data: Discussion of policy approaches

I. Complexity of the data governance problem

Although the conclusions in the last section seem to support the position of the independent service providers, the data governance problem in this ecosystem of connected driving is much more complex. Whereas both the “shared server” and the “on-board application platform” offer the chance to eliminate the exclusive control of the OEMs in regard to the in-vehicle data, they are themselves neither a clear nor a comprehensive solution for the governance of the in-vehicle data. There are many open questions: Who should operate a shared server and how should it grant access to what kinds of data and under what conditions? Should all data that are produced in the car be transmitted to this server or have OEMs and, e.g., component suppliers direct access to certain kinds of technical data (safety

and cybersecurity reasons, business secrets)? How to deal with data that are costly to produce compared to those with negligible costs? Should there be one shared server for each OEM or might it be better to pool the in-vehicle in one industry-wide shared server for a better exploitation of the advantages of data aggregation? Also the proposal of a transition to an interoperable on-board application platform does not clarify how the governance of the in-vehicle data will look like under this technological solution. These policy proposals do also not take into account the potential market failure problems in regard to information and privacy problems of car users concerning the provision of personal data and the protection of their privacy or the question whether and how car users should participate in the value of the data. In addition to that, there might be many more proposals for solving the problems, e.g. also voluntary measures as principles for the access to data.

These questions should only emphasize that the data governance problem in the ecosystem of connected and automated mobility is a very complex problem that needs much more research from a technological, economic and legal perspective.[82] This paper does not claim to have a clear policy proposal about the governance of these data, although it clearly suggests that the currently existing extended vehicle concept is not a suitable concept and that it is therefore necessary to think about (perhaps far-reaching) policy solutions. In the following, I will present an overview about some current policy discussions in regard to the governance of data and ask to what extent they might be helpful for solving problems of access to in-vehicle data in the ecosystem of connected and automated mobility. Section II will ask whether the current discussions about the introduction of data rights or the use of the data portability right (Art. 20 GDPR) can offer solutions. This will be followed by an analysis whether and how competition law might help independent service providers to get access to in-vehicle data (section III). The final section IV will suggest that a comprehensive sector-specific regulatory solution of the governance of in-vehicle data might be the most promising way for solving the problems.

II. Data rights and data portability

One group of options for solving data access problems to in-vehicle data are based upon the possibility of defining and assigning generally legal rights on data, which then can also be used for the data of the connected cars. Due to the many open questions about the governance of data, broad policy discussions have emerged about data rights and the necessity of further legislative initiatives in that respect. In this section we will focus primarily on two discussions about possible solutions: (1) The data portability right of European data protection law, and (2) the general introduction of new exclusive and/or access rights on data.

According to Art. 20 of the new General Data Protection Regulation (GDPR) data subjects have a right to data portability that allows the data subject to receive their personal data from

82 This problem is also not solved in the U.S.; see for the U.S. discussion about data governance in regard to connected cars, e.g., Fagnant/Kockelman, Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations. Transport Research Part A 77, 2015, 167, 178 -180; Anderson et al (n 5) 146; Determann/Perens (n 13) 978-984; Akalu (n 73) 37.

a data controller in a structured, commonly used and machine-readable format, or have them transmitted directly from one data controller to another. This right should give the data subjects more control of their personal data but also should foster competition between service providers by lowering switching costs.[83] Can this data portability right be an instrument for solving the data access problems of independent service providers in those cases, in which the OEMs have exclusive control of the in-vehicle data?[84] However, there are at least three main problems in regard to this solution: A first general problem of data portability is that the technical feasibility in regard to the meaning of commonly used formats and interoperability is so far very unclear. This problem might be solvable in regard to data in connected cars, because standardization in regard to in-vehicle data might be necessary anyhow. A second more difficult problem is that it is legally very unclear what kinds of in-vehicle data this right of data portability would encompass, because most of them are not uploaded data as in social media but are produced in the car (often under participation of the OEMs or component suppliers), or are anonymized data or also business secrets. It is also very doubtful whether the data portability right would allow for a fast or even real-time data portability, which would be important for many of the new services in regard to connected driving.[85] A third important problem is that this solution might lead to too high transaction costs, both for the car owners for exercising their right as well as for the independent service providers for convincing a sufficiently large number of car owners to use this right for making market entry profitable.[86] Therefore the new data portability right of the GDPR is theoretically a very interesting option for solving competition problems due to a lack of access to in-vehicle data, but there are still too many open technical and legal problems for making this solution workable in the next years. It might presumably also require sophisticated regulatory solutions for lowering the transaction costs sufficiently.[87]

Does the recent general discussion about the introduction of a new property-like right on machine-generated data or new mandatory access rights to data offer a solution for the access problems to in-vehicle data? The intensive discussion about a new IP-like exclusive right on machine-generated data with the ensuing proposal of the EU Commission of a “data producer right” that should be assigned to the owner or user of a smart device has led to a broad

---

83 See Article 29 Data Protection Working Party, Guidelines on the right to data portability (13 December 2016; rev. on 5 April 2017), 1. For the data portability right as a possible solution for competition problems caused by exclusive control of data see Schweitzer/Haucap//Kerber/Welker (n 59) 183, and, more generally, Graef/Husovec/Purtova, Data Portability and Data Control: Lessons for an Emerging Concept in EU Law (TILEC Discussion Paper, 2017-041.

84 Martens/Mueller-Langer (n 7) 25, see the data portability right as one of the main options for solving the data access problem to in-vehicle data; for a more general discussion in regard to the Internet of Things see Urquhart/Sailaja/McAuley, Realising the right to data portability for the domestic Internet of Things, Personal and Ubiquitous Computing, 2017.

85 See for a discussion of legal problems of data portability of in-vehicle data Störing, What EU legislation says about car data, Legal Memorandum on connected vehicles and data, 2017.

86 See Schweitzer/Haucap/Kerber/Welker (n 59) 183.

87 In the telecommunication sector the portability of phone numbers is facilitated through specific rules in telecommunication regulation.

consensus that the introduction of such an exclusive right cannot be recommended.[88] After a consultation also the EU Commission has decided not to pursue this proposal of such a general “data producer right”. In the same way also the proposal of a general mandatory access right to privately held data (under FRAND conditions) was much criticized and abandoned by the Commission, although the basic idea of facilitating more access and reuse of data has been broadly welcomed both in the academic discussion and by stakeholders in the consultation. One important result of this discussion is reluctance in regard to mandatory solutions compared to much more favored voluntary solutions for facilitating contractual solutions about more access to data.[89] The other important conclusion is that the economic benefits and costs of both exclusive rights and/or access rights are so different between different sectors and business models that general solutions in regard to defining and assigning new data rights seem to be extremely difficult or even impossible. Therefore a broad opinion has emerged that prefer more sector-specific tailor-made data governance solutions (see section IV).[90] Therefore, the general discussion about the introduction of data rights do not seem to offer a clear perspective for solving the problems of access to in-vehicle data.[91]

III. Competition law

Since the controversial discussion about the access to in-vehicle data in the extended vehicle concept focuses on competition problems on the markets for aftermarket and complementary services, competition law seems to be an obvious candidate for finding a suitable policy solution. It is surprising that so far competition law solutions for granting access to data

[88] See for this discussion Zech (n 36), Drexl, Designing competitive markets for industrial data: Between propertisation and access, Max Planck Institute for Innovation and Competition Research Paper No. 16-13, 2016, Wiebe, Protection of industrial data - a new property right for the digital economy? GRURInt, 2016, 877-884 from a legal perspective, and Kerber, A new (intellectual) property right for non-personal data? An economic analysis. GRURInt, 2016, 989-998 from an economic perspective; for in-vehicle data see Hornung/Goeble (n 35), and more general for mobility data BMVI, Eigentumsordnung für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive, 02.08.2017.

[89] See for these proposals in the Communication “Building a European data economy”, the ensuing consultation and discussion EU Commission 2017 (n 4), EU Commission, Synopsis report. Consultation on the "Building a European data economy" Initiative, 2017, EU Commission 2018 (n 4), Drexl, Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz, NZKart, 2017, 339 (Part 1) and 415 (Part 2), Kerber (n 4), Schweitzer/Peitz. Ein neuer Ordnungsrahmen für Datenmärkte? Neue Juristische Wochenschrift, 2018, 275-280, and Specht/Kerber (n 2) 69-99,151-169.

[90] See Drexl (n 90) 415, 419, and Kerber (n 4), 109, 133.

[91] It will be interesting to see whether the emerging discussion about mandatory access to large anonymized data sets for training algorithms in the context of artificial intelligence (AI) and machine-learning will lead to new legislative efforts for introducing general access rights for these purposes. See for a proposal of mandatory data-sharing Mayer-Schönberger/Ramge, Reinventing Capitalism in the Age of Big Data, 2018, 166-171.

have not played a prominent role in the policy discussion about in-vehicle data.[92] This section can only present a brief overview about the options that competition law might offer.

In section C.IV we have seen that in the extended vehicle concept the exclusive (monopolistic) control of the OEMs about the access to the in-vehicle data (and/or the car) can foreclose competition on the markets for those aftermarket and complementary services for which this access is necessary. If – as our preliminary analysis suggests – systems competition between entire bundles of connected cars and services does not work sufficiently, then no undistorted competition on these markets for aftermarket and complementary services can be expected, and an obligation of the OEMs for granting access to the in-vehicle data (e.g., under FRAND-conditions) might be an appropriate remedy from a competition economics perspective. The existing sector-specific obligation of OEMs for granting non-discriminatory access to repair and maintenance information in the type approval regulation is already such a solution (see section B). It can be asked whether this solution of mandatory access rights to in-vehicle data for independent service providers can also be achieved by applying the general rules of competition law in order to protect competition on markets for all aftermarket and complementary services. Although so far no competition law cases exist in regard to obligations to grant access to data, the increasing interest in the role of data in the digital economy has led to new discussions about solutions for data access problems in competition law. In a recent study about “Modernizing the law on abuse of market power” the author (jointly with Heike Schweitzer, Justus Haucap, and Robert Welker) has analyzed to what extent current European and German competition law might lead to obligations for granting access to data in digital contexts, esp. also in IoT-applications (as the connected car).[93] The following paragraphs try to apply the results of this study to the problem of access to in-vehicle data.

Can the refusal of an OEM to grant access to exclusively held in-vehicle data be an abusive behavior according to Art. 102 TFEU by applying the essential facility doctrine? Whereas there is a well-established case group of applying Art. 102 TFEU to refusals to grant access to physical essential facilities (as infrastructure) and to license IP rights, the essential facility doctrine has so far not been applied to the refusal to grant access to “essential” data sets.[94] Usually the requirements for applying the essential facility doctrine are very high. However due to the economic characteristics of data, esp. non-rivalry in use and the fact that often the incentives for data production are much less important than in the case of physical infrastructure and innovations, the essential facility doctrine can be applied much more flexibly in re-

[92] However the results of the consultation about the Communication “Building a European data economy” have shown that many firms who have problems in regard to access to data are skeptical about the extent that competition law can help to solve data access problems, esp. for small firms in situations with “unequal bargaining power”. The results of the consultation suggest that this kind of problem emerge especially in the automotive sector. See EU Commission, Annex to the synopsis report. Detailed analysis on the public online consultation result on "Building a European data economy", 2017, 13.

[93] See Schweitzer/Haucap/Kerber/Welker (n 59) 158-191.

[94] See, e.g., Autorité de la Concurrence / Bundeskartellamt, Competition Law and Data, 2017, 18; Schweitzer/Peitz (n 90) 81; Drexl (n 89) 46.

gard to data.[95] Besides the requirement of market dominance of the data holder the data have to be indispensable for offering the service, and the refusal has to lead to a threatening of the elimination of competition. If we assume that the relevant market are the brand-specific markets for aftermarket and complementary services (i.e. no system markets exist), the OEMs can be seen as dominant firms, and their exclusive control of the in-vehicle data can eliminate competition on these markets.[96] The additional criterion of a "new product" might not be a problem because of the new innovative services that are expected to being offered by the independent service providers. The last criterion is whether the OEMs have a justification for the refusal of access. We have seen that safety and cybersecurity concerns do not provide such a justification. More difficult is the question about the incentives for producing the data and covering the operating costs of the entire communication infrastructure. Since also the car users are participating in generating the data and have paid for the car and for additional services (of the OEMs), it is not clear whether and to what extent such an obligation would lower the incentives for data production. In addition to that, OEMs can also be compensated for their (operating) costs. Much more important is that often also the consent of the car users is necessary for complying with EU data protection law. Overall, it can be concluded that it might be possible that the refusal of OEMs to grant access to in-vehicle data to other stakeholders in the ecosystem of connected driving can be an abusive behavior according to Art. 102 TFEU.[97]

Since, however, the requirements for the "essential facility" doctrine in regard to data are still high (despite the possibility of more flexibility), the question arises about other options in competition law. In the above-mentioned study we particularly analyzed whether also § 20 (1) GWB of the German competition law can be used for claiming access to data. § 20 (1) GWB extends the prohibition of abusive behavior of dominant firms in German competition law also to firms with so-called "relative market power", i.e. firms from which other small or medium-sized firms are dependent, because they have not sufficient and reasonable possibilities of switching to other firms. This provision of German competition law has been used for a long time for solving specific market power problems below the threshold of market dominance. One of the case groups are firms (as authorized dealers) that have specifically invested into the relationship with another firm, and therefore have gotten dependent from this firm ("unternehmensbedingte Abhängigkeit").[98] Can the refusal of OEMs to grant access to in-vehicle data to independent providers of aftermarket and complementary services also

---

95 See Schweitzer/Haucap/Kerber/Welker (n 59) 171.

96 For an overview about court decisions in regard to market dominance of OEMs in aftermarkets and the reluctance of courts to accept system markets in the automotive industry see Schweitzer/Haucap/Kerber/Welker (n 59) 167-180.

97 It is also possible to ask whether the exclusive control of the OEMs to the connected car, which impedes interoperability ("closed" car), might be under certain conditions an abusive behavior of a dominant firm. For such an "interoperability obstruction", which also increases lock-in problems, see Kerber/Schweitzer (n 66) 55.

98 See for this provision in German competition law and its application Nothdurft, Relative Marktmacht: Gutachten zu Grundlagen, Bedeutung, Wirkung und Praxis der deutschen Missbrauchsverbote gegenüber relativ marktmächtigen Unternehmen, 2015, available at http://www.faire-importpreise.ch/pdf/gutachten.pdf).

be an infringement of § 20 (1) GWB? Whereas also here no cases in regard to access to data exist so far, it can be argued that under certain conditions firms on aftermarkets and in IoT-contexts with several stakeholders that need access to the same data for offering valuable services might claim access to the data that one stakeholder holds exclusively. In that respect a new case group relating to access to data in regard to value creation networks (as in connected cars) might be possible. The advantage of using this provision is that the data holder need not be deemed as dominant according to Art. 102 TFEU or § 18 GWB (in German competition law). However, it will take much more research for clarifying the specific conditions, under which such an obligation for granting access according to § 20 (1) GWB can be justified.[99] Therefore, in Germany § 20 (1) GWB might offer another way for solving data access problems in the ecosystem of connected driving.

Therefore competition law might offer interesting options for solving problems of access to in-vehicle data in those cases, in which the OEMs have exclusive control of these data, e.g. through the application of the extended vehicle concept. However, these case groups have still to be developed and it will need time to clarify the criteria that have to be taken into account for the necessary balancing of the potential positive and negative effects of mandatory data access rights that are based upon either European or German competition law provisions against abusive behavior of firms with market power. Another serious problem is that it might be difficult and expensive, esp. for small- and medium-sized companies, to enforce access to in-vehicle data in private litigation. Although more public enforcement through competition authorities would be helpful, the instrument of ex-post control of abusive behavior of powerful firms is always a difficult and lengthy process for solving problems. Therefore it can be asked whether competition law can also provide instruments outside of the control of abusive behavior. One approach might be the use of the instrument of a block exemption regulation according to Art. 101 (3) TFEU, in which problems of data access, e.g. in regard to complex multi-stakeholder situations of IoT applications, might be addressed, either more generally or in a more sector-specific way.[100] It can also be asked the question whether competition law could also challenge directly the exclusive control of data by the OEMs (in the extended vehicle concept). If after an investigation the application of the extended vehicle concept by the OEMs can be seen as a horizontal agreement between the OEMs about technological and data governance solutions (as discussed in section C.VII), the question of the fulfillment of the criteria for exempting this horizontal agreement according to Art. 101 (3) TFEU will arise. As part of such an assessment the competition authorities could ask about the efficiency effects of such an agreement and whether the exclusive control of in-vehicle data through OEMs with its negative effects on competition is necessary for achieving these benefits. The results of our analysis might raise serious doubts whether the exclusive control of in-vehicle data can be justified in such an assessment.

---

99 See for a deeper discussion Schweitzer/Haucap/Kerber/Welker (n 59) 172-191; due to a possible gap and for clarification we have made a proposal for amending § 20 (1) GWB of the German competition law for facilitating data access solutions, esp. in Internet of Things constellations (as also the connected car). See ibid. 191.

100 Block exemption regulations also have the advantage of allowing the publication of more specific guidelines that can deal with different kinds of problems.

IV. Sector-specific regulatory solution

The last two sections have shown that the already existing data portability right as well as competition law might help to find solutions for data access problems that arise through the exclusive control of in-vehicle data by the OEMs. However, all of these policy options are still more theoretical ideas which so far have not been tried out and which will need much more research, effort and time for implementation. Even if the instruments data portability and granting the right to access data as remedy against abusive behavior in competition law can be applied in the ecosystem of connected driving, it is not clear whether these options can be used broadly and fast enough for safeguarding competition on markets for aftermarket and complementary services. In addition to that, these policy instruments cannot help much in regard to market failures in regard to technological solutions and information and privacy problems of consumers (sections C.VI and C.VII). Although it is an option to try to solve the different market failure problems through applications of remedies from different legal fields as competition law, data protection law, consumer law etc., the complexity of the technological and data governance problems in this ecosystem is so large that it is very unclear whether this leads to a satisfactory solution. Therefore, it might be more promising to try to develop a tailor-made sector-specific regulatory data governance solution.

It can be suggested that the following problems should be addressed in such a sector-specific regulatory framework:

(1) Technological framework: Due to the huge impact of technological decisions on the question who has de facto control of data and can decide on (the conditions of) their use, a regulatory framework should encompass policies for promoting technologies that support a better use of data, less competition problems, and also more privacy-friendly solutions in regard to the protection of personal data. In that respect, the development of solutions for interoperable on-board application platforms might be particularly important. These technological solutions should be seen as part of the long-term development of the over-arching technological architecture of connected, automated and later autonomous mobility. This will require far-reaching solutions in regard to interoperability and standardization (esp. also in regard to safety and cybersecurity problems). Due to the ongoing and technological evolution a sophisticated strategy is necessary for enabling the benefits of interoperability and standardization without impeding innovation.

(2) Data access: Depending on the developing technological solutions specific regulatory solutions about the governance of the in-vehicle data might be appropriate. As long as external server solutions for the in-vehicle data are applied, regulatory solutions about the access to these data might be necessary for solving competition problems on market for aftermarkets and complementary services. One option can be a broadening of the current regulated access solution for repair and maintenance information to all service providers that need in-vehicle data in the ecosystem of connected driving. Another option is the already much discussed “shared server” solution, which would put all the in-vehicle data under the control of a neutral entity with the idea of granting non-discriminatory access. The question about the

institutional design of such a “shared server” also opens up the discussion about larger data pool solutions that can also be linked to new ideas of data trustee solutions. Another solution might be sector-specific regulations for making the data portability right an effective instrument for solving data access problems.[101] Also sector-specific rules about access to certain kinds of in-vehicle data for public authorities (traffic regulation, law enforcement etc.) might be part of these data access rules.

(3) Data economy and privacy: Different technological solutions as the on-board application platform would also enable different kinds of markets for data, since access to data could be obtained directly from the car users leading to new platforms for trading data. Therefore, the regulatory framework for in-vehicle data could support the emergence of these trading platforms. But even if the privileged position of the OEMs is eliminated, complex problems in regard to dealing with different types of data have to be solved. This refers first and foremost to personal data and the protection of the privacy of car users, where the mentioned market failure problem might lead to the need of regulatory solutions for contracts about the provision of data and a minimum of privacy options for car users. But also sector-specific rules about data that can be deemed as business secrets might be helpful. A sector-specific approach would also allow regulatory solutions for exploiting the advantages of data aggregation, i.e. that data analytics and AI can get access to a large pool of in-vehicle data to increase the quality of the results (e.g., in regard to traffic safety) or for a better training of algorithms.

The advantage of a sector-specific regulatory framework is that all of these questions are interrelated with each other, and that therefore the complex trade-offs between benefits and costs of different solutions for the governance of these data might be solved better in an integrated approach.

E. Perspectives

The discussion about access to in-vehicle data and resources is a very important policy discussion, because it raises many questions that are relevant also in other areas of the digital economy, and especially in the future world of “Internet of Things”, in which the production of sensor data will be nearly ubiquitous in the offline world. Smart manufacturing and smart retailing, smart home, and smart cities are some of the most important examples in that respect. In all of these areas it is so far very unclear how an appropriate data governance framework should look like. But in all of these contexts very similar questions will turn up as they have been discussed here in regard to the data in the ecosystem of connected and automated cars.

---

[101] See, e.g., also the sector-specific solution in the second Payment Services Directive (PSD2), through which third-party payment service providers with the consent of the account owners might get access to bank account data for offering their services to the consumers.