Abstract: The Internet of Things raises a number of so far unsolved legal and regulatory questions. Particularly important are the issues of privacy, data ownership, and data access. One particularly interesting example are connected cars with their huge amount of produced data. Also based upon the recent discussion about data ownership and data access in the context of the EU Communication "Building a European data economy" this paper has two objectives: (1) It intends to provide a general economic theoretical framework for the analysis of data governance regimes for data in Internet of Things contexts, in which two levels of data governance are distinguished (private data governance based upon contracts and the legal and regulatory framework for markets). This framework focusses on potential market failures that can emerge in regard to data and privacy. (2) It applies this analytical framework to the complex problem of data governance in connected cars (with its different stakeholders car manufacturers, car owners, car component suppliers, repair service providers, insurance companies, and other service providers), and identifies several potential market failure problems in regard to this specific data governance problem (esp. competition problems, information/behavioral problems and privacy problems). These results are in important precondition for future research that focus more on the specific policy implications for data governance in connected cars. Although the paper is primarily an economic paper, it tries to take into account important aspects of the legal discussion.

* Wolfgang Kerber, Professor of Economics, Philipps-University Marburg, kerber@wiwi.uni-marburg.de; Dr. Jonas Severin Frank, Senior Researcher, Philipp-University Marburg, severin.frank@wiwi.uni-marburg.de. We would like to thank Daniel Möller, Axel Gautier, Heike Schweitzer, Bertin Martens and the participants of the EALE conference in London (September 15, 2017) for very helpful comments on an earlier version of this paper.
1. Introduction

The Internet of Things (IoT) will be an important additional step in the ongoing digital revolution of the economy and society. The decisive difference to the current phase of digitization is that data are not only collected and produced, if individual persons actively go online, e.g., by using a search engine, social media, or an app on a smartphone, but that the offline world itself, in private homes, in cars, in firms, in shops, and in other public places will be equipped with many different devices that will produce an increasing number of data (esp. through sensors) for a wide range of different purposes. Often these data-producing devices will be "smart", i.e. that they will use these data for providing new valuable services for individuals, firms, and public authorities, e.g., also through applying data analytics, algorithms, and artificial intelligence. Since these devices will be integrated into the digital world, the offline world will no more be separated from the digital world but will be an inseparable part of it. Already well-discussed examples are smart home, smart cars, smart manufacturing, smart cities, smart health, and smart agriculture. There is a lot of discussion about the potential advantages and dangers of these technological developments. Despite serious concerns about privacy, cybersecurity, competition, and even democracy through the digital revolution, there is a broad consensus that the "Internet of Things" opens up the possibility to offer new innovative solutions for many private and public problems. However, it is also broadly accepted that there are many open questions about the appropriate legal and regulatory framework for IoT-applications, both in regard to enabling IoT and in solving potential problems through IoT. These issues encompass the problems of interoperability / standardization, security and safety, liability, privacy, and of data ownership and data trading. In this article we will focus on the question of the appropriate legal rules and rights for personal and non-personal data (data governance), and therefore on the privacy and data ownership issues.

One of the most prominent and discussed examples of the "Internet of Things" are connected (or smart and later autonomous) cars.¹ In the connected car a huge number of data, esp. through sensors, is produced, which allows many additional services for the car driver, as, e.g., Advanced Driver Assistance Systems. These are data about the technical functions of the car itself, the driving behavior, location data, data about the surroundings of the car (as other cars and traffic), data about weather and road conditions etc. The connected car is via mobile communication constantly connected to the internet and can exchange data in real time. These characteristics allow, on the one hand, for an increasing degree of automated driving (up to the possibility of self-driving cars) with the potential benefits of unburdening the drivers and of increasing safety through less accidents by human errors, and, on the other hand, for offering the car drivers (and car passengers) a wide range of additional services during driving, e.g. in regard to navigation, finding parking space, infotainment, online shopping etc., and also might allow public authorities to improve traffic regulation and reduce congestion and environmental problems. Both the EU and some member states, as, e.g. Germany, have started to design and implement policies for enabling connected driving as part of comprehensive mobility concepts, often in close collaboration with the most important stakeholders, as, particularly the car industry.² The most important regulatory problems refer to interoperability and standardization in regard to technical

---


and IT issues, how to solve potential dangers for safety and security, which is closely related to the issue of liability, how to protect the privacy of car owners (personal data of car drivers and passengers that are subject to EU data protection law), and how to deal with the question of the ownership in regard of the data produced in the car (including its potential use and commercialisation via data trading). Within the complex data ecosphere of connected driving a number of different stakeholders are interested in using these data (car owners/drivers, car manufacturers, car component suppliers and independent repair and maintenance providers, insurance companies, and many other independent providers who want to offer products and services to the car drivers and passengers).

The question is how the governance of the data in the connected cars should be organized for protecting privacy, ensuring an optimal use of data, esp. also in regard to competition and the innovation of services in the car but also for better traffic regulation and safety. Especially controversially discussed is the question whether and to what extent the car manufacturers should have exclusive control about the data and the resources in the connected car ("extended vehicle" concept) or whether other technical solutions (as the in-vehicle interface or the on-board-application platform) should be implemented which would allow more direct access to in-vehicle data for other stakeholders and might give the car owners more choices for deciding who should be given access to the data and the connected car. These questions are directly linked to the problem of data ownership and who should get the benefits of (using/selling) these data.\(^3\) This question about the legal and regulatory rules in regard to the data in connected cars is directly linked to the current policy discussion about data ownership, data trading, and data access and transfer, esp. in regard to machine-generated data through sensors.\(^4\) One part of the discussion is about the possibilities to trade personal data that are protected by EU data protection law. Although it is clear that there is no property on personal data, giving consent to the use of personal data for money or free services is one way of trading personal data.\(^5\) The other part of the discussion refers to non-personal machine-generated data, because they are usually not legally protected by property rights. Therefore in the legal discussion the question emerged whether a new IP-like exclusive right for those data should be introduced, which are neither personal data nor protected by traditional IP laws. This is particularly relevant for many (machine-generated) sensor data through IoT devices, e.g. also in the context of smart manufacturing.\(^6\) In the Communication "Building a European data economy" the Commission picked up this discussion and suggested a new "data producer right", which should be allocated to the owner (or the long-term user) of a data-producing device (esp. in the IoT context), for allowing to authorize the use of these data and therefore to facilitate the access and reuse of non-personal (and anonymised personal) data.\(^7\) The main concern of the Commission is that too many of the produced data are kept in-house and used only by the firms that hold these data but are not made available for further reuse, which might impede a thriving data economy. However, the Commission did also suggest solving the data access problem through far-reaching access rights to privately held data. Also in the legal and economic discussion there are many scholars who think that access rights to data might be more important than exclusive property rights. Whereas so far the dis-

\(^3\) See, in particular, C-ITS Platform (2016) and EC (2017c); for the general question of "ownership" of "mobility data" see BMVI (2017).


\(^5\) See, e.g., Specht (2017) and Schweitzer (2017) for a deeper analysis from the legal perspective,

\(^6\) See, e.g. Zech (2015a), Wiebe (2016), and Drexl (2016).

\(^7\) See EC (2017a, 2017b).
discussion mostly focused on the general question of "exclusive property rights" vs. "access rights" to data, the most recent contributions acknowledge the complexity of the appropriate legal solutions for data, and recommend a more sector-specific approach, which allows for a more specifically tailored solution of the appropriate sets of rights for data, esp. in complex multi-stakeholder situations. Therefore the question of data ownership, esp. also who has de facto control of data, and the issue of access (rights) to data, and who gets the benefits of the produced data in the connected and autonomous driving discussion is directly related to this general discussion about data ownership, exclusive rights and access rights on data in the digital economy. Therefore the topic of data governance in connected cars is an example of the much more general question of data governance in IoT contexts.

This paper would like to contribute to this discussion in two ways. After a brief summary of the general current discussion about data ownership and the controversial issue of "property" vs. "access" to data, section 2 intends to provide from an economic perspective a general theoretical framework for analyzing complex data governance regimes (consisting of all legal rules and rights that are relevant to data) in regard to its effects on competition, innovation, and welfare but also on privacy and distributional effects. An important part of this theoretical framework is the analysis of potential market failure problems that can arise in connection with data in IoT contexts. Such a more general framework is necessary, because the policy problems are often much more complex than the "property" vs. "access" right discussion suggests. This framework will be used in the main section 3 of this paper, in which we want to provide a first preliminary analysis of the potential market failure and other regulatory problems in regard to data in connected cars. After giving an overview about the basic structure of the connected car problems with its multitude of stakeholders and different types of data, we will analyze step-by-step the relationships and markets between the different stakeholders, esp. between car owners and car manufacturers, car manufacturers and components suppliers, independent repair services and other service providers, including insurance companies. Our results will show that there are a number of different potential market failures and problems, esp. in regard to privacy concerns, that are relevant for the question how a comprehensive data governance regime for the data of connected cars should look like. This will also be related to the current policy discussions about the extended vehicle concept of the car manufacturers and alternative proposals for the technical architecture in regard to communication and data in connected cars. Since our analysis is still exploratory and more about identifying relevant problems and tradeoffs in regard to data in connected cars, we are - at this state of our research - very cautious in regard to derive policy conclusions about the appropriate data governance regime for connected cars.

8 See, inter alia, Drexl (2017), Kerber (2017), and Schweitzer/Peitz (2017).
2. Theoretical Background: Data Governance Regimes

2.1 Data Governance instead of Property vs. Access

Data is codified information. Especially machine-generated data and sensor data that are being produced in the digital economy, esp. also through the IoT, is tremendously increasing. Since data are valuable inputs for the digital economy, either for increasing efficiency or for innovation, and are also increasingly traded, it is not surprising that a discussion among lawyers emerged about the question how data are protected legally. Whereas a part of data is protected by traditional IPRs, especially copyright law (e.g., digital music files), for most other data that are produced in the digital economy no exclusive property rights exist. As far as data qualify as personal data according to EU data protection law, individual persons are granted a strong set of rights about the collection, processing, and using of "their" personal data, which due to the "consent principle" resembles to some extent exclusive rights, but there is a consensus among lawyers that EU protection law does not lead to exclusive property rights about personal data. However, among lawyers there is a broad discussion about the possibilities and problems of "trading" personal data, e.g., in exchange for "free" services (data as counterperformance). For many machine-generated non-personal data it is clear that no exclusive property rights exist, although some protection of non-personal data is possible, partly through civil law, e.g., against destruction or compromising, and partly through trade secret law, because data can be trade secrets (if the usual conditions for trade secret protection are fulfilled), but only against certain forms of misappropriation, and this protection would not confer an absolute exclusive right on data (ergo omnes). Therefore proposals emerged, esp. among German lawyers, about the introduction of a sui-generis IP-like exclusive property right on data, which also has triggered the discussion about property rights on data at the EU level, and led to the already mentioned proposal of an exclusive "data producer right" in the Communication "Building a European data economy" of the EU Commission in January 2017.

These proposals have triggered a broad and controversial discussion about the necessity of (new) exclusive property rights on data. So far there has not been much research from an economic perspective about the need and recommendability of introducing exclusive property rights on non-personal data. In two earlier papers Kerber has analyzed from an economic perspective (a) the need and the potential dangers of introducing an IPR on non-personal data (Kerber 2016), and (b) the economic reasonings of the EU Commission in its Communication and the suggested policy proposals (including the "data producer right"; Kerber 2017). Using a "law and economics of intellectual property" perspective these papers come to the conclusion that a new IPR on data (as well as the suggested

---

9 See, e.g., Kilian (2015), Specht (2017), Schweitzer (2017); for the discussion about "propertization" of personal data see also Samuelson (2000) and Schwartz (2004); for personal data in connected cars see, particularly Hornung (2015), Hornung/Goeble (2015), and BMVI (2017).
10 For the legal protection of non-personal data see, e.g., Zech (2015a), Drexl (2016), Wiebe (2016), and EC (2017b).
12 Other papers that discuss the topic of property / governance on data from an economic perspective are Duch-Brown-Martens/Müller-Langer (2017a), OECD (2015, 2016), and Schweitzer/Peitz (2017).
"data producer right") cannot be justified and can even be dangerous for competition and innovation in the digital economy. In the following, we will summarize the most important reasoning that lead to this conclusion: Most important from an economic perspective is that data is a non-rivalrous good, i.e. that the marginal costs of additional use of the same data through additional parties is zero. This is also the main economic reasoning behind the objective of the Commission about promoting data access and data transfer. The second important characteristic of these data is that the data holders can exclude others from the use of these data also without exclusive property rights, e.g., through encryption and/or other technical means. So far there has also been no general complaints about a massive problem of copying data. Therefore we also do not have the typical incentive problems that justify the traditional IPRs on intangible goods (as innovation and creative works), where the reasoning always was that exclusive IPRs are necessary for ensuring innovation incentives. In fact, nobody in the discussion about property rights on data has claimed so far, that the digital economy suffers from a general incentive problem in regard to production of data. Additionally, the observed exponential increase of the produced data in the digital economy does not suggest a general under-production of data. Therefore the incentive problem as the main economic argument for justifying an exclusive property right on a non-rivalrous good does not hold in regard to these machine-generated non-personal data.13

The main arguments of those scholars who triggered the discussion about such a new IPR on data focused instead on the reasoning that exclusive property rights on data (1) might help to create markets for data, and therefore lead to better access and use of these data and (2) might solve problems that individual persons and especially also small- and medium-sized enterprises (SMEs) might not get a fair remuneration of their data through the contractual arrangements about data in the market. These are very similar to the reasoning of the Commission in the Communication "Building a European data economy".14 From the economics of traditional IPRs it is well-accepted that the "propertization" of innovation (and creative works) through the IPRs can help to create markets for innovations and might reduce transaction costs for trading and licensing innovations.15 From the few empirical studies that exist about trading of data (data brokers, data marketplaces etc.) we also know that trading of data in the digital economy is not well-developed so far. Although there is much need for more research in regard to data markets for understanding their transaction problems, these studies so far have not supported the hypothesis that the lack of property rights on data is one of the main causes for potential market failure problems in regard to the trading of data. It might be much more the problem of information asymmetries about data quality and data provenance, lacking demand for data (due to unawareness of the value of data), lack of interoperability and standardization, problems of pricing data, and strategic reasons of the data holders not to share, trade or give access to data.16 In regard to the second argument about the possibility of "unfair" remunerations of data, especially - as repeatedly suggested in the Communication - through "unequal bargaining power" situations in the market, it has

13 See Kerber (2016b, 992; 2017, 7-11).
15 See, e.g., Burk (2012) and Spulber (2015).
to be admitted that market failure problems through market power and/or information asymmetries with potentially "exploitative" results might occur. However, such problems cannot be solved by defining and granting exclusive property rights on data to the "data producers", because in such "unequal bargaining situations" such rights would be bargained away in the contracts. Therefore the proper solution for these kinds of problems is the application of competition law, consumer law (and in regard to data also data protection law) as the well-established policy solutions for these market failures. Therefore both reasoning cannot support the claim that new property rights on data are needed from an economic perspective. In addition to that, it can be shown that the introduction of such a new exclusive property right on data can lead to large costs and endanger competition and innovation, especially through legal uncertainty (about the specification and allocation of these rights) and through monopolisation of information and blocking of innovation. Exclusive property rights on data might, in particular, not fit into the functional logic of the digital economy, which relies on the access to and combination of as much data as possible, and therefore might impede data-driven innovation.

From an economic perspective so far no studies exist that would support the introduction of exclusive property rights on non-personal data. Although this topic is discussed among lawyers much more controversially, it seems that there is a clear majority of scholars who think that such an exclusive property right on data is either not necessary and/or does lead to so many potential problems in regard to legal uncertainty, not fitting into the system of IPRs and/or endangering competition and innovation that it cannot be supported. At least as important is that there is so far also no support from firms and industry associations for the introduction of such property rights.

This discussion however has triggered new debates about a wide range of different questions about rights on data. Especially important is the discussion about new rights on access to data. Should firms that are holding data have obligations under certain conditions to grant other firms, individual persons or public authorities access to these data? In regard to personal data, data protection law in the EU grants persons a large set of rights in regard to their personal data, e.g. to access them, to retrieve them, and also transfer them to other firms (data portability). The question is whether also in regard to non-personal data persons or firms might have or should have rights to access data, e.g., to certain sets of raw data for being able to enter markets for maintenance and repair services or for developing new innovative products or services, which cannot be offered without these data. Therefore, the Commission discusses in its Communication also several options for rules how and under what conditions such rights of access to data can be granted (EC 2017a, 2017b). Since data are non-rivalrous goods and there does not seem to be a general incentive problem for producing data, from an economic perspective the balancing of costs and benefits for granting access rights to privately held data might lead to a much more favorable assessment of mandatory access rights to data than in cases of compulsory licensing of patents and copyrights, where serious problems for innovation incen-

---

17 See Kerber (2016b, 995-996), DrexI (2016, 342); see for a broader analysis of possible distributional and fairness discussions Kerber (2017, 14-17).
18 See for the difficulties of specification and allocation of such a right Wiebe (2016), and in regard to connected cars especially BMVI (2017); for the many other dangers of introducing such a right for competition and innovation, see Dornier (2014, 625), OECD (2015, 195-197), DrexI (2016, 27-29), and Kerber (2016b, 996-997).
20 See for data portability from an economic and legal perspective Duch-Brown/Martens/Müller-Langer (2017a, 43-46) and Schweitzer/Peitz (2017, 39-45).
tives might emerge. In addition to that, also the economics of the digital economy and Big Data offer strong arguments about the crucial importance of access to data for data-driven innovation (OECD, 2015, 2016). Therefore, in regard to data also more far-reaching solutions are discussed (going beyond the well-established but narrow solutions in competition law, e.g., refusal to license as abuse of dominance according to Art. 102 TFEU).

Access rights to privately held data might play an important role in many IoT-applications that can be described as multi-stakeholder situations. For example, in "smart home" or "smart energy" applications, several stakeholders as the tenants, the facility management, the producer of the devices as well as energy companies, and others might have legitimate interests in the same data, and also might have contributed in producing them. In the same way also in the informationally integrated value chains of "smart manufacturing" several firms might have contributed to the production of data as well as many firms in the network might need to have access to the same data.21 We will see that a similar situation exists in the example of connected driving. In all these situations it might from an economics perspective not be optimal that only one party has either an exclusive property right or a de facto exclusive holdership of these data, because this allows for "data hold-up" situations with the possibility of exploiting other stakeholders and/or rendering them reluctant to invest in such informationally integrated value chains (and networks). If, however, each firm that is participating would be granted rights as legal "co-owners" of the data, then again hold-up and mutual blocking situations might emerge (anti-commons problem).22 Therefore it is necessary to find appropriate complex data governance solutions for dealing with the problems that several parties might contribute to the production of data and also several (and often different) firms might need these data.23

Usually we would expect that firms can solve these problems through appropriate private data governance solutions through contracts (and offering access rights voluntarily in the contractual arrangements), but it cannot be excluded that the market does not always work so well, especially in cases of complex multi-stakeholder-situations, as, e.g., connected cars. As a consequence it might be necessary to look for regulatory solutions to these problems. In that respect, the granting of certain data access rights to specific stakeholders is being discussed as an interesting solution.24 This would imply that certain stakeholders can claim to get access to certain data from the de facto holder of these data. In the motor vehicle industry such a regulated access for technical information already exists for "repair and maintenance service information" (RMI) for independent service providers.25 Since however the technological and economic conditions in different IoT-contexts can be very different, it is hard - on the basis of our current knowledge - to develop general criteria when and how such access rights

---

21 Another much discussed example is "smart agriculture" where both the farmers as well as the farm machine manufacturers have a large interest in the same data, the farmers for optimizing their agricultural activities, and the manufacturers for improving their machines. See for these examples, e.g., EC (2017b, 25-28), Duch-Brown/Martens/Müller-Langer (2017a, 33). For the characterisation as multi-stakeholder-situations and its implications see Kerber (2017, 16-21).

22 The anti-commons problem (Heller/Eisenberg 1998) is also well-known in the patent thicket literature leading to the danger of mutually blocking innovations due to overlapping patent rights (see Shapiro 2001).


24 See for such proposals especially MPI (2017), Drexler (2017) and the discussion in Zech (2017) and Kerber (2017, 18-20)

25 See EC (2014) and below in section 3.3.3.
should be granted (and about the specific conditions for access, as, e.g., fees). Therefore it is advisable to start with sector-specific solutions about solving these problems of data governance. In the next section we therefore try to develop a general theoretical framework that should help us from an economic perspective to find specifically tailored data governance solutions for the different data governance problems in different sectors and IoT-contexts.

2.2 Data Governance Regime: A Theoretical Framework

Since in many IoT-contexts we will have complex multi-stakeholder problems that presumably also require complex institutional solutions for dealing with data, we would like to use the term "data governance regime" for describing the entire set of institutions that deal with data. A data governance regime encompasses all legal rules and rights as well as contractual arrangements that are relevant for the production (collection) of data, the storing and processing of data, the analyzing of data, e.g. also through combination with other data, the use of data (for what kind of purposes), granting access to data for others through sharing, transfer or licensing, and the protection of data against destruction, compromising, copying, or misappropriation. From a legal as well as an economic policy perspective, we have to distinguish very carefully between two different levels of data governance. There are, on the one hand, the legal rules and rights on data that are part of the legal framework for markets, and which all private parties have to comply with (data governance regime level I), and, on the other hand, the data governance solutions that emerge in the markets, based upon contractual arrangements between private parties via freedom of contract (data governance regime level II).

Data Governance Regime Level II: Private Data Governance Solutions based upon Contracts in the Market

It is important to understand that a large part of the institutional solutions for the governance of data is based upon myriads of contractual arrangements between private parties in the market. This might be contracts about explicit trading (or "licensing") of data (data brokers, data market places) or about providing "free" services and allowing the service providers to use the data of the users ("data as counterperformance") as part of standard form contracts ("privacy policies"). In the connected cars example it can be expected that, e.g., car owners will provide a large amount of data through connected driving to the car manufacturers as part of their sales contracts and/or their contracts about specific services with the car manufacturers. But contractual arrangements about data are also crucial in many B2B contexts. Especially the contractual arrangements within the informationally integrated value chains (or networks), e.g., in "smart manufacturing" / "industry 4.0"), often include highly complex and sophisticated governance solutions for data. This implies that it is determined by contracts who (within this value chain or network) has de facto control about what kinds of data, who has rights to access and use these data (and for what purposes), who has the right to grant access to other parties, and can get the revenues from these data. In the digital literature it is often emphasized that firms build entire data ecospheres with many firms based upon contractual arrangements. Since the business models can be very different, also very different contractual solutions in regard to the governance of

26 See, e.g., Drexl (2017, 419), Kerber (2017, 21-23), and Schweitzer/Peitz (2017, 81).
the data in these value networks might be optimal and efficient. In the policy discussion about data ownership industry representatives have emphasized that these data governance solutions based upon contracts in B2B-contexts are generally working well and that therefore policy-makers should be cautious in regard to intervening into these data governance solutions that emerge in the market. Therefore in the discussion about new rules and rights in regard to data in B2B contexts many scholars and interest groups emphasize the importance of freedom of contract in regard to the governance of data (at least in regard to non-personal data).

Data Governance Regime Level I: Legal and Regulatory Framework for Private Data Governance Solutions: The "Rules of the Game"

Since markets need institutional preconditions as the protection of private property and freedom of contract and a large number of specific legal and regulatory solutions for ensuring a proper working of market and competition as well as remedying different kinds of market failures, the most important task of public policy is to establish a proper legal and regulatory framework for the market. From a constitutional economics perspective, which distinguishes between the market game and the rules for the market game that all players in the game have to comply with, the question has to be asked what the optimal rules for the market game in regard to data are.28

These rules would determine how private parties can deal with data. This would comprise rules what kinds of data can be produced (collected) under what circumstances (e.g. tracking surfing in the internet or the location of mobile phones, or identifying people by using face recognition in public places),29 whether and how (and how long) these data can be stored (and where), whether and for what purposes (and by whom) these data can be accessed and used, whether and under what conditions they can be analyzed (for what purposes) or they can be traded (licensed) on data markets, and who should get the monetary (or non-monetary) benefits for these data. However it would also determine whether and to what extent private parties are granted exclusive (property) rights on certain kinds of data (as, e.g., through traditional IPRs or the newly suggested data producer right), or a set of rights in regard to personal data (as in EU data protection law) that everybody has to respect, and which protects these data to a certain extent. From an economic perspective we could use the basic idea of the property rights approach that asks for the optimal specification and allocation of a bundle of rights on goods, and ask what might be the optimal specification and allocation of a bundle of rights in regard to data.30 Since data is a non-rivalrous good whose production also might often not raise an incentive problem, the optimal bundle of rights, especially in multi-stakeholder contexts, might look very different in different settings. Such a bundle of rights can consist of rights to exclude others (as, e.g., a traditional property right) but also grant rights to access these data to a certain set of stakeholders or only encompass certain specific protections for de facto holders of data, as, e.g., damage claims (based upon tort law).

---

28 From a constitutional economics perspective see Buchanan (1987) and Vanberg (2005); from the ordoliberal perspective of the Freiburg School of Law and Economics see Eucken (1952). Both closely connected theoretical (institutional economics) approaches view the setting of a proper set of rules for the market as the main task of economic policy.
29 One interesting example is the use of dashcams in cars, which is allowed in very different ways in different countries (see Hornung/Goeble 2015, 267).
30 See for an overview of relevant literature on property rights and its applicability to data Duch-Brown/Martens/Müller-Langer (2017a, 29-32).
in the case of the destruction of data or the obstruction of access to the data of a de facto data holder. Therefore there might be a wide continuum of optimal bundles of rights on data from a) traditional exclusive property rights at the one extreme, b) sophisticated combinations of protection against certain kinds of dangers for the data holder and access rights for other stakeholders, to c) open data solutions that put the data in the public domain at the other extreme.\footnote{One option is also that the de facto holdership of privately held data is respected and also to some extent protected by the legal system but that, e.g., the state or regulatory authorities might have access to certain kinds of data for specific purposes.} In that respect it is also necessary to distinguish between different types of data. It can be distinguished between raw data, processed data, and data as the result of data analytics (e.g. also inferred data), personal and non-personal data, data at the syntactical level (codified information) or the semantic level (meaning of information),\footnote{See for this difficult but very important distinction and the general complex relationship between data and information Zech (2015a) and Wiebe (2016).} and what kind of information about what data subjects can be found in the data (health data, behavioral data, buying history, location data etc.). Important is that for different types of data different legal rules and rights might exist and be appropriate.

All of these rules and rights constitute the legal framework under which the markets, e.g. in regard to IoT-applications, deal with data in the digital economy.\footnote{In an even wider notion of the concept of a data governance regime, we could also include social norms and therefore informal rules that might be relevant in regard to data. In institutional economics both formal institutions (legal rules and rights, contracts) and informal institutions are seen as relevant for the behavior of individuals (see, e.g. North 1990). In this paper, we will focus only on formal institutions.} Therefore what kinds of data can be produced, are available for use in the digital economy, and under what legal constraints, and therefore also what kind of private governance solutions can emerge in the market depend on this overall institutional framework in regard to data. It is important to take into account that for these questions not only data-specific rules and rights are relevant but also many other legal and regulatory instruments that are important for the working of markets. Therefore also competition law, consumer law, trade secret law, tort law, and other legal solutions for remedying market failure problems or achieving other important public policy objectives can be relevant for the question what the overall institutional framework is how private parties and markets can deal with data. If, e.g., competition law can be used for granting access rights to certain data (e.g. through Art. 102 TFEU) or trade secret law can be used for protecting non-personal data against certain forms of misappropriation, then also these legal rules are relevant for dealing with data, and therefore can be seen as part of the overall data governance regime.\footnote{From a legal perspective there are also a number of aspects in regard to data for which constitutional law and human rights considerations are relevant. See for a constitutional law perspective on property rights on non-personal data, e.g., Wiebe/Schur (2017).} This is important, because this opens up the possibility that perhaps many problems that can emerge in regard to data might not need specific solutions through the introduction of new rights on data or data-specific regulation of activities but can be dealt with the regular and well-established legal instruments for dealing with market failure problems.\footnote{For example, the problems of potentially "unfair remuneration" of data through "unequal bargaining situations" might perhaps be solved best by the application of competition law, and not through a "data producer right".}
Framework for Economic Analysis: Market Failures and Other Regulatory Problems

**Normative objectives and analytical approach:** The question how an optimal data governance regime should look like requires also a discussion about the normative objectives that should be achieved by the set of legal rules and rights in regard to data. From an economic perspective, it can be asked what governance regime would maximize economic welfare. Since data are seen as an important input for the innovation of new products and services (data-driven innovation), the production and use of data play a key role for increasing welfare. However, the normative objectives of democratically legitimized legal systems can be much more complex. In the EU privacy is a fundamental value that is protected by European data protection law. Therefore the very specific and far-reaching set of rights persons have in the EU in regard to their personal data is based upon a political normative decision that privacy should be strongly protected. From an economic perspective this implies that there might be tradeoffs between privacy and economic welfare (as usually defined in economics). Therefore privacy is an additionally important normative objective for data governance regimes. Especially in regard to connected cars there is a wide-spread consensus that the protection of privacy is an important objective of any solution in regard to the data of connected cars. But data protection can also play important roles in other IoT applications (as smart home or smart energy). Beyond economic welfare and privacy also distributional effects of different sets of legal rules and rights in regard to data might be relevant from a normative perspective. As we have seen, there are a lot of concerns about the question whether the market would lead to a fair remuneration of data, and therefore a fair participation of data subjects in regard to the benefits of "their" data. The objectives of an optimal data governance regime might therefore be a combination of economic welfare, privacy protection, and distributional concerns, which can lead to difficult tradeoff problems between these objectives.

How can the question about the optimal design of a data governance regime be methodologically approached from an economic perspective? Especially in the IoT-context, we have seen that there might be multiple stakeholders and complex tradeoff problems. A pragmatic methodological approach would focus the analysis primarily on the existence of market failure problems in regard to specific sectors, as, e.g., connected cars, but to take into account simultaneously the constraints through data protection law (at least within the EU). This implies that we accept the existing data protection law as a given constraint, and ask what set of other legal rules and rights that are relevant for data would solve market failure problems in regard to data and therefore increase welfare. The analysis of distributional effects would only be additionally included as far as this has emerged as a potential issue in the discussion about data. Therefore the main approach is an analysis of market failure problems with data protection law as an additional constraint. Since however in IoT-contexts often complex multi-

---

36 It can also be discussed whether a total welfare standard should be used or - as in competition policy - a consumer welfare standard.
37 For a broader analysis of normative concepts in law and economics see Schäfer/Ott (2004, 20-49).
39 There might also be more policy objectives, esp. also safety (e.g., avoiding car accidents), and cyber security (which are legally often defined in a way that go beyond their welfare effects).
40 These tradeoff problems are aggravated by the fact that these objectives might not be well-defined and their relative importance politically very controversial.
41 This is implicitly also the approach in the current policy discussions about data governance in the EU. If we however take into account that the specifics of EU data protection law is still evolving, then we could also take into account in an additional step of the analysis what the optimal solution for the
stakeholder situations emerge and therefore several or even many markets might be simultaneously
relevant and related to each other, one important question is whether and to what extent several dif-
ferent market failure problems might emerge simultaneously and how they interact with each other.
This also implies that a well-designed data governance regime might have to find a solution that helps
to solve several (different) market failure problems simultaneously (with the complex tradeoff problems
that might arise in such settings). In the following, we will present an overview of potential market fail-
ure problems that might be relevant in regard to the governance of data in a specific sector or IoT-
context.

**Market failures due to lacking rights on data:** First, it can be asked whether there a market failure
might exist in this specific sector in regard to the production and use of data. Does an incentive prob-
lem for the production of data exist in this sector? What about the benefits and costs of producing data
(e.g., fixed and variable costs, economies of scale and scope) and the possibilities through technolo-
gy and contracts to ensure de facto excludability of the data, also in the case of granting others access
to these data (via data sharing / licensing etc.). Does a serious (and privately unsolvable) problem of
copying of data exist? Are there significant positive or negative externalities in regard to the benefits
and costs of data production that might lead to a deviation of the private value of data from the social
value of data? Such differences between the private and social value of data through externalities can
lead to either too small or too large incentives for the production of data, and therefore to an economi-
cally inefficient under- or overproduction of data. The decisive point for this analysis is that in specific
sectors (as, e.g. connected cars or other specific IoT-contexts) the answers to these questions might
differ significantly and lead to different conclusions about the necessity of protection against copying or
the need for clearer legal definitions of the set of rights in regard to data.

Such sector-specific investigations, esp. also through empirical studies, are even more necessary in
regard to the analysis of the often complex structures of multi-stakeholder situations in regard to data.
The basic problems have already been described at the end of section 2.1. If one firm (or several firms
jointly) have either exclusive property rights or exclusive de facto control of certain data, then this can
lead to data hold up-situations in regard to other stakeholders that either need access to these data for
offering their services and for innovations or that even have specifically invested in collaborations with
these firms, and are therefore vulnerable to such data hold-ups. It has to be analyzed to what extent
such situations can emerge (or whether these firms can also get access to these data via other

---

42 In regard to the benefits of data, it also can be asked how important the data in the entire chain of
value creation is in comparison to data analytics and algorithms that use data as inputs.

43 Please note that the assessment that we do not have a general incentive problem for the production
of data does not imply that there might not be incentive problems for the production of certain kinds of
data (both in regard to too high or too low incentives). So far we do not know much about the optimali-
ty of incentives for the production of specific kinds of data. This is an important topic for future re-
search (see Kerber 2017, 9-11). See for the problems of divergences between the private and social
value of data also Schweitzer/Peitz (2017, 13-14).

44 What personal data are and perhaps what degree of anonymisation is sufficient for transforming
personal data in non-personal data (that can be traded without the restrictions of data protection law)
can be also differently defined in different IoT-contexts (see for the legal discussion about different
degrees of anonymisation Schweitzer/Peitz (2017, 22).
means) and what the economic effects of, e.g., monopolistically high prices for the access (or discriminatory access) to these data for competition and innovation might be. Since data are non-rivalrous goods, the balancing of the effects of granting access rights (with or without remuneration) does depend also critically on the question whether the data holder is in need of revenues as an incentive for producing these data, or whether this is not the case. If no serious incentive problems arise, then far-reaching access rights might be welfare-enhancing, because this can lead to a larger use of these non-rivalrous data and therefore might enable more innovation. This is also the basic rationale for reasonings which favor data governance solutions that are closer to "open data". This is also closely connected to the question whether from a public interest perspective certain kinds of data should be provided as a public good (as, e.g. for public statistics, and then granting free access to public sector information). From an economic perspective, this might be welfare-optimal for some kinds of data, implemented by either mandating free access or subsidizing free access to privately held data.

However the problem of finding well-balanced solutions between the interests of different stakeholders often might get additionally complex, if from a normative perspective not only welfare but also additional public policy objectives ("public interest"), as safety, security, environment, and especially privacy protection plays a large role, as we can see in a number of IoT-applications (and, in particular, in our example of connected cars).

Another interesting specific topic that is being discussed in regard to data is the question that in some contexts it might be necessary to aggregate as many data as possible (or even all data), because this would increase the quality of the results of data analytics. This, is, e.g., a topic in regard to health data but can also be relevant in regard to traffic data, and in other contexts. This would imply that a situation, in which there are a number of de facto data holders with each a limited set of data might lead to market failure problems in regard to the analysis of data, because a data analytics firm would need access to all these data for achieving the best results. In the scant literature about this problem, this issue has been described as "data fragmentation" or "data aggregation" problem. It can be investigated for specific sectors whether such advantages of "data aggregation" exist, and whether the market is capable of dealing with it, e.g. through "data pooling" or data trading, or whether market failure problems might arise in that respect. It might well be that the data holders might have enough incentives to agree to institutional arrangements that allows the analysis of an aggregated set of data. However there might also be serious impediments for such solutions, perhaps also through regulatory barriers for giving access to data (esp. also through privacy protection) that might make such private solutions difficult or impossible. Even if the market can solve the problem, the benefits of data aggregation can be so large that a natural monopoly situation might arise (i.e. that it is optimal that only one firm has all the data), which again might raise serious competition concerns that have to be dealt with.

---

45 For the problem of opportunistic behavior in hold up-situations with transaction-specific investments see the governance-approach of Williamson (1979). Important is that Williamson did in such contexts not focus on fairness-aspects through "unequal bargaining situations" but on the efficiency implications through reduced incentives for investing in such transactional relationships. Therefore from his perspective (unsolved) hold-up-problems might lead to less investment in such multi-stakeholder situations and therefore also to less innovation.

46 See for such a perspective OECD (2015, 2016).

47 See the proposals about mandating access to data in the "public interest" in the Communication "Building a European data economy" (EC 2017, 12).

48 See Burk (2015, 249) and particularly the discussion in Duch-Brown/Martens/Müller-Langer (2017, 29-32) with many additional references.
Market failures due to competition problems: In addition to these potential market failure problems in regard to the question how an optimal bundle of "rights on data" might look like, especially in regard to complex multi-stakeholder situations, there can also emerge a number of other market failures that might impede that the markets are capable of finding optimal data governance solutions based upon contractual arrangements. One possibility are market failures due to anticompetitive behavior of firms, which would call for competition law solutions. Already well-known are the market power problems that can arise through platforms with large direct and indirect network effects (multi-sided markets), which can lead to quasi-monopolistic market positions (Google for search engines and Facebook for social media) and might allow these firms to apply foreclosure strategies against competitors and perhaps exploitative behaviour in regard to the extent and transparency of data as counterperformance for "free" services.\(^{49}\) The question emerges to what extent also in the context of IoT-applications advantages of direct and indirect network effects can emerge with the danger of tipping of the market to one dominating platform. Dominant firms in regard to IoT-applications however might also emerge outside of the specific effects of platform economics and can lead either to a dominant position in regard to specific data, which can be used for foreclosing competitors on up- or downstream (or complementary) markets by refusing access to necessary data. However, it is also possible that firms conclude in regard to technological decisions about the design of data-producing devices or their business models in regard to dealing with personal and non-personal data. Both kinds of collusion might lead to the problem that consumers (and perhaps also other firms with complementary services) might not have a choice between different technical solutions of a data-producing device and/or data governance solutions, esp. also in regard to the question, to what extent manufacturers of data-producing devices offer different privacy and data governance options. Similar problems can emerge through mergers. An especially important competition problem might arise in regard to aftermarket services or complementary services for a data-producing IoT-device (with lock-in problems for the buyer), if these services need access to the data of this device for entering the market. This is already discussed intensively in regard to the data of connected cars, esp. in regard to repair and maintenance services but also in regard to other service providers.\(^{50}\)

Market failure due to information / behavioral problems: The other large group of potential market failure problems refers to information and behavioral problems, esp. of consumers, in regard to decisions about privacy and the provision of personal and non-personal data in IoT-contexts. In the economic and legal discussion about privacy the so-called "privacy paradox" has been discussed for some time.\(^{51}\) The privacy paradox describes the problem that most users of the internet express in surveys much concern about their privacy and would like to protect it, whereas at the same time most users of the internet seem to be very generous in regard to their data in their actual behavior, e.g., by not using privacy-protecting software etc. This privacy paradox has been interpreted very differently, and led to a lot of empirical studies about the reasons. The interpretations range from one extreme that most people do not really care about their privacy, because they do not have strong preferences

\(^{49}\) See, e.g., Monopolkommission (2015).

\(^{50}\) See C-ITS Platform (2016), EC (2017c), and, in much more detail, below in section 3.3.4.

for privacy, to the other extreme that individuals are not capable of making meaningful individual decisions in regard to their privacy, which would suggest that freedom of contract about the extent and conditions of providing data might not be the appropriate solution. Especially the massive collection of data through Google, Facebook, and other tech companies, as a de facto counterperformance for "free" services has triggered a discussion whether and to what extent the users of these "free" services are really capable of making "informed decisions" about the provision of data to these companies. The main concerns in this context are that the firms who are collecting these data are not transparent enough about the extent of their data collection and how they are using these data, and that they are offering in their "privacy policies" not only not enough information about this, but also do not offer enough options for the users to make differentiated decisions about the extent of provision of data and how these firms can use their data. In addition to information problems also behavioral (economics) insights into the privacy behavior of internet users play a large role in empirical studies. An important broadly accepted insight is that individual decisions about privacy and providing data can be very context-specific. All of these studies and insights have gotten a lot of attention in the legal and regulatory discussion about these issues. Especially important is the question whether the current solution of "notice and consent" is working sufficiently, whether the information requirements (i.e. the transparency of privacy policies) have to be increased, whether more privacy-friendly default rules should be implemented (privacy-by-design), or whether even the entire system of individual decision-making about the provision of personal data through "notice and consent" might suffer from fundamental problems and should be put under scrutiny. It is clear that all these questions are also relevant in IoT-contexts, and also in regard to the "consent" of car owners in regard to the provision of personal and non-personal data to car manufacturers. It is therefore necessary to analyze also specifically whether and how such problems can emerge in IoT-applications and how they could be solved in these specific contexts..

**Market failures due to transaction cost problems:** A smaller group of market failure problems can be linked to the problem of transaction costs in regard to data. One of the important discussions about possible problems for a thriving data economy refers to the problem that trading of data so far does not seem to work very well, although we still do not know enough about the reasons. One part of the reasons seems to be that firms often like to keep data for themselves for strategic reasons, which also might be linked with competition problems. But there also might be too large transaction costs in regard to data, perhaps partly due to legal uncertainty, esp. in regard to (the definition of) personal data, but perhaps also in regard to information asymmetries about the quality of data and problems of making contracts about the "licensing" of data and monitoring them. However the fact that not much direct trade can be observed need not imply that the information from these data are not commercialised, because this can also be done through offering services based upon data (as, e.g. targeted advertising). Therefore in regard to a certain sector or IoT-application it can be asked what kind of specific transaction problems in regard to the trading / licensing of data (beyond the excludability problem)

---

52 See Solove (2013), Luzak (2014), European Data Protection Supervisor (2014), and Acquisti et al (2016, 479). Schweitzer (2017, 277-291) is skeptical that competition is capable of determining a proper "data price" as counterperformance for "free" services in the individual decision model. Schweitzer therefore favors to use more the other legal exceptions of the future GDPR for processing data that do not need explicit consent but are subject to a balancing of interests, as, in particular, Art. 6 para. 1 lit. f GDPR. Such a balancing of interests can however imply large legal uncertainty.

53 See the references in fn.17.
might exist? Are there indications that not enough trading or sharing of data are caused by lacking property rights on data or - more generally - legal uncertainty about the "rights on data", esp. also in regard to personal data that are subject to data protection law? Or do we have a problem in this sector with the quality of data and information about the provenance of data or are these data largely standardized and can their quality and provenance easily be verified? Answers to these questions would allow a better assessment about the specific market failure problems due to transaction costs, and also whether specific possible solutions, as, e.g. default rules or model contracts for data trading or licensing that can reduce transaction costs might help in that regard.

After identifying possible market failure problems and problems in regard to privacy protection in a specific IoT-context it can be asked whether traditional legal solutions as competition or consumer law are sufficient for solving these problems or whether more far-reaching and also sector-specific regulatory solutions are necessary for solving the problems in order to achieve a suitable data governance solution for this IoT-application. This also can encompass the introduction of specific access rights for certain stakeholders or other specifications of bundles of rights on these data. One important dimension of possible solutions might also be the technical dimension, because decisions on certain technological designs might also have considerable influence on de facto holderships of data and therefore on the overall data governance regimes. This is particularly obvious in regard to interoperability and standardization, because these decisions influence, on the one hand, the openness of technical systems or platforms (and therefore influence lock-in problems), and, on the other hand, also the extent to which competition between different systems is still possible or eliminated. However, technological aspects are also crucial for the important questions of safety and security in many IoT-contexts, especially in the example of connected cars. A particular difficult problem is that the rapid technological progress in IoT-technologies requires that all regulatory efforts for solving data governance problems should not impede new innovations, i.e. that they should be open for new innovations. Therefore the legal framework for the governance of data should limit the freedom of private parties for finding new ways of producing, creating, and using data, and therefore developing innovations in form of new products and services only as far as it is necessary for solving market failure problems and achieving other basic normative objectives of society. However, at the same time, we also know that new innovations can lead to new kinds of market failures in regard to data governance and privacy protection, and might therefore require adaptations of the data governance regime. However such coevolution of technology and the legal/regulatory framework (which mutually influence each other) are a normal phenomenon in rapidly evolving economies.

---

3. Towards a Data Governance Regime for Connected Cars: An Explorative Analysis

3.1 Connected cars and data: Introduction

The main feature of a connected car is that it enables a wireless connection to the car and in particular a connection to the internet (Johanning/Mildner 2015, p. 2). It enables sending and receiving different kinds of data for different purposes. Internet connectivity can be established by either using a built-in SIM card in the car, an external SIM card used with an interface in the car, or by using a smartphone’s SIM card and a Bluetooth connection to the car (ibid. pp. 6). A connected car can also enable the possibility to communicate wirelessly with other cars or the surrounding infrastructure (“Car2x”55). The main benefits of a connected car are applications in three different areas: Traffic security and efficiency as well as infotainment (ibid, p. 5). As an example, car drivers can receive critical information updated in real-time about road and weather conditions over the internet. These vastly enhanced communication abilities can prevent accidents and make traffic flows more efficient (especially if they are also centrally coordinated). Infotainment systems connected to the internet allow the car driver to experience all kinds of digital services (e.g. social media) and assistance systems (e.g. navigation systems) (ibid., McKinsey 2015, pp. 13). It might also be possible to download apps directly to the car depending on the technologies used. For businesses, the connected car represents not only a product, but a platform for which digital services can be sold. This is in line with the notion of a connected car ecosystem which becomes more and more relevant (BVDW 2016, pp. 3). The market size of car connectivity is expected to increase to about 170-180 bn EUR by 2020 (Mckinsey&Company 2014, p. 7). The vision of autonomous vehicles, which also might communicate with each other and with the surrounding infrastructure, can be seen as a prospective development stage of the connected car and related technologies (OECD/ITF 2015, p. 14). The widespread adoption of autonomous cars then likely involves different intermediate steps and solving many technical and legal issues. This however can be seen as a realistic scenario in the future, based on the intelligent assistant systems active in cars today and the experiments we observe with autonomous vehicles. While a trend to more and more automation becomes evident, companies might also aim at directly developing autonomous vehicles (e.g. Google self-driving car) (Petrovic et al. 2015, p. 3).

On both sides of the Atlantic, authorities have started to adapt regulatory frameworks to take into account more and more connected and eventually autonomous driving. In the United States both on the state and the federal level regulatory adaptions are made or discussed regarding testing of autonomous vehicles and their operation in the public. On the state level (e.g. in California), this refers to very concrete approvals to test autonomous vehicles while on the federal level authorities develop best-practice and policy guidelines to foster research and development of autonomous vehicles (Gilbert/Zallone 2016, pp. 1). The European Commission aims at fostering and harmonizing automated driving and already implemented legislation (e.g. the ITS directive). On the one hand this relates to enabling research to foster more efficient transport systems and on the other hand to ensure public safety, e.g. through the e-call directive.56 Individual member states have their own programs to adapt

55 We can distinguish Car – 2 Car (a car wirelessly communicates with other cars) and Car – 2 – Infrastructure (a car wirelessly communicates with the surrounding infrastructure e.g. traffic light/signs or other traffic management systems (Johanning/Mildner 2015, pp. 66).

56 E-call is an automated and sensor based emergency call system in cars. It established an audio connection between the car driver and a Public Safety Answering Point in case of a severe accident.
regulatory frameworks to enable autonomous driving (Gilbert/Zallone 2016, pp. 11). However, the ensuing policy questions are complex and so far widely unsolved. They are also connected to many technical questions as the development to more and more connectivity and automation continues. Some of these questions refer to interoperability and standardization issues but there are also many unsolved legal and regulatory issues, especially in regard to liability questions in regard to connected / automated (and later autonomous) driving, to the problem of protecting personal data and privacy as well as to the issue of data ownership, access rights to data and trading of the data that are produced in the connected car.

One of the most controversial technical questions currently discussed is how the technical architecture of connected driving should look like, because this is important for the communication and technical possibilities for processing and accessing data. We will see that this is not just a technical question, but also a data governance question since the system of collecting and processing data determines who controls the data and can therefore grant access to it. The data collected can be very different and for example relate to technical data about the vehicle (e.g. engine type), the driving behavior (e.g. speed, direction) or the environment of the vehicle (e.g. weather conditions). Collected data can be personal or non-personal. The question whether data is personal or non-personal is also not clear-cut. For example, combining dynamic data about the vehicle (e.g. motor status, tire pressure) with location data might clearly point to a certain individual and even her driving behavior. Personal data could be generated by just connecting non-personal data with personal data (BMVI 2017, pp. 20). It might also be possible to generate personal data by connecting different non-personal data sets (Lüdemann 2015, pp. 250). This means that almost all data in the connected car might have a personal dimension (Deutscher Bundestag 2016, pp. 5, Lüdemann 2015, pp. 249). We will see that the interests of different stakeholders are partly in conflict with each other. For example, car manufacturers are interested in restricting access to vehicle data to ensure their control of the data and their competitiveness vis-à-vis large tech companies while independent operators are interested in having broad access to data for serving their customers (C-ITS Platform 2016, pp. 88, ACEA 2016b, pp.8). However, in regard to these conflicts we also should keep in mind that data are non-rivalrous goods which would allow that several stakeholders can use the same data simultaneously. In the following, we will present a brief overview about the most important stakeholders in regard to the governance of data in the connected car and about different technical architectures of a system of connected driving that are currently under discussion.
3.2 Connected Driving: Structure, Stakeholders, and Technical Models for Data Access

3.2.1 Data of Connected Cars: Stakeholders and their Interests

In regard to the data of connected cars we have a complex multi-stakeholder situation. Car manufacturers, component suppliers, spare parts producers, independent repair service providers, insurance companies and providers of infotainment applications for in-vehicle use (e.g. media apps) can use data to develop, offer and improve their products and services. The following fig. 1 gives a brief overview about the most important stakeholders.

Figure 1: Stakeholders of the connected car

Source: Own representation partly based on PwC (2016), p. 15.

The car manufacturers are producing and selling the cars on the car market. They are interested in getting as much control as possible about the vehicle data, because such a de facto control about the data allows them to commercialize these data and get additional revenues in addition to the sale of the connected cars to the consumers. The control about the data as well as control about the access to the IT-system of the connected car also might allow them to control additional markets for complementary services and products that can be offered to the driver and passengers of the cars. Independently from these additional sources of revenues they also need directly certain technical data about the car for monitoring and improving connected driving as well as for innovation. Car owners (and car drivers) are interested in the benefits of connected driving, e.g. Advanced Driver Assistance Systems, but they
might also be interested in being able to have access to many services in the connected car. In regard to data they might be interested to protect their personal data and privacy according to their specific privacy preferences but perhaps also in commercialising both the personal and non-personal data of the connected car. Since cars are produced through a value chain with many suppliers of car components, also these suppliers might be interested in the data for connected cars, partly because it might also be their components that produce part of these data but partly also because these data might help them to improve their components and also stimulate innovation. Another important group of stakeholders are independent providers of repair and maintenance services (as well as spare part producers). They might need access to certain kinds of data for being capable of offering certain services and products in the aftermarkets. It is important that in this context already before the emergence of connected cars a regulation had been established to make sure that independent providers of repair and maintenance services have access to technical information for ensuring competition in these markets for repair and maintenance services. Another particular group of stakeholders are insurance companies who are interested both in data about the behavior of drivers for offering more risk-adjusted insurance schemes to the car owners and general data about driving safety for helping car drivers to reduce the risks of accidents. One large and heterogeneous group of stakeholders finally are all providers of other kinds of (mobility) services for car owners, car drivers and car passengers, e.g., navigation, parking apps, intelligent assistants, and especially also infotainment, commerce and many others. They are above all, on the one hand, interested in the access to the IT-system of the connected cars for offering their services, but might also, on the other hand, be interested in different kinds of data that are produced in the connected car. The last group of stakeholders in regard to data are public authorities who could use certain data for improving policies in regard to traffic safety (e.g., e-call) and regulation, but also for environmental policy or even for fighting criminal behavior. In addition to that (and not included in fig.1), data from connected cars can also be used for data analytics in regard to the use in other sectors of the economy. Therefore, there might be an interest to sell part of these data on data markets (especially in an anonymised form) and/or combine them with other data. Due to the rapid technological progress the demand for specific data of the connected car through different stakeholders as well as the kinds of data produced in the connected car might change over time.

3.2.2 The C-ITS Platform Initiative and Its Five Principles of Access to In-Vehicle Data

Due to the complex structure of connected driving with many stakeholders the European Commission has started in 2016 the C-ITS (Cooperative Intelligent Transport Systems) initiative to foster “cooperative, connected and automated mobility” (EC 2016, pp. 4). The C-ITS Platform aims at bringing together authorities, the stakeholders (e.g. car manufacturers, component and system suppliers and more) and the European Commission to develop policy recommendations regarding rules and regulations for connected driving (ibid. p.4 at fn.14). One of the crucial subjects is the question how data access should be ensured for independent operators in the connected car. The C-ITS Platform (2016) report is very important, because it represents a first attempt to find a consensus between all relevant stakeholders in connected driving. Especially important for the data governance issue have been the discussions in the Working Group 6 about “Technical issues - Access to in-vehicle data and resources”, because this triggered an additional (very recently published) EU study about “Access to in-
vehicle data and resources" (EC 2017c), which analyzed this issue much deeper and also discusses different scenarios and policy options. We will refer in the analysis repeatedly to both reports. A very interested contribution to the governance discussion are the five principles about granting access to in-vehicle data and resources that they could agree upon in the first C-ITS report, and which were used as a normative benchmark for a deeper analysis in the most recent EU study (EC 2017c):

"The five guiding principles that should apply when granting access to in-vehicle data and resources are the following:

(a) Data provision conditions: Consent
The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.

(b) Fair and undistorted competition
Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.

(c) Data privacy and data protection
There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.

(d) Tamper-proof access and liability
Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and resources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

(e) Data economy
With the caveat that data protection provisions or specific technologic prescriptions are respected, standardised access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources."57

We will not discuss these principles here but they seem to represent well the current discussion about the potential objectives of policies and the trade offs that have to be taken into account in order to find an appropriate technical and regulatory governance solution for connected driving and the governance of the data produced in this system.

57 C-ITS Platform (2016, 11).
3.2.3 Technical Models for Accessing In-Vehicle Data

Currently three different technical models (or technical architectures) are discussed how in-vehicle data in the connected car can be accessed (see C-ITS Platform 2016 and its annexes for a more detailed description and EC 2017c): 58

(1) Data server platform (extended vehicle concept)

(2) In-vehicle interface

(3) On-Board Application platform

(1) Data server platform: The basic idea is that all in-vehicle data are transferred and stored on a central data server outside of the car (EC 2017c, pp. 45). In the concept of the "extended vehicle" which is proposed by the car manufacturers this data server platform is controlled by the car manufacturer. Specifications of the extended vehicle are adopted in ISO standards (C-ITS 2016 Annex WG6-A2D-Annex 3, p. 2). The data transfer is made via mobile data networks of internet service providers. Independent parties can access the data only through the central data server. In the discussions about the extended vehicle concept on the C-ITS platform the independent service providers and operators were very concerned about the conditions under which they can get access to these data. Car manufacturers might get competitive advantages on aftermarkets through their control of the vehicle data on the central server. In the proposal of the "extended vehicle" concept the car manufacturers emphasized that they would respect the existing regulations about personal data (data protection law) as well as the regulation about access to data for repair and maintenance services, but for other data and other purposes access to the data of the central server would be on a purely negotiated basis. 59 It has been very controversially discussed whether this would violate principle (b) for data access which should guarantee that all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the car owners. Therefore the independent service providers instead have suggested that access to the vehicle data on such a central server should be granted through a shared server operated by a neutral party or a consortium. The idea is that a consortium of stakeholders rather than the car manufacturer controls the central server (which technically could work similar to the central server in the extended vehicle concept). The car manufacturers expressed concerns about such a solution regarding security, liability, workability and organization (e.g. administering such a consortium of stakeholders) (EC 2017c, pp. 48). 60 61

---

58 Independent from these technical models it is also possible to display internet services or apps in a car or control it wirelessly. We find proprietary infotainment systems which can also have the possibility to connect them to smartphones as in the case of Tesla which allows a car driver to use a smartphone app to control certain elements of their car (controlling the temperature, the lights, battery status and other systems of the car or locking/locating the car). Systems like Android Auto and Apple Car Play allow apps which run on the smartphone to be displayed on the screen in the car (however they are no operating systems for the car yet and are rather extending the smartphone screen) (EC 2017c, p. 32). Applications like calling, navigating, using digital assistants or listening to music are possible. This works with compatible car models or in some instances with compatible aftermarket radios. Apple and Google collaborate with many car manufacturers to allow smartphones users to integrate their phones and apps into the car (Apple CarPlay, Android Auto).

59 See ACEA (2016a, pp. 5).

60 Although this adapted concept could possibly mitigate access problems, it is not so clear which data should be stored on a shared or neutral server and which should be exempted from it. It could be argued to not make available all kinds of vehicle data (e.g. if related to car manufacturer's or component supplier's IP rights) in a shared infrastructure (C-ITS Platform 2016, pp. 81). Also, it is not so clear which stakeholders should be part of a consortium controlling the shared server (or allowed to enter it),
(2) **On-board application platform**: “An on-board application platform allows unified deployment of applications on the HMI (Human-Machine Interface) of the vehicle whilst also allowing hosting of applications on the HMI using the vehicle internal resource” (EC 2017c, p. 32). Here the main idea is that the vehicle itself is the platform through which applications and services can receive and send data. This can happen wirelessly, e.g. through the mobile telecommunications networks. The “on-board application platform” can be regarded as a final stage of a development process which very likely requires intermediate steps (C-ITS Platform 2016, pp. 84, EC 2017c, pp. 32). The main difference in comparison with the extended vehicle concept is that the car owner (or car driver) has the de-facto control over her data. Therefore she can decide which third party service providers or apps can use the data. It is an open question, how an interface providing the car driver control over the data should look like in such a concept, and who should design it, because it does not seem necessary that the car manufacturer designs such an interface. The main concern of car manufacturers regarding this concept is security and safety of the car. Car manufacturers are concerned about the integrity of their vehicles if users can download third party apps, which cannot directly be controlled by car manufacturers (EC 2017c, pp. 42). This concept might solve the access problems of the “extended vehicle” concept (since third parties can be granted direct access through the car owner).

3) **In-vehicle interface**: This refers to a standardized physical connector to the vehicle through which a data stream can be made available. This plug can be used to collect data in different forms and also includes wireless transfer through, e.g., WiFi or the 4g networks. Such a solution can be seen as an upgraded “On-Board Diagnostic” (OBD) Adapter that is currently used for transmitting data for repair and maintenance purposes (C-ITS Platform 2016, pp. 82, EC 2017c, pp. 42). Although technically different this concept has many parallels in comparison to the “on-board application platform” in regard to data governance. In both concepts, it is the car owner (or car driver) who has the de facto control over the data. While the standardized connector determines which data can be transmitted and which cannot, the same is true for the “on-board application platform”. The main difference lies in the level of control for the car driver regarding sending and receiving data/connecting with third-party service providers, which is higher in case of an “on-board application platform”. Also, third parties’ access to the vehicle HMI and therefore to the consumer is lacking and “inferior” in comparison with the on-board-application-platform” (EC 2017c, p. 131). Car manufacturers expressed security and safety concerns regarding the “in-vehicle interface”, since the integrity of the car depends on controlling the entire system, including the adapter which is externally plugged in to transmit data (ibid.). Moreover the problem was identified that current in-vehicle interfaces potentially are not able to handle real-time data needs based on their computational power (EC 2017c, pp. 44).

In regard to these technical models or technical architectures of the flow and storage of the data of the connected car and technical options of accessing these data the extended vehicle concept of the car...

---

61 Another alternative proposal (made by IBM) consists of a “B2B marketplace” that would create a platform between the vehicle and service providers. This marketplace receives data from the car manufacturers’ servers (or the extended vehicle) but allows more direct interaction between different stakeholders (C-ITS Platform 2016, p.81). However this solution has not been seen as much different from the neutral shared server solution (EC 2017c, pp. 47).
manufacturers seems to be so far the clearest concept from a technical perspective which is also supported by an ISO standardization process. This is not so surprising, because the car manufacturers are in the best position to decide on these questions by technically designing the connected car. The decisive point however is that the decision about this technical architecture also can have far-reaching consequences about the question who has the de facto control about these data, which - at least in regard to non-personal data - would also imply a de facto ownership of these data in the absence of explicit legal rights on these data (see section 2). It might make a huge difference whether the legal or de facto rights to decide on the use of the data is primarily allocated to the car manufacturers or the car owners (or car drivers). Therefore, decisions about the technical architecture can influence the data governance regime in connected cars significantly, which however might be modified again through contracts in the market as well as appropriate regulation.

3.3 Analysis of stakeholders and potential market failure problems in regard to data of connected cars

3.3.1 Introduction

In section 3.2 we have seen that there are a large number of parties who are interested in the very different types of data produced in the connected car. We also have seen that different technical architectures for the connected car imply that different stakeholders in this system of connected driving can get the de facto control of these data, and that therefore the different stakeholders are interested in different technical solutions (extended vehicle, on-board application system etc.). This is particularly evident in the conflict between car manufacturers and independent service providers. However, a deeper analysis might show that this might be only one of the conflicts about data in the connected driving context. Therefore the objective of this section 3 is to analyze step-by-step these different stakeholders and their market relationships in regard to the data of the connected cars. Since some of these markets and relationships, as, esp. between car manufacturers, on the one hand, and their suppliers (of car components) as well as independent providers of repair and maintenance services, on the other hand, are well-known for specific competition problems and discussions about the need for regulatory solutions, we will analyze the specific emerging problems in regard to data within the much older context of these problems and regulatory solutions. Our analysis will focus primarily on the question whether there might exist market failure problems on the markets between these stakeholders and other regulatory problems, esp. in regard to the additional normative objective of protecting privacy. Therefore this analysis can be seen as a first step that applies (an important part of) the theoretical framework that we have presented in section 2. For an easier presentation of our analysis, it will often be convenient to use the "extended vehicle" concept of the car manufacturers as a starting-point for the analysis, which then can be compared to other solutions.
3.3.2 Car owners and car manufacturers: the market for connected cars

First we will look at the market for connected cars, with car manufacturers on one market side and consumers on the other. Connected cars allow for an increasing number of additional features and services that increase safety, convenience and fun for the drivers (and passengers) of the car. Right now there is competition between car manufacturers that offer both non-connected cars as well as increasingly more connected cars with a wide variety of features of connected driving (often in form of additional options that increase the price of the cars), and it will depend on the technological progress and the preferences of the consumers how fast and to what extent connected cars (and the extent of their connectivity) are spreading over time. Predictions show that rapid spreading of (elements of) connectedness of cars can be expected, but that there is much uncertainty about the velocity and extent of this diffusion process (McKinsey 2014, pp. 13). Concerns of the consumers about privacy and data security that might emerge with increasing collection of data in connected cars as well as concerns about the safety of automated (and later autonomous) driving and liability issues might influence the decisions of consumers and therefore the diffusion process of this innovation "connected driving". Therefore, solving all the open regulatory questions in regard to connected driving might be crucial for supporting and accelerating this diffusion process. However, there is a broad consensus that a rapid increase in the data that are produced by connected cars can be expected and therefore the issue of the governance of these data is important.

Ownership of data in connected cars: Legal starting-points

Both in the legal and political discussion the question emerged who is (or should be) the "owner" of the data that are produced by a connected car.\(^{62}\) We have already seen that many and perhaps most of these data are legally - at least in the EU - personal data according to the EU data protection law and therefore subject to a strong set of rights of the persons as data subjects with the need for consent for processing, storing and using these data for specific purposes. For simplification, we will assume in the following that the car owner is also the car driver (and also ignore the problem of personal data of other car passengers).\(^{63}\) Although EU data protection law grants individual persons strong rights to exclude others from using personal data, there is so far also a consensus that these persons do not have an exclusive property right in regard to their personal data. However, it is also broadly accepted that individual persons can give access to their personal data through contracts for certain purposes, both in exchange for money and in exchange for "free" services ("data as counterperformance").\(^{64}\) For non-personal data (e.g., purely technical data in the car) and for anonymised personal data no legal property rights and therefore no legal ownership exist. In the discussion about the proposals to introduce a new exclusive property right on those machine-generated non-personal data we have seen in section 2 that here the de facto data holder can sell the access to these data to other parties. If one

---

\(^{62}\) For legal analyses of data ownership in connected cars, see Hornung/Goebble (2015), BMVI (2017), and the legal annex in the recent EU study (EC 2017b, 179-199).

\(^{63}\) From the perspective of data protection law it is a difficult problem that car owners, car drivers and car passengers are different persons, each of whom has to give consent in regard to their personal data. This implies that the consent of a car owner for providing data of the connected car is not sufficient in regard to the personal data of a different car driver. See for this problem from a legal perspective Hornung/Goebble (2015, 272).

\(^{64}\) See, generally, Specht (2017) and Schweitzer (2017).
party has de facto exclusive control over these data (as, e.g., the car manufacturers in the "extended vehicle" concept), then this party is the de facto owner of these data, although this "ownership" is not legally recognized as property. But the data holder can trade the access to these data via licensing contracts, in which it is stipulated how these data are allowed to be used.

Summarizing these results about data ownership leads to the following conclusions: (1) Although there is no legal ownership of personal data, the consent principle of data protection law leads to strong rights to exclude other stakeholders from using these data and allow economically the choice between either not providing access (and protecting one's privacy) and/or selling the access to these personal data for certain purposes. (2) In regard to the non-personal data (and anonymised personal data) of the car there is neither an exclusive right on these data nor a legal decision on who should have the right on these data. This implies from an economic perspective that it depends on the de facto holder-ship of these data and the contractual arrangements between the car manufacturers and other stakeholders, especially the car buyers/owners, who will have exclusive or non-exclusive de facto control of these data, and therefore are "de facto owners" of these data.

Price/data market outcomes in contracts in the car markets

From an economic perspective, the next step is now the analysis what will be the market outcome in regard to the allocation of the legal or de facto ownership of data of the connected car, if we assume that there is competition in the market for cars. First, we have to understand that the transition from traditional cars to connected cars also implies that buying a connected car does not only encompass a sales contract but also an ongoing, long-term contract about services (and updates) and transfer of data to the car manufacturer, i.e. that both parties are de facto in a long-term contractual relationship. This implies also that there is no more a simple price for the car but presumably a complex pricing structure (consisting of, e.g. a fixed price and on-going subscription fees for certain connected services that can be expected to also encompass data as counterperformance). Theoretically the car manufacturers can offer different contracts about connected driving with different options about who has the right or the de facto control of data. There might be contracts, in which a consumer only buys the car and is the holder of all the data that are produced in the car, and there might be other contracts, according to which the car manufacturer will hold all the data (and also has far-reaching consent to use these personal data). There might as well be contracts, which entail a specifically defined solution what kinds of data (and for what purposes) will be transferred to the car manufacturer and which ones will remain with the car owner. Here also the specific (privacy) preferences of the individual car owners might play a large role. If the data of connected cars are valuable and can be profitably used and commercialised by the car manufacturer, either for improving their own products or innova-

---

65 From that perspective, the proposal of the Commission in the Communication "Building a European data economy" (EC 2017a, 2017b) would make a difference, because it implies that the owners (or long-term lessees) of data-producing devices are viewed as the data producer, to whom this data producer right should be granted. It is very interesting that this implication of the "data producer right" proposal does not play a role in the most recent EU study about "access to in-vehicle data and resources" (EC 2017c).

66 However, the car owner might allow the car manufacturer access to all those data that are necessary for certain technical functions of the connected car, but this might be contractually restricted for this specific purpose. This might also exclude that the car manufacturer can sell these technical data to third-parties (a right that the car owners might retain for themselves).
tion, and/or for getting revenues through providing access to these data to other firms, then allowing the car manufacturers to use personal data or accepting that they get de facto control of the non-personal data is economically a non-monetary part of the price consumers pay for connected cars (data as part of counterperformance).

It would be an interesting research project in economics to analyze with economic models (industrial economics / law and economics models) what kind of contracts would be optimal and what outcomes in regard to prices and data can be expected to emerge under different assumptions about competition, information problems, (privacy) preferences, and other relevant aspects. Under simple competitive conditions it can be expected that prices for cars (and connected driving) will be higher, if the consumers like to keep data for themselves, and lower, if they are willing to provide data to the car manufacturers. Therefore the extent to which data can be used as part of the non-monetary price for connected driving (and therefore the allocation of the legal and/or de facto rights about data) will have an impact on the prices of cars (and connected driving). Since however different assumptions can be made about competition, e.g. oligopolistic settings, the results in regard to prices and data might be very different. In regard to the question whether it can be expected that the data are ending up with the car manufacturers or stay with the car owners, it is also very important whether the car owners have options to sell the data of their connected car also to other firms that are capable for using and/or commercialising these data. If this is not the case, either technically or due to a lack of a well-functioning market for these data, then the car owners only have the option to retain certain data according to their privacy preferences and sell the other data to the car manufacturer. Although in this case there is no competition for the data of this specific car (after the purchase of the car), there is still competition between car manufacturers in regard to the cars themselves, which also would include the conditions for using data as counterperformance (bundling of connected cars and contracts about data). If however the car owner is capable of selling these data also directly, e.g., through giving direct access to the data to a third party, then there would be direct competition between the car manufacturers and other potential buyers of the data of connected cars. In this case economic theory would expect that the car manufacturers would only end up with the data, if they can use them more efficiently than other companies (with perhaps very different business models). Otherwise the latter would be capable of paying higher prices to the car owners.

---

67 In these reasonings we always assume that either the car manufacturer or the car owner gets the exclusive legal or de facto control of the data. However, it is also possible that they agree on contracts, in which both can use the data, because data is a non-rivalrous good. For example, one interesting solution might be that one party gets exclusive control but the other party has still a non-exclusive access right for certain purposes (without being allowed to provide third parties access to these data).

68 The problem that data as counterperformance can be seen as a non-monetary part of the price influences also who is investing in the data. Since the question who makes the investments in data is seen as a very important criterion for the question who should be granted the new "data producer right" that is being discussed, it would depend on the question whether the price for the car would also consider data as counterperformance, whether such a new right should be granted to the car manufacturer or the car owner. See for this problem very clearly BMVI (2017, 98-100). The problem is that it not clear how such an assessment can be made, especially if "unequal bargaining power" situations might exist.
**Market failure problems**

From an economic perspective, there are therefore two different interesting questions: The first one is whether the markets work well enough that the legal or de facto ownership of data is allocated to that party that is best capable of using and/or commercialising these data. This would also include that the car owners can make rational and well-informed decisions about what kinds of data they are retaining due to their privacy preferences and which they are selling, either directly to other purchasers of data or as counterperformance to the car manufacturers. The second question is whether competition between car manufacturers is strong enough that the price reduction for data as counterperformance is large enough that the car owners get a sufficiently large ("fair") share of the value of these data. Therefore the question arises whether there is market failure due to weak competition between car manufacturers\(^{69}\) and whether there might be additional other market failures that lead to a too low remuneration for the provided data or a non-fulfillment of privacy preferences of the car owners.

This leads to the second potential market failure in the car market in regard to data and privacy. This is about market failures due to information problems (e.g. asymmetries), intransparency, and behavioral problems. In section 2.2. we already discussed the potential market failure problems in regard to individual decisions about privacy and data (privacy paradox / "notice and consent"). It is obvious that this potential market failure problem can also be relevant for the problem of the provision of (personal and non-personal) data of the connected car. Already the current solutions for data provision of connected cars rely on standard terms contracts about the provision of data and therefore use the same solution of "notice and consent". In this context it is important to analyze from an economic perspective whether, how and to what extent there might be market failures in regard to the consent of the car owners to provide data to the car manufacturers. From an economic perspective different reasonings can be made why a market failure problem might occur. One group of reasons encompasses information problems. These information problems can refer to lacking information about the extent and kinds of produced data in the connected car, e.g. that also the behavior of the car drivers as well as certain health data might be recorded and not only technical data about the working of the car. Even if the car owners know this, they might not be informed about how these data can be used, for what kinds of specific purposes, and what consequences this might have on themselves (e.g. premiums of car insurances). They also might not be informed about the (monetary) value of these data, and therefore might consent to the provision of data for a much too low remuneration (either in form of an additional "free" service or a too low explicit price). In the entire discussion about provision of data, there are a lot of concerns that consumers are not aware of the value of their data, and that they should be educated about this.\(^{70}\) A second group of reasons is based upon the meanwhile broad research on behavioral economics. This research tries to explain the privacy paradox with insights about systematic decision errors through behavioral problems. In that respect a broad literature exists that offers support for the thesis that the decisions of individuals about privacy might suffer from a number of serious problems. It has to be analyzed whether and to what extent this might be an even larger or perhaps also smaller problem in regard to the data of the connected car. Perhaps it is also a problem for specific types of

---

\(^{69}\) Another potential problem that we do not deal with here are problems through the lock-in situation that car buyers are facing, because connected cars will require some kind of long-term contractual relationship with the car manufacturers.

\(^{70}\) See in regard to the value of data in connected cars, e.g., BMVI (2017, 125).
data but not for others, because we know from the privacy paradox discussion that the behavioral problems in regard to privacy protection decisions might be very context-specific.

Overall, we have seen that there might be both competition problems (including lock-in problems) and information / behavioral problems in the car markets in regard to data. It is also an interesting research question to what extent both kinds of potential market failures might interact with each other. One possibility, for example, is that effective competition between car manufacturers might reduce the impact of information and behavioral problems in regard to data provision. However, the combination of both market failures might also aggravate the problems significantly. A specific problem might be that competition might not be strong enough to force the car manufacturers to offer privacy policies that allow for granular decisions about data provision, leading to the result that specific privacy preferences of individual car owners cannot be fulfilled. All of these questions show that it might be advisable to analyze the effects of both potential market failure problems simultaneously. From an economic perspective, it seems that in regard to both of these market failure problems there is not a large difference between the provision of personal data and non-personal data. It also appears - from the perspective of our analysis in section 2 - that there is not a large difference in regard to these market failures between the case that we have an explicit exclusive legal right on data or only an exclusive de facto control about data. But for both questions much deeper research is necessary.

From a policy perspective, the question arises whether the application of existing approaches for solving these market failure problems in regard to data, i.e. the application of competition law, consumer law, and data protection law is sufficient for remedying the emerging problems or whether additional regulatory measures, esp. in regard to data, are necessary for solving the problems (e.g., minimum requirements for offering privacy options to car owners).\(^{71}\) In that respect, it might also be interesting to introduce the discussion about the so-called Personal Information Management Systems (PIMS).\(^{72}\) Since individual persons and consumers have usually problems in managing / protecting their privacy and monetizing their (personal) data on markets, the idea of PIMS is that independent service providers help consumers in regard to the protection of privacy and commercialization of their data according to their own preferences. If we would have a well-functioning market for personal information management systems, then these service providers could help the car owners in managing and selling their data. This might also encompass negotiations with the car manufacturers about contractual arrangements about data. Through the combination of the data from many car owners, these service providers also might increase the bargaining power of car owners which might allow them to negotiate higher prices for the data (or lower prices for buying connected cars or connected services).\(^{73}\) Therefore it also could be discussed whether the promotion of PIMS would help to reduce potential market failure problems that we have discussed in this section.

\(^{71}\) It seems that we already have some specific (non-waivable) rights of access for car owners in regard to the data under de facto control of car manufacturers, e.g., in regard to investigations about accidents and warranty problems. Another important discussion that we do not address here refers to the issue of data portability for the car owners.

\(^{72}\) See for the discussion about PIMS European Data Protection Supervisor (2016).

\(^{73}\) This can be linked to the discussion about countervailing power in regard to the buying power of car manufacturers in regard to data.
3.3.3 Car component suppliers

For a long time the automotive industry consisted of the car manufacturers which develop the cars and a large number of suppliers for thousands of components which are used as inputs in the factories of the car manufacturers. The relationship between the car manufacturers and their suppliers has always been very close and not without frictions. The market position of the component suppliers is very different. There are, on the one hand, strong suppliers as, e.g. Bosch, who contribute complex components based upon own highly developed technology, but most suppliers do not have a strong position based upon unique technology and can therefore easily be replaced by other suppliers with more competitive prices. At the same time, the necessity to develop components specifically for the car of one car manufacturer and investing specifically in capacities for producing these components led to the problem that suppliers often depend to a large extent on specific car manufacturers after they made transaction-specific investments. Williamson's analysis of the hold-up problem due to transaction-specific investments can well explain the dangers that suppliers face by producing components for car manufacturers (Williamson 1979). Complaints that car manufacturers abuse the ensuing bargaining power to reduce prices in an unacceptable way have been discussed regularly in competition policy since the 1970s. Therefore the relationship between a car manufacturer and its suppliers has always been one of the important topics in the competition policy discussion about buying power.74 Although such bilateral dependencies with asymmetric bargaining power can arise in these situations, the car manufacturers have large incentives not to exploit these situations, because they also need efficient and innovative suppliers for staying competitive in their competition with other car manufacturers. Therefore it is much more important to them to collaborate closely with the suppliers for cutting costs, improving quality, and, in particular, also jointly develop new innovations. This close relationship, which early on has been characterized as quasi-integration, has existed for a long time, both in regard to the innovative development of the car itself but also in regard to the manufacturing of the cars (as, e.g., through the introduction of just-in-time production). Important is that this relationship is characterized by a combination of close collaboration between car manufacturers and the suppliers in this value chain, in which however the car manufacturers play the dominant role (as "system leaders") and in which they can exert a lot of pressure on most of the suppliers in regard to quality and prices through the threat of replacing them with others.

It is unclear whether the digital revolution will change the basic characteristics of this relationship between car manufacturers and their suppliers in a profound way or whether the new possibilities of digitalization only intensifies the close collaboration but perhaps also the dependencies and conflicts between the car manufacturer and the suppliers in the value chain75. One important part of this discussion is "smart manufacturing" (or industry 4.0), i.e. to use the possibilities of informationally integrated manufacturing processes along the value chain, for improving efficiency, cutting costs, and achieving a new level of flexibility for producing specifically customized cars. Data can play here a new critical role

74 See the discussion of buying power problems in the car industry in Kerber (1989). For a recent study of these problem from a competition law perspective, see Raeder (2016).

75 There are signs that component suppliers (like Bosch) try to use the connectivity of cars to directly connect with end customers. The Bosch smartphone app “fun2drive” connects via Bluetooth to the OBD adapter of the car. This makes it possible that car functions can be monitored on the smartphone and customers are informed about the nearest Bosch repair service (McKinsey 2014, pp. 16, Bosch 2013).
in smart manufacturing, esp. also the exchange of "real-time" data between the firms within the value chain.\textsuperscript{76} Therefore also the question of data governance within such informationally integrated value chains has emerged in the discussion about data ownership. There were particularly concerns that in value chains that are dominated by large firms (as, e.g., in the automotive industry) smaller firms, esp., SMEs might not get a fair remuneration for "their" data due to "unequal bargaining power" situations. Since in the automotive industry it cannot be denied that asymmetric bargaining situations between car manufacturers and their suppliers can occur, this concern has to be taken seriously also in regard to contractual arrangements in regard to data. Within the value chain of the automotive industry the governance of data, i.e. who is the de facto holder of data, and who has access to which kinds of data, and who can grant access to these data is decided in the negotiations between the car manufacturers and suppliers. However it is only one part of the overall negotiations about prices, quality, quantities, joint R&D projects, and many other aspects of these business relationships. Usually car manufacturers do not have incentives to negotiate data governance solutions within the value chain that are inefficient. Although "unfair" exploitation of "unequal bargaining situations" can occur, there is no economic reason why we should treat "unfair" results in regard to the data component in these negotiations differently from "unfair" results in regard to the price component, because both are part of the same negotiations. If therefore policy-makers like to intervene in regard to the "remuneration" of data in these relationships, then they also have to be prepared to control the negotiated prices. There are good reasons why competition law so far has avoided doing this.\textsuperscript{77}

How does this discussion relate to the data governance problem in regard to the connected car? The crucial point is that a part of the data produced in the connected car is either produced by components of certain suppliers and/or is relevant for certain suppliers, either for diagnostic reasons or for monitoring and improving the components. Data of the connected car can therefore be important inputs for suppliers for improving the quality of the components and for innovation. Therefore access to data for component suppliers is not only a topic for data produced within "smart manufacturing" value chains but also in regard to a part of the data that are produced in connected cars. In the concept of the "extended vehicle" all these data are under de facto control of the car manufacturers and they have a de facto right to decide whether and under what conditions they are willing to provide these data to the component suppliers. In regard to data governance it can be discussed whether the component suppliers should have a right to access data that are produced by the components they supplied to the car, or whether they also should get an access right to other data, which might facilitate developing entirely new components or business models. However, if the market works well in regard to the relationship between car manufacturers and suppliers, then access to these data are again a normal part of the negotiations about the contractual arrangements between the car manufacturers and the suppliers. Also the car manufacturers might be interested in providing the component suppliers with these data for ensuring that the suppliers can improve the quality and have the possibility to innovate. In that case, the question of the access to data from the connected car can be left again (as in the case of

\textsuperscript{76} For "smart manufacturing" and its problems in regard to data ownership and data governance, see Zdanowiecki (2015).

\textsuperscript{77} This does not exclude that a discussion about (minimum) access rights to certain data might be possible.
“smart manufacturing”) to negotiations between car manufacturers and the component suppliers and therefore to private governance solutions based upon contracts.78

3.3.4 Independent repair and maintenance service providers and spare part producers: the aftermarkets

The problem of competition in the aftermarkets in the automotive sector has been an important topic in competition law for decades. If a consumer buys a car of a specific brand, then he will need repair and maintenance services during the lifetime of the car as well as car-specific spare parts. Since the dealers in the distribution systems of the car manufacturers have always provided repair and maintenance services and sold original spare parts to car owners, the car manufacturers have often tried to impede competition through independent repair service providers and spare part producers through a wide range of different business practices. Therefore the car manufacturers can try to tie the sale of cars de facto with the aftermarket services. The problem of competition on aftermarkets is a general problem that exists on many markets for durable products. Particularly well-known is the printer-toner-problem, where the laser printer manufacturers sell their printers at low prices and hope to make profits through the selling of toner at prices that are much higher than the production costs of the toner. The ensuing problem that other firms enter the market with much cheaper toner for those printers has induced the printer manufacturers to search for technical or legal solutions for impeding the usage of this cheaper toner in their printer. However, from a competition economics perspective it is not so clear why this lock-in problem in regard to aftermarket services need to be a problem as long as competition on the markets for printers works well, because it can be assumed that rational consumers would take into account the expected costs of toner when deciding to buy a printer.79 However, the situation is very different, if a printer manufacturer has market power on the printer market. The basic economic reasoning are the same also for aftermarket services in the automotive industry.80 The repair and maintenance services as well as spare parts are usually considerably more expensive than the services and spare parts from independent firms, and therefore there have always been concerns that the car manufacturers have incentives to foreclose the provision of these services and spare parts through independent firms.

In EU competition policy already a long time ago a clear decision was made that competition in the aftermarkets of the automotive industry should be protected, i.e. that independent providers of repair maintenance services as well as spare part producers should be capable to compete with the corresponding services of the car manufacturers. This decision is based upon the expectation that competition through independent firms would lower prices for these services and spare parts (and therefore would also lead to more secure vehicles and lower pollution). In EU competition law the regulation of

78 This does not imply that there cannot be specific situations with “unequal bargaining power”, in which justifications for specific access rights might be possible. In German competition law § 20 GWB about bilateral dependency relations between firms (“relative” market power) might be applicable in such cases.

79 In the competition law discussion this reasoning can be taken into account in the market definition. If consumers choose between entire systems (printer plus toner), then we can also define the market in the same way. See for the discussion about defining system markets in regard to the aftermarkets for repair and maintenance services, Wegner (2010a, 1805).

80 For a summary of economic arguments about the problem of aftermarkets, see Ardiyok (2010).
vertical agreements according to Art. 101 (3) TFEU was used for ensuring that independent repair service providers are not foreclosed from this market. This is one of the reasons why since 1985 an own block exemption regulation for vertical agreements in the automotive industry was introduced and regularly updated. We cannot discuss the specific evolution of this regulation since the 1980s here. However one important tradeoff should be mentioned, because it emerges again in the current discussion about connected cars. The main line of defence of the car manufacturers, why it is important that they should control the provision of repair and maintenance services as well as the provision of spare parts, was that the quality and safety of cars can only be guaranteed if they provide these services and spare parts themselves. Economically, this reasoning might be supported to some extent by the danger of adverse selection due to information asymmetries on the markets for spare parts in regard to the quality of these spare parts. As a consequence, the regulation that protects the supply of aftermarket services and spare parts through independent firms was complemented by a regulation that required the spare part producers to get a certification about the quality of their spare parts, in which also the car manufacturers are involved. It is important that such a certification solution can be seen as a suitable instrument for simultaneously allowing competition for spare parts on the aftermarkets and solving the potential quality and safety problems through information asymmetries. Therefore certification solutions might also play an important role in regard to connected cars.

In regard to competition on the aftermarket for repair and maintenance services the EU has implemented a far-reaching regulatory solution that ensures that independent repair and maintenance service providers can offer their services to the car owners. Partly through the regulations in regard to vertical agreements in competition law and partly through the regulation for the type approval of cars the car manufacturers have obligations to provide access to technical information that is necessary for a range of providers of services in the aftermarkets ("vehicle repair and maintenance information "RMI"). These providers are not only the providers of repair and maintenance services themselves but also manufacturers of spare parts, tools and diagnostic equipment, distributors and wholesalers of these goods, publishers of technical information, technical inspection associations, testing centers and a multitude of adjacent markets. This information has to be given over the internet, using a common format with unrestricted, standardized, simple and immediate access to the information at a non-discriminatory basis, and against reasonable fees. The legal structure of this regulatory approach is complex and not easy to understand. Initially it was part of the Block Exemption Regulation for the automotive sector, then it was mainly included into the Regulation about type approval for vehicles, but it also still plays a role in regard to the exemption of selective distribution systems as part of the gen-

82 See Art. 5 Directive 2007/46/EC.
83 See Art. 6 no. 1 Regulation (EC) No 715/2007 (type approval): "Manufacturers shall provide unrestricted and standardised access to vehicle repair and maintenance information to independent operators through websites using a standardised format in a readily accessible and prompt manner, and in a manner which is non-discriminatory compared to the provision given or access granted to authorised dealers and repairers. With a view to facilitating the achievement of this objective, the information shall be submitted in a consistent manner, initially in accordance with the technical requirements of the OASIS format. Manufacturers shall also make training material available to independent operators and authorised dealers and repairers."
eral Block Exemption Regulation of vertical agreements. In 2014, the EU Commission published a study on the operation of the system of access to vehicle repair and maintenance information (EC 2014), which analyzed the experiences and problems with this access regulation. Although a number of difficulties and problems could be identified (e.g., in regard to intransparency of fees etc.), the overall assessment led to the conclusion that this system of access to technical information for allowing the provision of repair and maintenance services for vehicles and for protecting competition of these aftermarket services works well and would only need minor improvements (esp. in form of clarifications of the specific rules) (EC 2014, 5-10).

Important for our analysis is that this regulation for access to technical information already can be interpreted as a regulation for giving access rights to information to a certain set of firms for maintaining competition in the aftermarket of cars. Since part of this information are also data from the on-board diagnostic systems (OBD), this regulation also encompasses already mandatory access rights to data in the vehicle that are relevant for repair and maintenance services. In the current general discussion about access rights to data in regard to IoT-applications this already existing regulated access to data for repair and maintenance services therefore has been seen as a potential model for a more general regulation of access to data for data-producing devices in the IoT. Important is that this regulation of mandatory access to data does not require the existence of market dominance according to Art. 102 TFEU. This example of a regulated access to information and data is also interesting, because the experiences with this regulated access, as they can be found in the study of the EU Commission (EC 2014), might also be instructive and helpful for designing other regulatory solutions for access to data. Especially interesting here are questions about the clear definition of the information, how this should be provided, and how the rules for fees should look like. However, it also should be taken into account that this regulated access to information and data for aftermarket services does exist in the EU only in regard to the motor vehicle sector, and is therefore a sector-specific exception.

The interesting question now is what will change in regard to this regulation through the transition to connected cars. The discussion about data in connected cars so far seems to be characterized by a large (political) consensus that competition through independent repair and maintenance services and spare part producers should also be protected in connected cars, i.e., that these independent firms should have access to the relevant information and data also in the future, even if the technical solutions about data and data transfers, e.g. in the extended vehicle concept, might look very differently from today. However in regard to the scope of data that should be made accessible there is an open conflict between the car manufacturers and many independent providers of services, esp. independent

---


86 See, e.g., also the Commission in EC (2017b, 38).

87 See C-ITS Platform (2016, p. 72) and EC (2017c, pp. 23 ff.).
repair services. On the one hand, the car manufacturers accept that based upon the current regulation of the automotive aftermarkets independent operators and service providers should have access to certain kinds of data but they insist to “define the data needs of third parties on the basis of specific use cases, i.e. when it is clear which data are requested for which purpose by which party” (C-ITS Platform 2016, 87). This implies that these data access rights should be narrowly defined, and only for specific purposes and for specific parties. Of course, the car manufacturers would be willing to provide also access to other data, but only on a purely negotiated basis, i.e., that they can freely decide to whom and under what conditions (esp. also prices) they provide access to these data. This implies that they can control the markets for those products and services which need these data as a necessary input. The independent operators and service providers, on the other hand, argue that "purely a use case based release of data would seriously restrict services and innovation". They would like to have broader access to data "which would allow for the flexibility needed as regards innovation of new use cases." (C-ITS Platform 2016, 88). From a competition perspective the decisive point is that the scope of regulated access, i.e. who has a right to access to what kinds of data for what kinds of purposes also determines the scope of products and services, for which the car manufacturers cannot foreclose competition through refusing access to certain kinds of data as a necessary input or control this competition by determining the conditions under which the firms in these markets can get access to these data.

It is clear that the transition from traditional cars to connected cars will change the technological conditions for the relationship between car manufacturers and independent repair and maintenance service providers significantly. One problem is that the set of automotive services and products in the aftermarkets will change in any case and therefore new definitions of the kinds of data to which these firms have regulated access are necessary. Therefore the rules about access to information have to be adapted in any way in this transition process to connected cars. Whether this requires - from a legal perspective - new regulations or "only" an adaptation in form of a redefinition of the necessary information is one of the questions that have to be answered. However the decisive open policy question is whether independent providers of repair and maintenance services should also have broader access rights to the data of the car manufacturers that would allow them to develop, in an innovative way, also additional new services and products for the owners of cars or whether these data access rights should be defined narrowly as proposed by the car manufacturers. Another policy solution which the independent service providers would prefer is that a technical model for the connected car is chosen, as, e.g. the on-board application platform or a neutral shared server solution, that would not give the car manufacturers an exclusive de facto control of the data in the connected car in the first place. If the independent service providers could get the necessary data directly, e.g. from the car owners, then this possibility of the car manufacturers for foreclosing competition on the aftermarkets through denying access to these data would not exist and therefore not lead to a need for a regulated mandatory access. Therefore this competition problem is one of the main issues behind the entire discussion about the advantages and problems of the three technical models "central server platform" (extended vehicle), "in-vehicle interface", and "on-board application platform" (EC 2017c).

88 This was one of the major and non-resolvable conflicts in the C-ITS process of finding common principles among the different stakeholders for connected cars; see the chapter about Working Group 6 in C-ITS Platform (2016, 78-89).
However the question of access to data of the connected car for providing new products and services is not limited to the component suppliers (section 3.3.3) and independent repair and maintenance services (section 3.3.4) but also can be asked with very similar economic reasoning for many more providers of products and services that need access to certain data of the connected cars (or need access to the IT-system of the car) for offering these services to the car owners, car drivers and/or the passengers of the car (see the next sections 3.3.5 and 3.3.6).

3.3.5 Insurance companies

Car insurance is provided to a large extent by (often) large independent insurance companies, although also the car manufacturers increasingly offer their own car insurances. So far insurance companies have a number of possibilities to differentiate premiums by using a number of criteria for classifying car owners in different risk classes. This might be types of car, regions, age, the driven kilometers per year, and especially also the individual history of insurance claims (and many more). The basic idea is that these criteria allow for a more or less good classification of those who drive the car in regard to the risk of causing an accident, on which basis the insurance companies can pool similar risks and offer risk-equivalent insurances (with premiums that correspond to these specific risks). The transition to connected cars with its huge amount of produced data can have several effects on car insurance: (1) Through the new "Advanced Driving Assistance Systems", as, e.g., lane departure warning, forward collision warning, park assist systems, blind spot information, driver monitoring etc., a general considerable reduction of car accidents is expected. These are one of the huge benefits of connected driving and also will lead to a long-term general reduction of insurance premiums. (2) But more important for the insurance model is that the data of the connected car allow for a direct monitoring of the driving behavior of the car drivers, and therefore for a much better assessment of the specific accident risks (as well as higher incentives to drive cautiously). This does not only encompass the driving behavior (speed etc.) itself, but also on what roads, when and how much the car is driven, because also this influences the probability of accidents independent from the driving qualities of the car driver. Therefore these data allow for a much better risk classification, leading to a higher equivalence of individual risks and premiums on the insurance markets. These possibilities allow the inclusion of "driving behavior" (through driver monitoring) as additional criteria in the insurance policies but also the development of entirely new types of car insurance as, e.g., Used-based Insurance (UBI). (3) Another important development is that the market position of traditional insurance companies is threatened through new competitors. This can be, on the one hand, tech companies with their specific digital competence, and, on the other hand, car manufacturers who might get advantages through the possible exclusive de facto-ownership of the data of the connected car, which also would encompass

---

89 An additional effect is that the combination of the data of connected cars with other real-time data, as, e.g., data about weather and road conditions, can also help to reduce the probability of accidents, because drivers can be warned in real time in the car about dangerous conditions. Depending on the extent of ADAS adoption an accident reduction rate between 11% (on other roads with Basic ADAS) and 45% (on motorways and Advanced ADAS) is expected until 2020. See HERE/Swiss Re (2016, 15).

90 By comparing the behavior of many drivers on the same roads and under different weather conditions etc., the insurers have many possibilities to identify the different risk levels of different drivers. For this "context-aware vehicle behavior analytics (VBA)" see HERE/Reswiss (2016, 22-24).

91 See for the new insurance schemes HERE/Reswiss (2016, 18).
data about driving behavior. From that perspective, it is not surprising that also the insurance companies are very concerned about an exclusive de facto data ownership of the car manufacturers.

What kinds of market failure problems can arise in regard to car insurance and data of the connected cars? Two different problems can be distinguished. One refers to the question of access to data for insurance companies in the relation to car manufacturers as the presumptive de facto holders of these data. However, more important is that nearly all of the data which are so interesting for insurance companies are personal data of the car owners, esp. about their driving behavior. Therefore it is clear that using these data for the purpose of car insurance requires the consent of the car owners. However, if the insurance companies offer lower premiums for insurance with such a personal data transfer about driving behavior, it can be expected that many car owners will accept such offers, and therefore make these kinds of personal data available to the insurance companies, although this might have effects on their privacy. In that respect, car owners "sell" part of their privacy in exchange for a lower insurance premium. There is some discussion whether such a development might be a problem. One of the arguments is that offering such kinds of insurance schemes can lead to an "unraveling" of insurances, i.e. that if more car owners accept such an insurance, then also other car owners might increasingly be de facto forced to do this. The reason is, if the low risk car owners choose these new insurance schemes, then the insurance companies will have to increase the premiums for those who do not want to reveal this information (and are therefore presumed as being drivers with higher risks), leading to the consequences that the "solidarity" function of insurances might not work anymore and that privacy protection might be compromised. From an economic perspective, the evolution to more premium differentiation according to the individual risks is not a problem; rather it increases the efficiency of the car insurance market through less adverse selection and moral hazard problems (which are caused by information asymmetry between the insured drivers and the insurance companies). It is true that this will lead to less de facto redistribution between low risk and high risk drivers through the insurance, but in regard to car insurance it was never a public policy objective that the low risk drivers should subsidize the high risk drivers (in contrast to other kinds of insurances, as health insurance that also have an explicit social policy objective). Therefore this "unraveling" of the car insurance through using more direct data about driving behavior increases the efficiency of the car insurance market and improves the incentives for car owners to drive carefully (and only letting other careful drivers use this car). In that respect, it can be expected that this also would lead to a further reduction of car accidents and therefore improve traffic safety.

Much more important as a potential market failure problem is the privacy issue: We already have seen in section 2 that there is a huge discussion about the question whether individual persons are capable of making rational and well-informed decisions about their privacy. Therefore the question can be discussed whether the car owners - due to information and behavioral problems - might be lured too easily to give up their privacy in regard to their driving behavior for perhaps relatively small reductions of their insurance premiums without taking into account the long-term consequences of this decision. However, this also depends on the question how the insurance companies are using these data and

---

92 In an economically efficient insurance market the insurance would still lead to redistribution between those with and without accidents, but this redistribution would only be between individuals with the same risk level.
how transparent they are about this.\textsuperscript{93} This refers to the question whether car owners can make rational, well-informed decisions about their own individual trade off between protecting their privacy and the monetary benefits of lower insurance premiums.\textsuperscript{94} From the (data protection supervisor's) perspective of protecting privacy as a fundamental value (!), however, it also can be asked whether privacy should be more protected, and that therefore the "selling" of such personal data (driving behavior, location etc.) through the individual car owners should be allowed only under much more restrictive conditions.\textsuperscript{95}

The discussion above only referred to the relationship between the car owners and the car insurance companies without taking into account the role of the car manufacturers. This would be sufficient, if the car owners can easily control whom they are granting access to their personal data (as, e.g., in a future on-board application platform). If, however, the data about the driving behavior are under the de facto control of the car manufacturers, and they are getting a general consent of the car owners using these data also for this purpose, then the car manufacturers play an important own role. One question is whether the car owners can get these data from the car manufacturers for reveling them to their insurance company. Data protection law and especially the right on data portability should give the car owners sufficient legal rights for achieving this (at least in the EU). This does not exclude that there might be a lot of problems and costs in implementing this. This cannot be discussed here in more detail. However, one specific potential competition problem should be mentioned here. Since the car manufacturers, in any case, make contracts with the car owner about connected driving and about the consent to use personal data, the car manufacturers can very easily bundle their connected car services with the offer of an own car insurance, and get a rather broad consent of car owners for using their personal data (and also data about their driving behavior). Therefore, such an exclusive de facto ownership of data (about the driving behavior) might give the car manufacturers (technically supported in an "extended vehicle" model) the control about an important input resource for making more competitive insurance schemes, and therefore a competitive advantage in comparison to the traditional insurance companies without such a direct access to these data. From a competition perspective, it can be asked whether such a position might allow the car manufacturers to distort competition on the car insurance markets and foreclose insurance companies from this market for complementary (after-market) services. The potential problem might again be that car manufacturers claim high prices for these data (which would lead to higher insurance premiums for the car owners), or that they can control the access to this market (e.g., for making exclusive agreements with insurance companies) or try to retain the market for themselves (by not making these data available to others).

\textsuperscript{93} In that respect, it is again possible talking about regulatory requirements as, e.g., transparency about use of these data etc. One interesting question is, for example, whether these insurance companies can use these data about driving behavior also for other kinds of insurances (in-house), in which psychological traits about cautiousness of the insured persons are important, or whether this is not allowed.

\textsuperscript{94} For an interesting empirical (experimental) study about the behavior of car owners in regard to the tradeoff between privacy and lower insurance premiums (with also much more literature) see Derix et al (2016). The results of this study also support the thesis that individuals often differentiate between different aspects of privacy (e.g., driving behavior, location) in these decisions.

\textsuperscript{95} This would imply that individual decision-making according to individual preferences should not be always respected. A deeper analysis would presumably show that this might lead to tradeoffs between privacy as a fundamental value and economic welfare but this need not necessarily be the case (e.g., if individual privacy decisions lead to externalities).
These potential problems, can, on the one hand, be used for raising the question whether insurance companies should have an access right to such data (with the consent of the car owners due to the personal character of these data); however, on the other hand, the question can be asked whether these problems can be solved better by strengthening the rights of car owners, esp. in regard to the portability of these data. But this example shows that also the basic question what kind of technical architecture for connected driving (central server platform with the options extended vehicle or neutral server platform or the on-board application platform etc.) should be chosen might have again a huge impact on this competition problem.96

3.3.6 Other independent service providers

There exists a very heterogeneous group of stakeholders which can offer a variety of other services in the connected car. Firstly, we can distinguish stakeholders which offer mobility services. These include travel services (e.g. hotels, flights, trains), car sharing or rental and in the future potentially services like robo-taxis. Secondly, there are diverse other service providers in areas like advertising, health, education, fintech, communication (social media), commerce, payment and content provision (music, video) (PwC 2016, p. 15.). These stakeholders have in common that their services and business models either depend or can be improved through accessing data of the connected car. If, for example, a third party provider wants to offer a hotel reservation system for the connected car, it probably will need access to location data, access to microphones in the car (in case the car driver wants to call the hotel), access to information about the car and passengers (to take into account available rooms and parking space) and a connection to the internet (to make the reservation). Similarly, payment systems for the connected car (e.g. for road toll, gas stations, parking) will likely require internet access, access to car data (e.g. to calculate fees), access to the purchase history, location data and user profiles (including bank information). Such kinds of services not only require access to data but also a way to directly connect with the car driver, hence being integrated in the IT-system of the car. This means that compatible services and applications for connected cars have to be presented (in some form) to the car driver. This could be similar to smartphones where apps are provided through an application store. The heterogeneous group of other service providers would profit to a large extent or even require such a distribution platform.

The main problem from a market failure perspective is whether access to data for these different stakeholders is possible and broad enough to enable competition and innovation. This problem is much related to competition and access problems on aftermarkets for independent repair services which have been addressed by regulatory solutions in the EU (see section 3.3.4). Today, car manufacturers have their own infotainment systems and offer mobility services. As outlined above, they are interested in long-term relationships with the car owner which might also be based on services and apps offered for their connected car. In the "extended vehicle" concept car manufacturers control the access to data and the access to the IT-system of the car. This means, they have the ability to fore-

96 Other questions that have not been addressed in this section are the issue of the use of anonymised personal data about driving behavior, e.g., also for public policy objectives (as traffic safety), and, in relation to that, the question of "data aggregation" for better data analytics in regard to car insurance and in regard to traffic safety and regulation.
close aftermarket service providers or pursue other forms of discriminatory conduct. This includes pre-installing apps on their connected car and/or making it difficult to install competing apps, exclusive contracting or price discrimination. From a competition policy perspective the question is, whether vertically integrated car manufacturers (which also offer these other connected car services) really have an incentive to foreclose. The result of foreclosure could be less competition (or even a monopoly), higher prices and less innovation on these aftermarkets.

On first sight, this problem seems to be rather similar to the closed system of Apple on their iPhone, which does not allow using the iPhone with other distribution platforms or apps than those which are approved and admitted by Apple. The app developers have to pay a price to Apple and share their revenues in order to be capable of offering their app services. In case of the connected car, the incentive to foreclose likely depends on competition on the market for connected cars. If the connected car market is competitive, the problem of foreclosure or discriminatory conduct might be mitigated. If available apps and aftermarket services are part of an ecosystem of the connected car and the market for connected cars is sufficiently competitive, car manufacturers have a large incentive to encourage or even subsidize service providers to be present on their platform. Alternative models to the “extended vehicle” concept (as the on-board application platform) would allow for more direct communication of the service providers with the car owners and their passengers without establishing a monopolistic bottleneck that controls both sides of the market. Another very important question in this regard is also to what extent it is technically possible (or should be even required by regulation) that in the car itself a parallel system of mobile access can be implemented or used that would allow some competition with the integrated mobile system of the connected car. Taking into account the vast potential of products, apps and services which could be developed for the aftermarket of the connected car, encouraging innovation requires levels of data access and direct communication with car drivers which should be rather broadly than narrowly defined.

### 3.3.7 Public authorities

Data from the connected car can also be very important for a number of different public authorities. Most important are certainly real-time data about the location of cars and traffic flows on roads for traffic regulation (esp. avoidance of congestion) which would allow the optimisation of traffic management systems (including management of parking capacities). However data from connected cars can be used by public authorities for a number of different tasks. These tasks can encompass, e.g., road maintenance, and measures for solving environmental problems (e.g., through car emissions). They can also be used for a better planning of integrated traffic systems of entire cities and regions. In

---

97 So far competition policy has accepted such a behavior in regard to Apple, mostly because there is still competition between the manufacturers of smartphones.
98 This means facilitating access to data and giving service providers a distribution platform.
99 Also already the normal smartphones of car passengers do allow for an alternative form of access, at least to the car passengers, and limit to some extent the “monopolistic” control of the car manufacturers in the “extended vehicle” concept.
100 This would also be an argument for implementation of access depending on terms and conditions of each application and not depending on specified use cases (EC 2017c, pp. 30).
101 This example is also explicitly mentioned by the Commission in its Communication (EC 2017a, 12).
that respect they also can contribute to the different policy issues that are addressed under the heading "smart cities". These data might also be very interesting for dealing with criminal behavior, either for prevention or for prosecuting criminals. Many of the data can also be interesting for scientific research, e.g., data about the behavior of drivers (attention, fatigue, etc.), which can help to develop policies about improvements of traffic safety etc. But these data also might be interesting for many different kinds of economic, sociological, medical, and technical research, as well as for public statistical offices which provide statistics about different aspects of traffic and transport.

In the Communication "Building a European data economy", the Commission discusses the option that public authorities can get access to privately held data in the "general interest". At least for certain kinds of data of the connected cars it might be well justified that certain public authorities can get access to these data. The interesting question is more which public authorities should get access to which kinds of data (and in what specific or aggregated form), whether the de facto holders of these data have to give access with or without remuneration (and whether a fee should only cover the costs of the access or can also be higher), and whether and to what extent the public authorities can give other public or private parties access to these data, or that these are even put online and anybody can use them for free (as, e.g., statistical data published by statistical offices). Since there is a broad consensus that traffic management and traffic safety are important public policy objectives, there are strong arguments, also from an economic perspective, that public authorities should have far-reaching rights to those data they need for achieving their public interest objectives. However, from an economic perspective, also the question of incentives for data production, the protecting of business secrets (and privacy), as well as the costs for providing access to these data have to be taken into account for any policy solutions in that respect.102

3.4 Market failures and regulatory problems: a preliminary analysis

Based upon our separate analyses of potential market failure and regulatory problems this section has the task of offering a preliminary comprehensive analysis of such problems in regard to data governance in the context of connected cars. It will be a combination of a summary of the most important results in section 3.3 and an analysis of additional important questions that so far have not been discussed.

Market failures: Competition/innovation, information/behavioral, and privacy problems

One specific field of potential problems refers to the car market itself and the contractual relations between car owners and car manufacturers. In that respect, we have identified two main issues: The first one is to what extent we can expect that in regard to data the same problems, esp. in regard to privacy, emerge as in regard to the provision of data for free services in the internet, namely that con-

---

102 Independent from these "public interest" justifications, mandatory access to data of connected cars can also be very important in litigation before courts (data as evidence), e.g., in litigation about damages in car accidents (between car owners or their insurance companies) as well as litigation about defects of cars (between car owners and car manufacturers or repair service providers). In those and other cases, it might be important that plaintiffs and/or defendants have a right that relevant data are disclosed for settling disputes.
sumers are too generous in regard to providing their data, because they are not aware enough of the value of their data, or are too careless - due to behavioral problems - about their data, and/or the firms do not give enough information about the extent and the further use of the data they produced. Therefore "notice and consent" solutions might not work well enough. This is relevant both for personal and non-personal data. One part of the problem is also that car manufacturers might not offer enough choice for making granular decisions what specific kinds of data the car owners want to provide to whom and for what purposes. It is not clear whether competition on the car market will lead to enough differentiation in regard to the offered privacy options for car owners (and to enough transparency in their privacy policies) for allowing them to fulfill their specific privacy preferences. Therefore one issue focusses on privacy concerns and the fulfillment of privacy preferences of car owners. This is a crucial problem, because failures in this regard in the contracts between car manufacturers and car owners have many further consequences, because these data will be used and reused by perhaps many firms through data licensing and data trading.

This first main issue is directly linked to the second main issue, which refers to the question how well competition works between car manufacturers. Although nobody claims that there are dominant firms in the car market, in most geographical markets we have oligopolistic market structures that might lead to considerable market power in certain market segments as well as collusive behavior. Especially interesting are the recently emerged allegations that (German) car manufacturers might have colluded in regard to technical features, because such forms of collusion might also play a role in decisions about technical solutions in regard to connected cars.\footnote{It can be asked whether an agreement between car manufacturers upon the "extended vehicle" concept and additional technical details are in itself an anticompetitive agreement, because it might limit competition between different technical systems and therefore also between different de facto data governance solutions.} The other interesting topic in regard to competition between car manufacturers is to what extent this competition leads to a remuneration of the (personal and non-personal) data provided by the car owners, either through direct payments, additional "free" services or lower car prices. This is an important topic for future research that also fits into the general question, who is getting the benefits of the valuable data that are produced in connected cars. In addition to that, the already existing lock-in problems of a typical valuable durable product as a car in regard to aftermarket services will be amplified through additional potential lock-in problems through the need of permanent communication and (car) -IT-services (including updates) for the connected car. The consequences of these additional lock-in problems, based on this long-term relationship between the car manufacturer and the car owner, also need more research.

The second field of potential problems is competition and innovation in regard to repair and maintenance services in the aftermarket and in regard to additional services from other service providers. From the perspective of data governance, it is very interesting that we already have a regulation about rights to access to information that is necessary for providing repair and maintenance services. This access regulation has been established explicitly as a solution for competition problems. In the current discussion about data governance in connected cars there is a clear consensus that access to necessary data for repair and maintenance services should also be given in the case of connected cars. However we have seen that the interesting policy question is whether the scope of data to which regulated access is granted should be defined much broader or remain narrow. A first economic analysis
would suggest that granting broader access to these data would open up the opportunities for competition and innovation in regard to more services and products, esp. allowing these independent aftermarket service providers to develop more easily new services and products. However, the same economic reasonings can also be applied to the question whether many other service providers who want to offer complementary or additional services for connected driving to the car owners (and car passengers) should have a right to access certain kinds of data that are produced in the connected car and/or get access to the IT-system of the car for the possibility of direct communication with the car owners (or drivers). In regard to the economic effects on competition and innovation there are no large differences, whether these are traditional repair and maintenance service providers, insurance companies, or other service providers. In all these cases, it can be argued in the same way that providing more and/or easier access to the in-vehicle data and resources might allow for more competition and innovation.

However, we also should take into account that there might be other effects, which might justify a more restrictive approach. One possibility is that either the car manufacturers and/or the car owners can get revenues for these data by selling access, which would increase profits and/or reduce the costs of connected driving. The other possibility is that restrictions to access might also be necessary for ensuring safety and security. Both aspects will be discussed in more detail below. But both aspects also refer to the question of the conditions for access, both in regard to prices, discrimination, and technical and other criteria. Important is that the legal or de facto exclusive control about certain types of data that are essential for the provision of certain services in the car allows this data holder to set high access prices as well as decide freely whether and to whom access is granted (and under what conditions). Therefore other firms can be foreclosed in regard to entering this market. However, from an economic perspective, it still can be asked whether this harms consumers, if there is still effective competition between car manufacturers on the market for cars.

**Safety and security issues**

One of the crucial problems in the entire discussion about connected cars is the question how the security of the IT-system (including the data) and the safety of connected driving can be ensured. In the discussion about the "extended vehicle" concept it is the main argument of the car manufacturers that security and safety can only be achieved if the car manufacturers have full control of the entire IT-system, all the data, and all the (mobile) access to the connected car.104 Whether this is true or not is a technical question that has to be clarified by technical and IT experts. In the literature this question is discussed controversially. The most recent EU study (EC 2017c) about "access to in-vehicle data and resources", which also analyzed deeply the technical issues about safety and security, the authors came to the conclusion that the safety and security issues are solvable for all three technical models, although the "in-vehicle interface" and "on-board application platform" might lead to more problems and therefore higher costs (EC 2017c, 12). From an economic perspective the question is to what extent it is necessary that the firm which is responsible technically for the safety and security of the IT-system of the car has to have simultaneously also the de facto rights to sell the access to the in-

---

104 See ACEA (2016a).
vehicle data and resources of the connected car. Safety and security concerns might justify that the firm responsible for the safety and security of the car has full control about who can get access to the system ("read" and/or "write" data) from the perspective of interoperability and the fulfilment of minimum requirements in regard to safety and security (e.g., in regard to apps). This can also imply that it has to be authorised to bar anybody from the access to the connected car, whose data or apps are not tested, e.g., in a certification process, in regard to compatibility, safety, and privacy concerns. However, such a function does not imply at all that the same firm also has to have the right to make the business decisions about who gets access to the data of the connected car (and under what conditions, esp. prices) or gets access to the HMI (human-machine-interface) for communicating with the car drivers (and passengers). It is not clear why the technical questions of compatibility, safety and security should not be separable from the economic questions about the legal or de facto rights on data, i.e. who can use the data for what purposes, and under what conditions. In regard to personal data these rights are initially, in any case, "owned" by the car owners/drivers, and this can also be the case for non-personal (and anonymised) data.\textsuperscript{105} Therefore the decisive question is the technical separability of different functions and processes in the connected car. One important aspect is the technical separability of the running of safety- and security-critical processes from other processes, e.g., by using hypervisor-technologies.\textsuperscript{106} An additional but closely related question is whether it is (or should be) possible to run also a parallel mobile communication system in the connected car.\textsuperscript{107} All of these technical questions have to be clarified to a larger extent.\textsuperscript{108} However, from an economic perspective, narrowing down the exclusive control of access to data and resources of the connected car would open up the possibility of more competition and innovation in regard to products and services that can be offered to the car owners and car passengers in connected driving. From a policy perspective, this problem has close similarities to the well-known problem of monopolistic bottlenecks and the policy strategies of narrowing down these bottlenecks as far as possible in order to allow for more competition and innovation.

**New exclusive rights on in-vehicle data for connected cars?**

So far we have not discussed the problem whether the current legal situation that no property rights exist for non-personal (or anonymised) data does lead to market failure problems and whether in re-

\textsuperscript{105} Even if it seems necessary that certain kinds of data and functionalities that are critical for safety and security should be in the sole control of car manufacturers (to prevent unauthorized tampering with such critical infrastructure by car owners or other service providers), then also such a safety requirement would not necessitate that the car manufacturers need the rights to commercialize these data or all the other data which are not relevant for security and safety. It is not even clear whether car manufacturers should provide and run the IT-system in the car and should be responsible for the security and safety of the IT-system.

\textsuperscript{106} *A hypervisor manages the separate execution of software tasks: in this context allowing the management of messages to vehicle ECUs and the prevention of unauthorised access to safety-critical ECUs or to functions that are not authorised for the application* (EC 2017c, 9, fn.5); see for more technical details EC (2017c, 77).

\textsuperscript{107} This would allow at least some degree of "multi-homing".

\textsuperscript{108} These questions are also linked to the problem of liability. In regard to the technical aspects another important issue is interoperability and standardization, which is also a difficult problem that has to be solved in regard to connected driving.
gard to the data of connected driving exclusive property rights (as, e.g., the "data producer right" as suggested in the Communication "Building a European data economy") should be introduced for solving problems in regard to rights on data. This question is important, because the proposal of a "data producer right" has been made specifically for the many data that are produced by IoT-devices (EC 2017a, 13). In section 2.2, we discussed what kind of questions should be asked in this respect from an economic perspective. First and most important is the question whether there are incentive problems for the production of data in connected cars. At first sight, it cannot be seen that car manufacturers have incentive problems for sensor data in regard to "assistant systems" or other functionalities, because if consumers prefer connected cars with these functionalities, then they are also willing to pay higher prices. So far there are also no indications that there is a (much larger) copying problem of data of the connected cars than for other machine-generated non-personal data, or that the granting of access to data, esp. also the selling of (anonymised) data to other service providers or on data marketplaces would lead to much more serious transaction problems than for other data (problem of trading data). On the contrary, it can be presumed that data from connected cars are much more easily definable standardized data, and that therefore the problems of information asymmetry in regard to the quality and provenance of data might be considerably smaller than in regard to many other data that can be offered on data markets. The problems and possibilities of monitoring the compliance of buyers of data with the conditions of the contracts about the authorized use of data, e.g. also through technical restrictions, do presumably not differ much from other types of data. Since we have seen in section 2 that the allocation of a specific exclusive data right, e.g., to the car owner in regard to the non-personal data of the car, would not help to solve market failure problems through market power and through information and behavioral problems, such an exclusive right also would not achieve a potential distributional objective that the car owners should get the benefits of the data of the connected car, because such a right would be contracted away in the contracts between the car manufacturers and the car owners. Therefore a first preliminary analysis does not support the view that there is a need for protecting non-personal (or anonymised) data in connected cars with a new exclusive property right (as the proposed data producer right).

3.5 Alternative data governance regimes for connected cars: Some perspectives

This article has only an explorative character, is still "work in progress", and therefore does not claim to provide a comprehensive analysis of the data governance problems in connected cars from an economic perspective. We have identified some potential market failure problems in regard to data in

---

109 This is also a consequence that "connected driving" will require a far-reaching standardization of (the definition and quality) of data.

110 However, it cannot be excluded that a deeper analysis that also encompasses externalities of the production and use of data and other aspects, as, e.g., the data aggregation problem, might lead to more differentiated results in regard to the incentive problem. For example, it could be that from a public interest perspective (as traffic regulation or road maintenance), certain kinds of data should be produced in the connected cars, for which neither the car manufacturers nor the car owners have sufficient incentives to cover the costs for additional sensors. But this question also raises the important economic question, what data and how many should be produced in the car, and whether there are optimal incentives for producing additional data for specific purposes.
connected cars, but we do neither claim that all of them are really market failure problems nor that we have identified all potential market failure problems. We also did not try to analyze the specific effects that emerge through the simultaneous existence of several of these market failure problems in this connected driving context. We also did not analyze all aspects that might be relevant from the perspective of our theoretical framework for the analysis of data governance in IoT-contexts in section 2.2. However, all of these questions should be clarified in future economic research, which should consist both of theoretical and empirical studies, both from an "industrial economics" and a "law and economics" perspective. Particularly important is interdisciplinary research between lawyers and economists. In this article we already tried to include in our analysis also the legal questions and discussions. This is not only important due to the relevance of the law, esp. data protection law, but also because so far the lawyers are far ahead in their discussions of data governance problems compared to the economists. For such an interdisciplinary research a number of research questions would be particularly interesting. One of the most interesting projects would be an empirical study about the already existing contractual relationships between the different stakeholders in regard to the data of connected driving. This would focus primarily on the contracts between the car manufacturers and the owners of connected cars (esp. in regard to personal data), but also the contracts between the car manufacturers and other stakeholders as component suppliers, insurance companies, and others would be very interesting. This would also be linked to an analysis of the strategies (and strategic alliances) of car manufacturers, e.g., also in regard to collaborations with the large tech companies as Google or Apple.111

What is also missing in our study is the long-term perspective of the step-by-step evolution from traditional cars to connected cars to autonomous cars, because this transition also will have far-reaching consequences for the question of appropriate data governance regimes in regard to "mobility data". If it is true that in a world of autonomous driving it might not be interesting any more that private persons own cars themselves but can use autonomous cars similarly to cabs today, then the structure of stakeholders and the markets between them might look very differently as well as the appropriate data governance regime. However, this future might still be far away, and therefore the question of an appropriate data governance solution for a world with a large share of connected (but still privately owned) cars will be relevant for the next one or two decades.

This article has not had the objective to discuss explicitly policy options or even make own policy recommendations. As can be seen very well in the most recent study of the EU (EC 2017c), the discussion so far focusses mostly on the question what kind of technical model of "access to in-vehicle data and resources" (data server platform with different variants, in-vehicle interface, or on-board-application platform) should be favored. The EU study tried to analyze, whether all three technical models are legally and technically feasible (also in regard to safety, security, and privacy concerns), and came to the conclusion that this is the case (although with different advantages and problems for the different models; EC 2017c, 11). In an additional step of the analysis, the study tried to assess these three models by using the normative benchmark of the five principles of the C-ITS platform (see section 3.2) and developing different policy scenarios. Especially the competition problems (principle (b)) have led them to the conclusion that, in the long-term (under "scenario 3") the "on-board-

111 See for a very interesting overview of the manifold strategies of different car manufacturers in that respect EC (2017c, 67-72).
application platform” might be the superior technical model (EC 2017c, 16). However, the study could only make qualitative assessments, and has focused its analysis rather narrowly on these three technical models and these five principles. It, particularly, did not analyze in a broader way market failure problems and the overall governance problem of data of connected cars from an economic perspective. What is missing in this analysis are the potential market failure problems in regard to competition between car manufacturers and information/behavioral problems of car owners in regard to data/privacy decisions in their contracts with car manufacturers as well as the general question of the proper data governance regime for the data of connected cars (including the question how the benefits of these data are shared).

An explicit policy discussion about data governance in connected car is beyond the objectives of this paper. But, in the following, some basic perspectives about possible data governance regimes for the data of connected cars are outlined, which also look beyond the above discussion about these three different technical models. There can be no doubt that the future data governance regime for data of connected cars will be complex and consist of a combination of rights of different stakeholders in regard to these data. Very important is that it will be necessary to differentiate clearly between different types of data, due to legal, technical, and economic reasons. Therefore the appropriate sets of rights might be very different for different types of data. Especially privacy protection and therefore the rights of car owners (car drivers and passengers) will play an important role. The access to certain kinds of data for safeguarding competition of independent repair and maintenance service providers will presumably also play a role in the future. Also public authorities will have rights to access certain data justified by public interest rationales. But the open questions are how far-reaching all of these rights from these stakeholders will be, who has the legal and/or de facto control about the huge sets of data that are produced in connected cars, who can decide who has access to them, and under what conditions, and under what regulatory conditions contracts (about data) can be made between car owners and car manufacturers.

For the economic and legal analysis (as well as the political discussion) it might be helpful to distinguish the following three different basic perspectives on the issue of “ownership” and governance of data in connected driving:

(1) The first one is based upon the most clearly developed concept right now, and this is the solution that all data are transferred and controlled on a central server outside of the car, with either the car manufacturer (“extended vehicle concept”) or a consortium of stakeholders (“neutral shared server”) as the exclusive de facto holder (and therefore the de facto “owner”) of the data. They would control all the data and access to the connected car in a similar way as Apple with its iOS operating system. Such an “exclusive” position might lead to a lot of problems for competition and innovation for additional products and services offered in the connected car. The question is to what extent competition between car manufacturers and the contracts between them and the car owners (about “consent” in regard to personal data) limit the exclusivity of the control about these data, or whether a number of additional regulatory remedies, e.g., in regard to access rights and/or requirements about non-

112 For the difficulties of getting information about the costs of different solutions see EC (2017c, 254).
113 Therefore one part of the already existing discussion are classifications and definitions of in-vehicle data.
discrimination of access to data, and/or fair and reasonable fees for these data, are viewed as necessary for ensuring a more acceptable regime of data governance.

(2) In another alternative approach it would be the car owners who are the stakeholders who have exclusive legal and/or de facto control about the data of their cars, and who decide where the data should be stored (e.g., also at an external server as a service provider), which data should be made available to whom and under what conditions (including as counterperformance for money of services). This approach could be combined with the concept of personal information management systems (PIMS) that should help the car owners managing their privacy but also making prudent decisions about access/commercialisation of their personal and non-personal data. This could also encompass the commercialisation (or the "donation" of an "anonymised" version of their personal data). It can be expected that in this approach it might be necessary to limit the exclusive control of car owners through certain minimum access rights for other stakeholders, e.g., here the car manufacturers and public authorities. It might also be that certain (technical) data in regard to the car might be protected as trade secrets and therefore not under the control of car owners.114

(3) However, it might also be helpful to look at the governance problem from a third perspective. Whereas it still would respect privacy protection as well as the protection of certain data as business secrets for car manufacturers (and component suppliers), the basic approach would be to apply an open data approach to the huge mass of data of the connected car, i.e. as far as there are no other specifically defined rights of stakeholders, all these data could be made freely accessible (or for a small fee for covering the costs of running a secure and safe data governance system) in a non-discriminatory way. The basic economic idea is to maximize the use of these data (due to the non-rivalry in the use of data).115 The idea would be that such a solution would lead to much more innovation than the other approaches, and also allow for more competition in regard to additional products and services that could be developed and offered to car drivers (and passengers) based upon the access to these data.116 It certainly has to be ensured that such a data governance regime is safe and secure and that all rights of stakeholders, esp. also business secrets and rights for protecting privacy, are well-respected. However, in such a regime it has to be asked whether and to what extent such an approach might lead to incentive problems in regard to the production of data in connected cars.117

References

114 One big question in this scenario is whether powerful intermediaries (platforms with large direct and indirect network effects) might take over the role of PIMs, i.e. managing and commercialising the data of car owners, which might lead to new market failure in regard to data governance.
115 This approach would pick up the idea of the OECD (2015, 2016) who emphasized that in the digital economy data should be seen primarily as an "infrastructure". See also in regard to the data of connected cars, Hornung/Goebble (2015, 272).
116 It would be interesting to discuss the question who would in this approach get the benefits of the data, since neither the car manufacturers nor the car owners could "sell" these data any more. Since the service providers and new innovators could use these data for free, we could hypothesize from an economic perspective that the benefits of these data will end up to a large degree with the consumers of these new products and services, due to more innovation but also because they can be produced and provided with lower costs.
117 Such an approach however might solve a potential market failure problem, namely the data aggregation problem, i.e. that widely spread ("fragmented") exclusive "ownership" of data of the connected cars (either legally or on a de facto basis) might lead to a lower quality of data analytics through not enough access to as much data as possible (see section 2.2). This problem can emerge both in the first and second approach.
BMVI (2017), Eigentumsordnung für Mobilitätsdaten?
BMWi (2017), Weissbuch Digitale Plattformen: Digitale Ordnungspolitik für Wachstum, Innovation, Wettbewerb und Teilhabe.
BVDW (2016b), Connected Cars – Geschäftsmodelle.
DIRECTIVE 2010/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport.


Drexl, J. (2017), Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz, NZKart, 339 (Teil 1) and 415 (Teil 2).


EC (2014), Study on the operation of the system of access to vehicle repair and maintenance information. Final report.

EC (2016), Communication "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility".

EC (2017a), Communication "Building a European data economy".

EC (2017b), Staff Working Document "Building a European data economy".

EC (2017c), Access to In-Vehicle Data and Resources – Final Report.

Eucken (1952), Grundsätze der Wirtschaftspolitik, Tübingen.

European Data Protection Supervisor (2014), 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.


FTC (2014), Data Brokers. A Call for Transparency and Accountability, Washington, D.C.


Guidelines 2010/C 130/01 on Vertical Restraints.


HERE/ Swiss Re (2016), The future of motor insurance. A joint white paper.


MPI (Max-Planck-Institute for Innovation and Competition) (2017), Position statement on the European Commission's "Public Consultation on Building the European Data Economy" (26 April 2017).


Norberg/Home/Home (2007), The privacy paradox: Personal information disclosure intentions versus behaviors, Journal of Consumer Affairs, 100.


OECD (2015), Data-driven innovation: Big data for growth and well-being.

OECD (2016), Maximizing the economic value of data: Understanding the benefits and challenges of enhanced data access, DSTI/CDEP 4, 21.


REGULATION (EC) No 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 (EEC) No 123/1985 on the application of Article 85(3) of the Treaty to categories of motor vehicle distribution and servicing agreements.

REGULATION (EC) No 1400/2002 on the application of Article 81(3) of the Treaty to categories of vertical agreements and concerted practices in the motor vehicle sector.


Schwartmann, R./Hentsch, C.-H. (2015), Eigentum an Daten - Das Urheberrecht als Pate für ein Datenverwertungsrecht, RDV, 221.


