Kerber, Wolfgang

Working Paper

Data-sharing in IoT ecosytems from a competition law perspective: The example of connected cars

MAGKS Joint Discussion Paper Series in Economics, No. 21-2019

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

Suggested Citation: Kerber, Wolfgang (2019) : Data-sharing in IoT ecosytems from a competition law perspective: The example of connected cars, MAGKS Joint Discussion Paper Series in Economics, No. 21-2019, Philipps-University Marburg, School of Business and Economics, Marburg

This Version is available at:
https://hdl.handle.net/10419/204816

Joint Discussion Paper Series in Economics

by the Universities of

Aachen · Gießen · Göttingen
Kassel · Marburg · Siegen

ISSN 1867-3678

No. 21-2019

Wolfgang Kerber

Data-sharing in IoT Ecosytems from a Competition Law Perspective: The Example of Connected Cars

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

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

Data-sharing in IoT Ecosystems from a Competition Law Perspective: The Example of Connected Cars

Wolfgang Kerber*
(University of Marburg)

(version: August 26, 2019)

Abstract: This paper analyses whether competition law can help to solve problems of access to data and interoperability in IoT ecosystems, where often one firm has exclusive control of the data produced by a smart device (and of the technical access to this device). Such a gatekeeper position can lead to the elimination of competition for aftermarket and other complementary services in such IoT ecosystems. This problem is analysed both from an economic and a legal perspective, and also generally for IoT ecosystems as well as for the much discussed problems of "access to in-vehicle data and resources" in connected cars, where the "extended vehicle" concept of the car manufacturers leads to such positions of exclusive control. The paper analyses, in particular, the competition rules about abusive behavior of dominant firms (Art. 102 TFEU) and of firms with "relative market power" (§ 20 (1) GWB) in German competition law. These provisions might offer (if appropriately applied and amended) at least some solutions for these data access problems. Competition law, however, might not be sufficient for dealing with all or most of these problems, i.e. that also additional solutions might be needed (data portability, direct data (access) rights, or sector-specific regulation).

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

Keywords: Internet of Things, data sharing, data access, competition, digital economy, connected cars

* Professor of Economics, Marburg Centre for Institutional Economics (Macie), School of Business & Economics, University of Marburg, kerber@wiwi.uni-marburg.de. The author declares no conflict of interest.

1. Introduction

The “Internet of Things”, i.e. smart connected devices that are collecting, producing, and processing often huge amounts of data, are spreading exponentially in private and business environments as well as in public places. Besides the already ubiquitous smartphones, smart home applications (as smart TV, personal assistants as Alexa), smart agriculture (with data-collecting farm machinery), smart retailing, smart manufacturing, and also smart cities applications indicate the wide range of IoT applications. The problem of the governance of the huge amount of data collected and produced in IoT has raised not only questions about privacy and data protection but has also led to a new discussion about data access and data-sharing as part of the recent more general discussion about the new challenges of the digital economy for competition policy. Due to the essential role of data for innovation in the digital economy, there are large concerns that firms can use their exclusive control of certain sets of data for impeding competition and innovation, e.g. by blocking market entry of other firms, or leveraging their market power to other markets.[1] This article wants to focus on the question whether and to what extent competition law might provide options for solving data access problems in IoT contexts. Since the structures of IoT applications can be very different, this paper focusses on one particularly important group of cases, in which digital ecosystems emerge and often one firm, usually the manufacturer of the IoT device, controls the collected data and/or the technical access to the device. This might lead to the problem that this firm has a gatekeeper position with regard to this ecosystem and the data which might allow for the control of all markets, whose products and services either need access to these data and/or access to the ecosystem for offering them to the consumers, who are often locked-in into these ecosystems, usually after the purchase of the IoT device.[2]

In this paper the example of “access to in-vehicle data and resources” in connected cars will be used, because here already a well-developed policy discussion has emerged about a clear conflict between the car manufacturers, who through the application of the so-called “extended vehicle concept” are in such a gatekeeper position through their exclusive control of the access to the in-vehicle data and to the connected car, and a broad group of independent service providers. They claim that this position of the car manufacturers leads to the danger of foreclosing them from the emerging ecosystem of connected driving, which would lead to less competition, innovation, and consumer choice for car users. Whereas the car manufacturers defend their concept (with the im-

---

[1] See, e.g., Schweitzer/Haucap/Kerber/Welker (2019, 29), Crémer/de Montjoye/Schweitzer (2019, 73).

[2] Therefore the article does not focus on the discussion about data-sharing for AI and training of algorithms, or the discussion about direct data-sharing with horizontal competitors as in the proposal of Prüfer/Schottmüller (2017).

plication of closed ecosystems) with safety and security reasons, the independent service providers demand a regulatory solution for solving the competition problems caused by this position of exclusive control of the car manufacturers. This example is also particularly interesting, because one of the possible solutions that is being discussed (and demanded by the independent service providers) is the transition to a different technological solution, i.e. an open interoperable telematics platform, which would eliminate the gatekeeper position of the car manufacturers and allow the possibility that the car users themselves have the control about the access to the in-vehicle data and the connected car.[3] Therefore this example also shows that the competition problems in these ecosystems can be caused not only be the exclusive control of data but also by lacking interoperability and the closedness of these ecosystems. Although the EU Commission has acknowledged with regard to connected cars the existence of this competition problem and the need for dealing with these access problems in the ecosystem of connected driving, it has so far been very reluctant in proposing regulatory initiatives, i.e. this is a still open and unsolved policy question.[4]

Although this paper uses the connected car example, its main objective is to discuss in a general way the question whether and to what extent competition law is capable of solving problems of data access and data-sharing with regard to digital ecosystems in IoT contexts. As an economist, I will analyse these issues primarily from an economic policy perspective. Therefore this paper is based upon the broad discussion on the law and economics of rights on data (ownership/access/governance of data),[5] previous research of the author on data access problems in connected cars,[6] as well as the recent economic and legal discussion about solving data access in competition law, as, in particular, the three recent reports about challenges of the digital economy for competition law in Germany, the UK and the EU, all of which have put a special focus also on these data access problems in digital ecosystems and IoT contexts.[7] Therefore in section 2 first a brief overview about the most relevant results of the economics of digital ecosystems and the economics of data and interoperability with regard to such ecosystems will be presented. This is followed in section 3 by an overview about the competition and other market failure problems in our example of the ecosystem of connected driving. This also includes the policy question about more suitable solutions than the current

---

3 See for this discussion TRL (2017), Kerber (2018), and the literature in section 3.

4 See EU Commission (2018a, 13), in which the Commission acknowledged the problem and announced a recommendation, which so far has not been published.

5 See Zech (2016), Kerber (2016, 2017), Drexl (2017a, 2017b, 2018), Schweitzer/Peitz (2018), Schweitzer (2019).

6 See Kerber/Frank (2017), Kerber (2018), and Kerber/Gill (2019); from an economic perspective see also Martens/Mueller-Langer (2018).

7 See Schweitzer/Haucap/Kerber/Welker (2018) (German report), Furman et al (2019) (UK report), and Crémer/de Montjoye/Schweitzer (2019) (EU report).

extended vehicle concept for facilitating competition and innovation through easier access to the in-vehicle data and the connected car.

Section 4 is the main part of this paper that analyses to what extent European (and also German) competition law can be used for solving such data access problems with regard to digital ecosystems. Section 4.2 will focus on the question whether the refusal to grant access to data within an IoT ecosystem can be an abusive behavior of firms with market power. An important result of the analysis is that firms that control exclusively the access to certain sets of data and/or an ecosystem can be seen as dominant according to Art. 102 TFEU with regard to aftermarket and other complementary services, and their refusal to give access can be an abusive behavior due to the leveraging effects of market power on these secondary markets within the ecosystem. Although a careful analysis of the markets and a sophisticated balancing of the positive and negative effects of such a mandatory solution for access is necessary, we will see that from an economic perspective the requirements for granting mandatory access with regard to data might be considerably more flexible than in the traditional “essential facility” doctrine for access to physical facilities and IPRs. Another briefly addressed option is the use of Art. 102 TFEU for getting technical access to connected devices for solving interoperability problems. Since proving market dominance with regard to firms that have exclusive control of ecosystems might turn out to be difficult, this article will also discuss a recent proposal about applying also the provision of § 20 (1) GWB in German competition law, which prohibits abusive behavior of firms with “relative market power” (bilateral dependency of firms), for solving access problems to data in digital ecosystems (including a proposal for amending German competition law in that respect).

Overall, sections 4.2 will show that the provisions in European (and German) competition law about abuse of market power can be a powerful instrument for solving access problems with regard to IoT ecosystems, but that these case groups have to be developed step-by-step, which might be difficult and need a long time. Therefore, in section 4.3, it will also briefly be discussed, whether and how European competition law can be used for preventing the emergence of such positions of exclusive control of access to data. In addition to merger control and the law of abuse of dominance (e.g., regarding foreclosure strategies of acquiring data), also the prohibition of horizontal agreements between manufacturers of connected devices (as connected cars) are relevant (Art. 101 TFEU). In that respect a preliminary analysis will suggest that the “extended vehicle concept” of the car manufacturers might itself be seen as an (perhaps non-exemptible) anticompetitive horizontal agreement that restricts their competition on technology and governance of data, and leads to such exclusive gatekeeper positions in closed ecosystems of connected driving.

In the brief final chapter 5 the results of chapter 4 will be discussed in the broader context of other solutions for solving data-sharing problems and the access to digital ecosystems. Important conclusions will be that competition law can and should be used much more for solving these access problems to digital ecosystems, but that a comprehensive policy discussion should also take into account a broad set of other instruments for achieving satisfactory results. This can encompass facilitating more voluntary data-sharing between firms, the use of the data portability right (Art. 20 GDPR), direct legislative measures for defining access rights to data, measures for facilitating interoperability/standardization, and also sector-specific regulatory solutions (as, e.g. for connected cars). However, it will be claimed that competition law can and should always play an important role as general fallback solution in the case of the lack of other effective solutions.

2. Connected devices and IoT ecosystems: Some economics of data access and interoperability problems

Although the data access problems might vary considerably with regard to IoT applications (due to different economic and technological conditions), the current discussion about data access and data-sharing problems has shown the relevance of several economic reasonings about data and competition problems for digital ecosystems in IoT contexts. This section will provide a brief overview about the most important economic theories.

Economics of data: Since data are non-rival in use, i.e. the same data can be used by many firms with marginal costs of zero, a simple welfare economics analysis would imply that data should be used as much as possible for maximizing the value from these data. The danger of under-using the huge amount of existing data has been well recognized in the current discussion about the data economy, leading to demands for facilitating data-sharing, esp. also for data-driven innovation (e.g., also for data analytics and training of algorithms).[8] However, also the costs for the collection, processing, storage, and communication of data in connected devices have to be considered. These costs can be covered either through the price of this device (paid by the users) and/or by the manifold options for monetizing these data, which are often kept under the exclusive control of the manufacturer of the device. The exclusive de facto control of the data is

[8] See the Communication "Building a European Data Economy" of the EU Commission (2017a). However, for personal data such a simple welfare-theoretic reasoning might be misleading, if the privacy of persons and therefore their personal data are especially protected in a jurisdiction, as, e.g., in the EU, where privacy is protected as a fundamental right. Each additional use of personal data can violate the privacy rights of these persons.

economically similar to a de facto (but not legal) ownership of the data.[9] Since however in many IoT contexts (as also in the connected car example) often a number of firms / consumers contribute to the production of the data and/or need access to these data for offering services to the users of this connected device (multi-stakeholder situation), the exclusive control of the data by one firm (usually the manufacturer) might be an economically suboptimal solution for the governance of these data due to manifold hold-up problems with regard to the other stakeholders and too high prices for data access (leading to an inefficient underuse of data).[10]

Economics of interoperability: In addition to that, manufacturers usually also have the possibility to decide on the degree of interoperability of their devices, i.e. to what extent the owner of a device can give access to this device to other service providers and/or enabling them to offer additional services on this device (open vs. closed ecosystems). This might be traditional aftermarket services, as, e.g., repair and maintenance services, or additional services that are complementary to the services of the device. Important results of the economics of interoperability are, (1) that often more interoperability can lead to advantages in terms of more competition and innovation on markets for complementary products and services and to a larger choice of the users of the device, but (2) that there also might be advantages of closed proprietary systems, especially with regard to quality and product differentiation.[11] However, economic theory has shown that firms often have too many incentives for choosing systems with a too low level of interoperability, leading to too closed systems with a too low level of openness and interoperability.[12] This problem also seems to be very relevant with regard to IoT applications, where many complaints about too many firm-specific proprietary solutions can be found, leading to the demand for more interoperability and standardization.[13]

Economics of ecosystems, user lock-in, bundling and leveraging problems: Through controlling the access to the data of connected devices as well as to the device itself, the manufacturer of a device gets into the position of a monopolistic gatekeeper to the

---

[9] For the discussion why there is no need for an introduction of exclusive IP-like rights for data from an economic perspective see Kerber (2016) and the other references in fn. 5.

[10] See for the data governance problems in multi-stakeholder situations as they are typical in many IoT ecosystems Kerber (2017) and Kerber/Frank (2017) about the concept of data governance regimes. For the economics of data see also Duch-Brown et al (2017) and Schweitzer/Peitz (2017).

[11] For advantages and costs of interoperability see Palfrey/Gasser (2012), Gasser (2015), and from an economic perspective Choi/Whinston (2000), Farrell/Simcoe (2012), and as overview from a competition law perspective Kerber/Schweitzer (2017, 41).

[12] For market failures with regard to interoperability (and standardisation) due to misaligned incentives see Farrell/Weiser (2003), Farrell/Simcoe (2012), and more generally Kerber/Schweitzer (2017, 42-48) and Furman et al (2019, 71).

[13] See PwC (2017, 132)

entire ecosystem of services and products that can be offered through or in combination with this device. Due to the investment in the connected device (and other sunk costs) the users can have large switching costs (lock-in). Such an exclusive control of the access to the data of the connected device and/or the technical access to the device can be used by the manufacturer of the device (as a primary product) for foreclosing all independent providers of services on the markets for aftermarket and complementary services (secondary products), as far as such an access is necessary for providing these services and entering these markets ("essential resources"). Therefore the manufacturer can leverage this monopolistic gatekeeper position to all markets for those services which depend on this access, and therefore can control these markets.[14] This problem is well-known in the economic and legal literature about aftermarkets but can have a much larger relevance in digital ecosystems due to the often broader range of complementary services in digital ecosystems (or on digital platforms).[15] From an economic perspective this can be seen also as a de facto bundling strategy, because the user of the device is not free to choose providers of aftermarket and other complementary services in the digital ecosystem but has to accept the entire bundle of the connected device and services offered by the manufacturer.[16] Important is that such a bundling strategy can be implemented either by denying access to necessary data, lack of interoperability, or also through a contractual bundling of these services.

However, from a competition economics perspective it is not clear whether such closed ecosystems and bundling strategies are really harming the consumers, even if independent service providers are foreclosed from these secondary markets. One important question is whether systems competition among the manufacturers of connected devices works so well that it can be seen as a sufficient substitute for the lacking competition processes on the markets for complementary services. The lower the value and durability of the device, the smaller and less complex these bundles are, the better informed the users of these devices are about the benefits and costs of these bundles, and the lower the switching costs (through sunk costs) for the users are, the better systems competition might work.[17] Therefore a careful and deep case-specific analysis of this

---

[14] Please note that there might be complementary services, which only need access to the data produced with the device, others might need technical access to the device, and again many others might need both.

[15] See for the economics of these ecosystems, supply-side economies of scope, consumption synergies, bundling, gatekeeper positions, and the leveraging of market power as well as the effects on market entry and innovation see the comprehensive survey of economic literature in Bourreau/de Streele (2019, 9-21).

[16] This does not mean that all these services are offered by the manufacturer itself or that the user of the device cannot choose between service providers, but it is the manufacturer who has exclusive control whether and under what conditions service providers can enter these markets.

[17] See for the economics of aftermarkets Shapiro/Teece (1994), Shapiro (1995), Borenstein et al (2000), Hawker (2011), and the broad legal and economic overview in OECD (2017).

question might lead to different conclusions for different connected devices and IoT ecosystems. This is also directly related to the question whether the bundling of the device with other services has positive effects on efficiency and innovation, e.g., through economies of scope on the supply-side or consumption synergies on the demand-side. Therefore it has to be asked whether the benefits of a closed ecosystem, in which one firm has exclusive control as a gatekeeper and can foreclose competition on these secondary markets, can be expected to be larger than the benefits of competition through independent service providers on the markets for aftermarket and other complementary services in these ecosystems.

Therefore in IoT ecosystems three different market failure problems can emerge: (1) The possibility of exclusive control of the manufacturer about the data produced with the device and the technical access to the device can lead to competition problems on the secondary markets for aftermarket and other complementary services. (2) There might be a market failure with regard to the optimal level of interoperability leading to the danger of too closed ecosystems. (3) The exclusive control of data can also lead to an under-utilization of these data, esp. also with regard to the reuse of these data outside of these IoT ecosystems.[18] Whereas the last concern also refers to the current discussions about the benefits of data aggregation and about (mandatory) data-sharing with respect to AI applications and training algorithms (which is beyond the scope of this paper),[19] we will focus on the potential negative effects for competition and innovation through the exclusive control of access to (a) the data and (b) the connected device (interoperability). Important is that these two problems often have to be solved simultaneously. This can be called the “twin problem” of data and interoperability in IoT ecosystems. The often (but not always) existing simultaneous relevance of both problems has been particularly emphasized in the EU and UK report.[20] In that respect, the EU report offers a valuable distinction between “data interoperability” as the combination of data portability and protocol interoperability, which implies that a specific form of interoperability is necessary for enabling data access / sharing / portability, and the socalled “full protocol interoperability” that, in addition to that, also allows that independent service

---

Crémer/de Montjoye/Schweitzer (2019, 88-91) emphasize the need for “an update of the traditional competition law analysis of aftermarkets” in regard to the specificities of data (ibid., 10).

[18] See for such a market failure framework Kerber (2018, 316-325), which also entails in addition the huge problems of “notice and consent” solutions with regard to privacy policies in the contracts between the manufacturers of connected devices and the consumers (ibid., 323). Here market failures through information and behavioral problems can arise, as they are well-known from the “privacy paradox” discussion. These problems of connected devices and IoT ecosystems are not discussed in this paper.

[19] See, e.g., Schweitzer/Haucap/Kerber/Welker (2018, 185).

[20] See Cremer/de Montjoye/Schweitzer 2019, 83-86), Furman et al (2019, 71-74).

providers can interoperate with the IoT ecosystem.[21] Both forms of interoperability are deeply linked with needs for standardisation. Whereas for "data interoperability" the introduction of APIs is seen as a possible solution (ibid., 84), "full protocol interoperability" is much more difficult to achieve, and can also raise significant safety and security issues (as we will see in the connected car example).

Whatever policy instrument will be used for solving these problems (competition law, data access rights, data portability right or sector-specific regulation), from an economic perspective it is always necessary to find a governance solution for these data and the access to the ecosystem (interoperability), which carefully balances the often manifold benefits and costs of different solutions for avoiding harm to consumers and respecting other legitimate interests (as, e.g., privacy or business secrets and intellectual property rights).

3. The problem of "Access to in-vehicle data and resources" in the ecosystem of connected driving

The connected car is one of the most important examples of IoT applications with the emergence of a new ecosystem of connected driving with its own specific problems of data access and data-sharing as well as interoperability problems. Important characteristics of the connected car are that a huge amount of different kinds of data are collected, produced, and processed in the car (often through sensors). These "in-vehicle data" can be technical data about the car and its components, data about road, weather and traffic conditions, the driving behavior of the car drivers, location data but also data about the use of entertainment, navigation and many other services of the car users.[22] Through mobile communication with external entities ("connectivity") data can be transmitted in real-time from and to the car, which technically allows a direct real-time access to the in-vehicle data but also the transmitting of data to the car. The connectivity and the in-vehicle data allow for many new (and innovative) services that can be offered to the car users. They can include new forms of repair and maintenance services (as, e.g. remote diagnostics and maintenance), navigation services, parking apps, search services for hotels and restaurants, entertainment, online-shopping, but also new insurance schemes (as used-based insurance), and many others.[23] The ecosystem of connected driving encompasses therefore a large number of complementary services (including

[21] See Crémer/de Montjoye/Schweitzer (2019, 84-85). In the Furman report the implementation of personal data mobility and systems with open standards is seen as one of the tools within their "pro-competition policy in digital markets" (Furman et al 2019, 57-79).

[22] Most of these data are personal data according to the GDPR.

[23] See generally about connected cars OECD/ITF (2015); Anderson et al. (2016), Alonso Raposo et al. (2017); for the new business opportunities through the connected car see McKinsey (2016).

aftermarket services), which can offer many benefits to the car users during connected driving, and also a broad range of firms that would like to provide these complementary services to the car users, and which jointly with the car manufacturers (OEMs: original equipment manufacturers), component suppliers, and authorised dealers and repairers can be seen as part of this ecosystem of connected driving.

The current policy discussion about "access to in-vehicle data and resources" in the transition to connected cars[24] is triggered by the attempt of the car manufacturers to establish the "extended vehicle concept" as general solution for the governance of the in-vehicle data and the connected car.[25] This concept implies that all in-vehicle data are directly transmitted to an external proprietary server of the OEMs, which gives them an exclusive de facto control of these data, and access to these data is only possible through the OEMs. Additionally, the "extended vehicle concept" also implies that the OEMs have exclusive technical access to the connected car, i.e. car users cannot allow independent service providers direct access to the car, e.g. for performing repair and maintenance services. Therefore the "extended vehicle" concept leads to closed proprietary ecosystems of the OEMs, in which they have exclusive control both about the in-vehicle data and the access to the IT-system of the cars. OEMs defend this closed ecosystem with safety and security arguments. As a consequence, the OEMs have a monopolistic gatekeeper position with respect to the markets for all aftermarket and other complementary services within these brand-specific ecosystems of connected driving, which require access to either in-vehicle data and/or the connected car. This also implies a lock-in situation for the car owners, because after buying the car they only can choose between the services and service providers the OEMs are offering. Therefore the concerns of the independent service providers that the implementation of the "extended vehicle" would allow the OEMs to foreclose them from the markets for aftermarket services and other complementary services in the ecosystem of connected driving are justified.[26]

In the policy discussion about the problem of "access to in-vehicle data and resources"[27] a broad coalition of independent service providers demands a regulatory

---

[24] See for this discussion C-ITS platform (2016), TRL (2017), Kerber (2018, 312-315); for position papers of the stakeholders see ACEA (2016a, 2016b), VDA (2016), FIGIEFA (2016), FIA (2016), AFCAR (2018), and as an overview of the positions of the stakeholders Specht/Kerber (2018, 49-55).

[25] For the "extended vehicle" concept see ACEA (2016a, 2016b) and VDA (2016).

[26] For the already existing mandatory access regime for necessary technical information for traditional repair and maintenance services, see below at the end of this section.

[27] This term also shows the twin character of access to the "in-vehicle data" and access to "resources" of the car. The latter means primarily the IT system of the car for either downloading data ("read") or also uploading data or providing services in the connected car ("write") as re-

solution for these access problems.[28] For the short-term, the so-called “shared server” concept has been proposed. This would imply the same technical solution of transmitting all in-vehicle data to an external server, but this server would be under the governance of a neutral entity, which could provide non-discriminatory access to the in-vehicle data to all stakeholders (including the OEMs) in this ecosystem, which would lead to a level-the-playing field with regard to access to the data for the secondary markets. In the long run, the preferred technical architecture for the Independent service providers would be an open, interoperable telematics system, the “on-board application platform”. This is a technical solution that would establish industry-wide standardised interfaces for V2X communication of connected cars, and would therefore offer the technical possibility of direct access to the in-vehicle data and the IT-system of the car. It would technically enable the car drivers to decide directly who gets access to in-vehicle data and the IT system of the car. The basic idea of both solutions is the elimination of the exclusive “monopolistic” control of the OEMs regarding access to in-vehicle data and resources. The independent service providers claim that such a regulated solution would lead to more competition, innovation, and consumer choice than the currently applied “extended vehicle concept”.

How can the “extended vehicle” concept with its implication of closed ecosystems be assessed from an economic perspective? In the following, only a summary of preliminary results of the few studies that exist on this problem can be presented.[29] The control of the brand-specific ecosystems allows the OEMs several strategies: They can monopolise certain services entirely for themselves by not giving access or they can allow entry for a limited number of service providers for fees (e.g., also with exclusivity agreements) that allow them to reap the profits on these secondary markets. Therefore the OEMs can leverage their market power to the markets for aftermarket and other complementary services. In addition to that, they also can sell access to anonymised data sets of the in-vehicle data to third parties outside this ecosystem with monopoly prices, because only they can sell these in-vehicle data. As a consequence, the OEMs can control competition and innovation within their ecosystems, i.e. the OEMs can decide which innovation activities of the independent service providers they allow or not. Since the empirical experience in automobile aftermarkets is that the prices of repair

---

mote diagnosis or software updates. Another aspect of access refers to the Human-Machine-Interface (HMI or dashboard), with whose control the OEMs can impede the direct independent communication between car users and independent service providers. See TRL (2017, 75-92) and Martens/Mueller-Langer (2018, 7-10).

[28] See for the following position of the independent service providers FIGIEFA (2016), FIA (2016), AFCAR (2018).

[29] See in much more detail Kerber (2018, 316-325), but see also Kerber/Frank (2017), Martens/Mueller-Langer (2018) from an economic perspective and various other studies about different aspects of the problem (Quantalyse Belgium/Schönenberger Advisory Services 2019, 53-55).

and maintenance services as well as spare parts of OEMs are much higher than those from independent service providers,[30] the concerns of consumers that the elimination of competition on aftermarket and complementary markets would lead to higher prices and less consumer choice has to be taken very seriously. So far there are also no arguments (e.g., by the OEMs) that such closed ecosystems of connected cars would lead to efficiency advantages or more innovation with regard to aftermarket and complementary services. On the contrary, it is the independent service providers who emphasize the danger that their independent innovation activities with regard to these services are blocked through lacking access to the in-vehicle data and the car, thus possibly leading to less innovation.[31]

For defending their "extended vehicle" concept the OEMs rely entirely on the safety and security argument.[32] Although they are trying to frame the policy discussion as a trade off-problem between maximum security on the one hand and fair and undistorted competition on the other hand, the discussion among experts make it increasingly clear that such a trade off between more security and more competition does not exist.[33] The main argument is that most IT experts think that an open interoperable telematics system with a multi-layered safety and security system (including certification) can achieve at least the same security levels than proprietary closed systems. Therefore access of independent service providers to the connected cars is possible with an open interoperable telematics system without compromising safety and security. This is also one of the main results of the comprehensive TLR report (TRL 2017), which was commissioned by the EU Commission. Independent from this discussion about the safety and security issues of the technical access to the car, it is, in any case, clear that the de facto "appropriation" of the in-vehicle data through transmitting them to a proprietary server of the OEMs and the ensuing possibilities for monetizing this exclusive gatekeeper position to these data cannot be justified through safety and security arguments.[34] Therefore the safety and security argument cannot be a justification for the exclusive control of the access to the in-vehicle data and the connected car with its ensuing potential negative effects on competition and innovation on secondary markets in the ecosystem of connected driving.

Much more relevant from an economic perspective is however the question whether systems competition, i.e. competition between the closed ecosystems of the OEMs, might work well enough for avoiding (or limiting) the alleged negative effects on prices,

30 See, e.g., Quantalyse Belgium/Schönenberger Advisory Services (2019, 24).
31 See FIGIEFA (2016, 3)
32 See ACEA (2016b, 5).
33 See Kerber (2018, 318) with more references.
34 Ibid., 319.

innovation, and consumer choice for aftermarket and complementary services. Since cars are very durable, valuable and complex products with large switching costs, and it is very hard for consumers to assess the value of the bundle of connected cars and the future services in these ecosystems, it is very doubtful whether systems competition can work well enough for being capable of being a substitute for the positive effects of competition processes on independent markets for aftermarket and complementary services within the ecosystem of connected driving. However, the question whether and to what extent competition among OEMs can at least limit the negative effects of these closed ecosystem is a question that deserves a deeper investigation. Such an analysis should also encompass the increasing role of new players in the ecosystem of connected driving (as Google, Apple etc.)[35] as well as the question whether OEMs use the extended vehicle concept for restricting their (systems) competition with regard to technology and data governance (see below section 4.3.2).

Although much more research on the effects of the "extended vehicle concept" and possible regulatory options is necessary, the results of the so far existing studies clearly suggest that the "extended vehicle" concept of the OEMs is not the best solution, esp. due to its negative effects on fair and undistorted competition. From an economic market failure perspective, the following problems can be identified (Kerber 2018): (1) The exclusive control of the access to in-vehicle data and the connected car can lead to a serious market failure in respect to competition on the markets for aftermarket and other complementary services, which can be expected to lead to higher prices, less innovation, and less consumer choice as well as a too low level of data-sharing for the data economy. (2) The OEMs' choice of such closed proprietary ecosystems can itself be the result of a market failure with regard to the optimal level of interoperability, i.e. a more open interoperable telematics system might be a superior technological solution, esp. also with respect to the medium- and long-term development to integrated mobility systems.[36] Other studies came to similar critical assessments of the "extended vehicle" concept.[37] Especially important is the already mentioned TRL study that came to the conclusion that, in the short term, the "shared server" concept, and in the medium term, the transition to an open interoperable telematics system (on-board application platform) would be superior solutions compared to the "extended vehicle concept" of the OEMs.[38]

---

[35] See also Martens/Mueller-Langer (2018).

[36] In addition to that, there might also be a market failure with regard to the consent of car owners about the provision of data in the contracts with the OEMs (due to information and behavioral problems).

[37] See from an economic perspective also Martens/Mueller-Langer (2018).

[38] The TRL study (2017) analysed whether different technological access solutions, as, in particular, the "extended vehicle" concept, the "shared server" concept, and the interoperable "on-board application platform" would be compatible with 5 principles on which all stakeholders

Although there seems to be a wide-spread consensus that the "extended vehicle" concept is not the best solution, and that it is necessary to think about regulatory solutions, so far no clear comprehensive regulatory solution has been developed and proposed. One problem is that the alternatively discussed policy options of the "shared server" and the "on-board application platform" do not solve all problems but need much further elaboration, and presumably also additional regulatory solutions. Another big problem is that the in-vehicle data are themselves very heterogeneous, which implies that the optimal data governance solutions might be different for different types of data.[39] This refers not only to the important distinction between personal and non-personal data (compliance with GDPR) but also to the distinction between raw and processed/aggregated data, data about technical functions of the (components of the) car or about traffic, road and weather conditions etc. Depending on the type of data also business secret (and IP) concerns and incentive problems for the production of the data might play a more or less important role. Therefore an economic analysis of the benefits and costs of granting access rights to data to certain service providers within the ecosystem of connected driving might lead to different results for different types of data. It might also depend on the types of the data whether a remuneration for these data should be required, and what a reasonable level of fees is. Similar questions arise also for the question of the optimal technological choice with regard to interoperability and openness of the connected cars.[40]

This complexity of the ecosystem of connected driving with this simultaneous problem of access to in-vehicle data and access to the car, the multitude of involved stakeholders and many complementary services that will be offered within this ecosystem suggests that looking for a sophisticated sector-specific regulatory solution might be the best path for dealing with this problem and finding a tailor-made governance solution that balances properly the manifold positive and negative effects within such a complex IoT ecosystem. In this regard it is important that in the EU we already have an (overall well-functioning) long-standing regulated regime in the automobile industry for the access to technical information (and diagnostic data in the OBD adapter) that are necessary for repair and maintenance services of independent service providers (RMI: repair and maintenance information). But this access regime was designed for the old technology before the transition to connected cars. Since 2007 this sector-specific access

---

agreed on the C-ITS platform (see for these principles, which also entails "fair and undistorted competition" C-ITS platform 2016, 75). The TRL study however stops short of recommending a mandatory solution.

39 For the necessity to take into account the heterogeneity of data see Crémer/de Montjoye/Schweitzer (2019, 98-107).

40 For a broad and very insightful discussion about advantages and problems of "open cars" in comparison with closed systems see Determan/Perens (2017).

regulation can be found in the motor vehicle type approval regulation, which was amended last year.[41] The objective of this regulatory solution was always the protection of competition of independent service providers with the authorised dealers and repairers of the OEMs but only on the secondary markets of traditional repair and maintenance services. According to this Regulation the OEMs are under obligation to grant access to the necessary technical information in a non-discriminatory way and for reasonable fees (FRAND-like solution). Since this well-established solution, which faces considerable challenges in this transition process to connected cars, already encompasses both mandatory access to information and mandatory technical solutions for access to (diagnostic) data and safety and security solutions,[42] it can also be seen as a starting-point for a necessary much broader general sector-specific governance solution for solving the "access to in-vehicle data and resources" problem in the ecosystem of connected driving.[43] Since however it is not clear at all whether such an effective sector-specific regulatory solution will be found and implemented in a successful way, it is also very important to analyse in the case of connected cars, to what extent other solutions, especially through general competition law, can lead to satisfactory solutions or solve at least part of these access problems.

4. Competition law solutions for data governance problems in IoT ecosystems

4.1 Introduction

This section 4 focuses on the question what options competition law can offer for solving such governance problems with regard to data and interoperability in digital IoT eco-

41 See Regulation (EU) 2018/858 of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, Official Journal of the European Union, L 151/1, 14.06.2018, which replaces the current Regulation (EC) No 715/2007 of 20 June 2007 on type approval of motor vehicles and on access to vehicle repair and maintenance information. Official Journal of the European Union, L 171/1, 29.06.2007. See for an assessment of this regulation EU Commission (2014).

42 See for an analysis of this regulated access regime for "repair and maintenance information" and its reform in 2018 in the context of the transition to connected cars Kerber/Gill (2019). This paper claims that the reform will not solve the main problems of access to data and the connected car for independent service providers in the automobile aftermarkets, esp. with regard to the new innovative services of remote repair and maintenance services. Therefore also this access regime needs further evolution during the transition to connected cars.

43 Another way of introducing such a tailor-made sector-specific regulation has been suggested by the Furman report, in which a newly created "digital markets unit" should have the regulatory powers to set up mandatory rules for data mobility and interoperability („open standards") where this will lead to more competition and innovation. The "access to in-vehicle data and resources" of connected cars would be a very suitable example where this approach can be applied. See Furman et al (2019, 9 and 64-82).

systems. It is however necessary to keep in mind that also other legal instruments can be used for solving such problems in digital ecosystems. One group of solutions entails proposals to introduce through legislation data rights, either as property-like exclusive rights ("data producer right") or as access rights on data.[44] Another group of solutions is based upon the data portability right with regard to personal data (Art. 20 GDPR), and then asks whether this data portability right (and perhaps its extension also to non-personal data) can help to solve the data access problems.[45] A third group of solutions asks whether contract law solutions (esp. in combination with the Unfair Trade Practices Directive) might offer sufficient possibilities for dealing with these data governance problems.[46] A fourth alternative option to general competition law are sector-specific regulatory solutions (as suggested for the connected car problem in the last section). However, the analysis in this chapter will only focus on possible solutions through general competition law. A comprehensive comparison of these different solutions is beyond the objective of this paper.

So far in the literature much scepticism can be found whether general competition law is suitable for dealing with such problems of data access. Especially, in the discussion about using the "essential facility doctrine" of Art. 102 TFEU as an instrument for granting access to data, many legal scholars are very reluctant whether this is a feasible and recommendable instrument.[47] Particularly interesting in that respect are also the results of the consultation of the EU Commission on "Building a European Data economy", which showed that many stakeholders who have data access problems, esp. in situations of "unequal bargaining power", do not believe that competition law offers sufficient instruments for helping them.[48] Whereas one reaction in this discussion is that we should look for solutions outside general competition law (as the solutions described above), another reaction is to ask whether we can also do more within competition law, either by developing new reasonings and theories of harm for applying existing competition law rules or by amending competition law (e.g. by legislation). Both the German report and the EU report about the challenges of the digital economy for competition policy have analysed to what extent general competition law can deal with these ques-

---

[44] See the comprehensive study of Drexl (2018).

[45] See Crémer/de Montjoye/Schweitzer (2019, 81), Furman et al (2019, 65-71), and generally Art. 29 Data Protection Working Party (2017),

[46] See Schweitzer/Haucap/Kerber/Welker (2018, 180-183) and EU Commission (2018b, 2018c).

[47] See, e.g., Autorité de la Concurrence/Bundeskartellamt (2016, 18), Körber (2016, 303), Drexl (2017b; 2018, 36), Schweitzer (2018, 279), and especially also the UK report (Furman et al 2019, 55). The Furman report explicitly claims that traditional competition law is not capable of solving these problems, which leads to its proposal of a "digital market unit" that also should have regulatory powers for solving data access and interoperability problems (ibid, 55-81).

[48] See EU Commission (2017b, 14).

tions of access to data in IoT ecosystems, and what can be done in competition law for facilitating these solutions.[49]

The following analysis is divided into two main sections. Section 4.2 will start with the assumption that one firm in an ecosystem (usually the manufacturer of a smart device) has exclusive control of the data of the connected device and/or exclusive control of the technical access to the device. It will analyze whether the refusal to grant access can be a prohibited abuse of a firm with market power. Whereas in section 4.2 the gatekeeper position of this firm as exclusive holder of the data is not challenged itself, and the focus is on whom to give additional access to these data and the device, the following section 4.3 analyses whether this exclusive position can be directly challenged by competition law, esp. in cases, in which this exclusive position might be itself a result of anticompetitive behavior that infringes competition law. In that respect, also merger control and Art. 101 TFEU might get relevant. Although the main focus of the analyses will be on data access problems, also interoperability problems will be addressed to some extent.

4.2 Refusal to share exclusively held data as abusive behavior of firms with market power

With regard to the connected car example we start with the current situation that car manufacturers apply the extended vehicle concept, in which all data are transmitted to a proprietary external server of the OEMs. Therefore it can be asked whether independent providers of services on aftermarkets and other complementary markets can claim access to certain kinds of in-vehicle data based upon the argument that the refusal of OEMs to grant access or share the data is an abusive behavior of a firm with market power in competition law. Similar claims can also be made by independent service providers in other IoT ecosystems.[50] Such a claim could be based upon the prohibition of abusive behavior of dominant firms according to Art. 102 TFEU (or § 19 (2) GWB in German competition law). We will analyze this option in the following section 4.2.1. Since it might be difficult in such cases to prove that the firm with exclusive access to data and/or the device (as here the OEMs) has market dominance, we will additionally analyse in section 4.2.2 whether such a claim can also be based in Germany upon a specific provision of German competition law (§ 20 (1) GWB), which prohibits abusive behavior also for firms that are not dominant but have so-called “relative market power”. In the recent discussion about the challenges of the digital economy it was suggested

[49] See Schweitzer/Haucap/Kerber/Welker (2018, 158-191) and Crémer/de Montjoye/Schweitzer (2019, 73-109).

[50] It is a different case, if the user of the connected device is a consumer who would like to have access to the data or interoperability for being capable of using this device better. See for an analysis from the perspective of consumers Drexl (2018).

that this provision of § 20 (1) GWB could also be used for dealing with data access problems in IoT ecosystems.[51]

4.2.1 Abusive behavior according to Art. 102 TFEU

Claiming access to data from the exclusive holder of data in a digital ecosystem can be based according to Art. 102 TFEU either on the "essential facility doctrine" (EFD), which has been developed step-by-step by the European courts,[52] or more directly on the argument that the refusal to grant access to data can foreclose independent competitors on aftermarkets and other complementary markets within the ecosystem, and therefore might lead to a leveraging of market power.[53] Both the German and the EU report suggest that in the case of IoT ecosystems and aftermarkets, in which one firm is the gatekeeper that can foreclose independent providers of aftermarket and complementary services, a direct balancing of interests based upon the reasoning of leveraging market power might be legally a more suitable solution than using the well-established "essential facility doctrine" with its so far very high requirements.[54] Since however from an economic perspective the economic reasonings and necessary balancing of benefits and costs of granting mandatory access to data are in both legal solutions within Art. 102 TFEU basically the same, the problem will also be discussed from an essential-facility approach. However, in a first step, we have to analyze whether and under what conditions manufacturers of IoT devices (here: the car manufacturers) can be deemed as having a dominant position as a precondition for the application of Art. 102 TFEU.

Market dominance of exclusive data-holders in digital ecosystems

If the manufacturer of a smart device is dominant according to the usual criteria on the market of this type of smart devices, and therefore there is no effective competition among the manufacturers of those devices, then we have no particular problem that the manufacturer as exclusive gatekeeper to the secondary markets is a dominant firm. However it is much more difficult, if there is competition among the manufacturers of the primary product (as in the case of connected cars). If independent service providers would like to have access to certain sets of in-vehicle data that are exclusively held by the OEMs, the latter can be deemed dominant in two different ways: (1) As far as these

---

[51] See Schweitzer/Haucap/Kerber/Welker (2018, 178, 187-191).

[52] See Case C-7/97, Bronner, EU:C:1998:569; Case C-241/91P, Magill; Case C-418/01, IMS Health, EU:C:2004:257; Case T-167/08, Microsoft, EU:T:2012:323.

[53] See for the following discussion also Schweitzer/Haucap/Kerber/Welker (2018, 162-177) and Crémer/de Montjoye/Schweitzer (2019, 98-108).

[54] See Schweitzer/Haucap/Kerber/Welker (2018, 172); Crémer/de Montjoye/Schweitzer (2019, 98).

data are not accessible otherwise (e.g. through data from smartphones), the OEMs have a monopoly on all of these data that are produced in the cars they have sold. Therefore it is possible to define an OEM-specific market for data that might be necessary for offering certain services to the users of these cars, on which the OEMs are monopolists and therefore dominant according to Art. 102 TFEU.[55] (2) After the sale of a car to consumers they are locked-in into the OEM-specific ecosystem of connected driving, and therefore the exclusive control of the OEMs grants them a dominant position on the OEM-specific secondary markets for aftermarket and complementary services.

If we ask from a consumer welfare perspective, whether such dominant positions and the ensuing foreclosure of competition on secondary markets will harm consumers, then the question of the effectiveness of systems competition emerges. In section 3 we already discussed this problem for connected cars, and suggested as a preliminary result that in the case of such a complex and durable product as a connected car the competition forces might be too weak for being a sufficient substitute for direct competition on these secondary markets in these ecosystems. Therefore with regard to market definition these secondary markets are separate markets, on which the OEMs can be seen as dominant firms with regard to the data access claims of independent service providers who want to offer services on these secondary markets.[56] Since, however, the effectiveness of systems competition depends on many determinants, it can be expected that the extent of negative effects through these dominant positions for the consumers might differ significantly between different types of smart devices. If smart devices are relatively cheap and/or not very durable, and the range and value of secondary services limited,[57] then competition among device manufacturers might work sufficiently well, with only limited negative effects on consumers with regard to prices, innovation and consumer choice on these secondary markets. In this case systems markets can be defined and no separate markets for these secondary markets exist.

Refusal to grant access to data as abusive behavior

---

55 For the problems of defining data markets see also Graef (2015).

56 See Schweitzer/Haucap/Kerber/Welker (2018, 176) for a number of court decisions, esp. in German courts, in which brand-specific definitions of secondary markets in the automobile industry were accepted. The EU Commission has been so far more restrictive with regard to brand-specific secondary markets. However it should be noted that if we assume the effectiveness of systems competition between car manufacturers, then also the entire regulated regime about access to repair and maintenance information (RMI) in the EU Motor Vehicle Type Approval Regulation would not be necessary, at least from an economic perspective.

57 See again OECD (2017, 42) with its long list of relevant criteria for the determination of separate secondary markets. For an overview about the legal situation with regard to the aftermarket doctrine in EU competition law (and US antitrust law) see Bell/Kramer (2015).

For the following analysis, it will be assumed that the manufacturer with its exclusive control of the data is dominant. Then the question arises whether the refusal to grant access to certain sets of data that are demanded by an ISP who wants to provide complementary services is an abusive behavior. According to the "essential facility doctrine" of Art. 102 TFEU several conditions with high requirements have to be fulfilled:[58] (1) The access to the data (or the access to the car) has to be indispensable for providing the service of the independent service providers. This implies that the data cannot be obtained through other channels or can be substituted through other data.[59] From an economic perspective the fulfillment of this criterion is necessary, because otherwise the data controller could not foreclose the independent service providers from the markets for aftermarket and other complementary services. (2) Without access to these data (or the access to the car) competition is threatened to be eliminated on these secondary markets. If the data are a necessary input for offering these services, then the refusal to get access would eliminate competition on these markets, i.e. also this criterion can be expected to be fulfilled. It is more difficult, if the data holder is willing to grant access but only at high prices and other contractual conditions that limit the independent service providers in their competition on secondary markets (as often in the case of connected cars). In that case the conditions for access might lead to a significant distortion of competition on these secondary markets, esp. if the manufacturers would offer their own providers of services more favorable terms (self-preferencing),[60] and therefore threaten to eliminate competition. (3) With regard to the refusal to grant a license to an IPR, the ECJ additionally required the so-called "new product test", i.e. that through this license a "new" product or service can be offered. From a legal perspective, it is very unclear whether the "new product" test in data access cases is necessary, because these data are not protected by patents or copyright.[61] But in many IoT contexts (as in the connected car example), it also could be argued that the independent service providers would offer complementary services that are not offered by the manufacturer of

[58] See for a brief overview on the "essential facility" doctrine Schweitzer/Haucap/Kerber/Welker (2018, 162-171).

[59] One interesting question is whether the data can be made accessible through the use of the data portability right of the car owners (Art. 20 GDPR). It is however so far very unclear whether this can be an effective instrument. See generally Article 29 Data Protection Working Party (2017) and for a more sceptical view about its effectiveness Furman et al (2019, 68).

[60] This is important for the discussion about access to in-vehicle data, because the OEMs in their extended vehicle concept emphasize that they are willing to offer access to data via free B2B-negotiations, but they can decide freely, what kind of data they make accessible to whom, and under what conditions.

[61] See from a legal perspective Schweitzer/Haucap/Kerber/Welker (2018, 168) and Crémer/de Montjoye/Schweitzer (2019, 106), where it is argued that the "new product rule" should not be applied to data cases.

the smart device.[62] (4) The last and very important criterion is whether the refusal to grant access to the data (and/or the connected car) can be objectively justified. In that respect a number of justifications might be discussed with regard to access to (data in) digital ecosystems, and, in particular, also with regard to our example of the ecosystem of connected driving.

One important objective justification of refusing access to data is the necessity to comply with the GDPR, if the demanded data is personal data, as it often might be, if an ISP wants to provide specific complementary services to individual car users. Therefore a tension with the GDPR will arise with the need for finding a way of data access that complies with data protection law.[63] Another possible justification for refusing access to data are concerns about safety and security. In our example, the car manufacturers defend their "extended vehicle concept" with the argument that the exclusive access to data and the connected car is necessary for maintaining a maximum level of safety and security of connected cars. It is clear that safety and (cyber)security of the connected car are very important objectives (from the perspective of both the car users and public policy). Therefore safety and security concerns can be an important issue that might lead to a justification in IoT contexts. However, as already discussed in section 3, in our example of connected cars safety and security concerns do not justify that the OEMs also have the exclusive control of all the data that are produced in the connected car.[64]

With regard to the mandatory access to physical essential facilities or intellectual property rights it was always seen as necessary to balance the benefits of the access to the facility with the necessity of maintaining incentives for the investment in these essential facilities. The ownership of physical facilities and intellectual property rights is protected by the legal system through explicitly acknowledged property rights. Since the data that are under the control of a data holder are not similarly protected through the legislator by explicit property rights, a legal obligation for granting access to these data can be justified much easier from a legal perspective than in the cases of essential physical facilities or intellectual property. However, from an economic perspective also with regard to data the incentives for the production of data have to be taken into account.

---

[62] From an economic perspective, the requirement of a "new product" can be subsumed under the more general question, whether the granting of a license leads on balance to higher consumer welfare, and is therefore a part of the necessary overall balancing of benefits and costs of granting access to data (see next paragraph). See for an economic interpretation of the "new product test" Leveque (2005).

[63] See for a discussion of different options to solve this problem Crémer/de Montjoye/Schweitzer (2019, 104).

[64] This might be different for the refusal to give technical access to the car, as long as technical access solutions with a sufficient safety and security level do not exist, at least in the short-term. The question of the refusal to grant technical access to the connected car will be more broadly discussed below in the context of the interoperability issue.

Therefore also for data it is necessary to ask whether a mandatory access to data (or a more general data-sharing) would undermine the incentives of the manufacturers of the smart devices for producing the data. However the costs of producing data might be very different, from a nearly costless "harvesting" of data as a by-product of a service to perhaps in some cases expensive production of data (e.g. through specific sensors).[65] Therefore the balancing of the potential negative effects on the incentives for producing data and the manifold and potentially also large benefits of making data broadly available to other independent service providers can lead to very different results, and therefore can also often lead to the granting of data access for other independent service providers within this ecosystem of the smart device. Therefore from an economic perspective the essential facility doctrine can and should be applied with much more flexibility than in the case of physical facilities or IPRs.[66]

However this also depends very much on the type of data, to which access is sought. This is very clear for data, whose access can lead to a revealing of important business secrets of the car manufacturer (or one of its component suppliers). Since business secrets are protected against misappropriation by trade secrets law, this also has to be taken into account in such a balancing approach. Another type of data, for which the incentive problem might be very important, are "inferred data" or the results of data analytics. Here the balancing might lead less often or only in rare cases to the solution of granting access to these data. With regard to connected devices, it additionally has to be taken into account that the costs of producing data in connected devices (as the connected car) can also be covered already by the price that the users pay for the device (including its operation).[67] In this balancing approach it has also to be taken into account that the mandatory access that might be granted by Art. 102 TFEU is usually not without remuneration, i.e. the costs of producing and storing data as well as making them available for independent service providers can be covered by reasonable fees.[68] A particularly interesting criterion might also be to what extent other stakeholders in this ecosystem have participated in the production of the respective data. If either the data claimant or the user (owner) of the device have contributed to the production of these data (as, e.g. the car user by driving the car), then even the legitimacy of the exclusive control of the data by the manufacturer can be questioned, and it can be argued that also other stakeholders, esp. also the user of the connected device, should benefit from

65 See Kerber (2017, 119), Crémer/de Montjoye/Schweitzer (2019, 105)

66 See also very explicitly Schweitzer/Haucap/Kerber/Welker (2018, 171). The German report directly recommends that both the competition authorities and the courts should apply the essential facility doctrine with much more flexibility (esp. if the costs of producing data are low).

67 See also Crémer/de Montjoye/Schweitzer (2019, 105).

68 See for the principle of reasonable fees for the access to necessary repair and maintenance information (RMI) in the Motor Vehicle Type Approval Regulation Kerber/Gill (2019, 5).

these data.[69] This can also happen indirectly through the benefits of more competition and innovation on secondary markets. These and additional reasonings could be used for developing a consistent framework of criteria and effects that can be applied for the analysis in those refusal to grant access to data cases in Art. 102 TFEU.[70]

Whether such an analysis of the balancing of positive and negative effects of granting access to certain sets of data for independent service providers in such ecosystems is easier carried out through a greater flexibility within the well-established legal doctrine of access to "essential facilities" or more directly with a separate case group that uses an analysis of the effects and possible justifications of foreclosing behavior and leveraging of market power in such IoT ecosystems is a question of the most appropriate development of legal doctrine within Art. 102 TFEU. The above-mentioned recommendations in the German report and, still more explicitly, in the EU report for solving the problem in Art. 102 TFEU outside of the "essential facility doctrine" might be based upon the legal consideration that the necessary flexibility of this balancing of interests might be harder to achieve within the traditional "essential facility" doctrine.[71] From an economic perspective, such a balancing can also be done within the "essential facility" doctrine.

It should however be kept in mind that this analysis only refers to claims for access to data that are made by service providers who need this access for offering services, which are directly linked to the use of this connected device. This differs from other scenarios, in which firms might be interested into the access to these data for offering other products and services outside of these ecosystems or in respect to getting access to data for training algorithms or other AI applications. Although Art. 102 TFEU might also be offering a solution for these data access problems through such a balancing approach, these issues are beyond the scope of this paper.

Remedies

---

69 See for this criterion also Schweitzer/Haucap/Kerber/Welker (2018, 171). This is also directly linked to the discussion about rights on data, and especially the often discussed question who should get the benefits of the produced data. In the proposal of the EU Commission about a "data producer right", the owner or long-term user of the device should have gotten this exclusive right on these data. See EU Commission (2017a), and for a deeper analysis Kerber (2017) and Drexl (2018, 132). For the possibility that the exclusive control of the data is in itself the result of anticompetitive behavior of the data controller, see below section 3.3.2.

70 Such a balancing of interest approach is very close to the approach of balancing "legitimate interests" for defining and assigning non-waivable data access rights in Drexl (2018) as an alternative to this competition law solution.

71 See Schweitzer/Haucap/Kerber/Welker (2018, 172); Crémer/de Montjoye/Schweitzer (2019, 98).

An important question of any competition law solution with regard to the prohibition of abusive behavior refers to the problem of effective remedies. Although granting access to a certain set of data that is exclusively held by the manufacturer of a connected device seems to be a straightforward remedy, a number of probably sometimes difficult questions have to be solved. The problem of compliance with data protection law for personal data was already mentioned. It might not be a big problem in the case of a contract between the ISP and the car user.[72] A bigger problem might be that the data that are given access to have to be in a common format for being able to be processed by the independent service providers. This is a problem well-known in the data portability discussion, which however is solvable. In fact, in the motor vehicle type approval regulation the requirement of making necessary technical information and diagnostic data available in a common format for easy and fast access for independent service providers has been a well-established principle in this regulation for a long time. It can certainly also be part of an Art. 102 TFEU remedy. A particular important and difficult problem is the latency of the data access. For a number of aftermarket and complementary services in IoT contexts (and, in particular, also in the ecosystem of connected driving) it is necessary for independent service providers to have real-time access to technical or location data for offering remote services, as, e.g., remote monitoring of the car or navigation services to the car users. Granting real-time access to a data stream from connected devices might however require considerable technical preconditions in terms of interoperability (see also below).[73] A very important additional part of a remedy might be that for ensuring fair and undistorted competition on the secondary markets for IoT devices, it might often be necessary that this access should be made available in a non-discriminatory way to all independent service providers that would like to have access to the same type of data. This would lead to a FRAND-like solution for access to certain sets of (exclusively held) data of the manufacturer of the device. In this case also a specific regulatory solution might be sometimes a superior option.[74]

Particularly interesting is the question whether a remedy within Art. 102 TFEU could also encompass solutions that correspond to the “shared server” solution that is dis-

---

[72] It might be much more difficult in the case of the need for aggregated but not anonymised data. See again Crémer/de Montjoye/Schweitzer (2019, 104)

[73] See with regard to remote diagnostics and repair services in connected cars Kerber/Gill (2019, 15-17). Therefore it might be less clear whether a balancing of benefits and costs of granting access would lead to the granting of such a real-time access solution.

[74] See also Crémer/de Montjoye/Schweitzer (2019, 107). With regard to the example of the automobile industry we have already seen that such a (FRAND-like) non-discriminatory access regime to technical information and diagnostic data already exists in the current type approval regulation for protecting competition, innovation, and consumer choice on the aftermarkets for repair and maintenance services. See Kerber/Gill (2019) why this regulated access regime (even after its reform) cannot deal with all the challenges of the transition to connected cars for the automobile aftermarkets..

cussed in the connected car example. As already mentioned, in the “shared server” solution an entity (independent from the car manufacturer) would have exclusive control of the external server, to which all in-vehicle data are transmitted, and this independent entity could act as a data trustee who grants non-discriminatory access to these data to all independent service providers (including the car manufacturers) according to certain general principles.[75] It is widely acknowledged in the literature that this would solve many of the competition problems on the secondary markets, because the OEMs would lose their exclusive control of the in-vehicle data.[76] From a competition policy perspective, this can be seen as an unbundling solution, which certainly can be a remedy according to Art. 102 TFEU. Whether such a solution can be recommended in IoT contexts, depends again on an economic analysis of the benefits and problems of such a solution. In the case of data in connected cars, the results of the so far existing studies suggest that this might be a suitable solution of the competition problems (at least in the short-term), and therefore can also be a remedy in an Art. 102 TFEU case.[77] This solution however goes way beyond giving access to data, because it directly changes who has de facto control of the data (see below section 4.3).

The problem of closed ecosystems and lacking interoperability

In chapter 2 we have seen that data access problems in IoT contexts (and especially in our connected car example) often emerge in combination with problems of lacking interoperability. This can be at the level of the format of data, in which they should be made accessible. But often the provision of aftermarket and other complementary services with regard to connected devices might also require a direct technical access to the device for performing certain services (as, e.g., repair and maintenance services). If manufacturers have designed their device as closed systems, to which they have exclusive control, then they can foreclose all independent service providers who need this technical access for performing these complementary services to the users of this device. In the connected car example, this is, e.g., very relevant for the performance of remote services (as remote repair and maintenance services), which require that an ISP can also perform a remote repair service (e.g., through a software update) directly in the car, which so far is not possible, because the OEMs do not allow such a remote access

[75] These principles would also need to entail specific rules about a different treatment of different types of data, as, e.g. business secrets, personal data, as well as data, where incentives for data production play a particularly important role, i.e., that the criteria that are important for balancing the interests of the stakeholders would also have to be taken into account in such a solution.

[76] See Martens/Mueller-Langer (2018).

[77] However, a “shared server” solution does not solve the problem of technical access to the connected car (interoperability problem).

through independent service providers.[78] This problem can be very relevant for repair and maintenance services for all kinds of IoT devices.[79]

Can such a refusal to grant technical access to the connected device for performing services, e.g., through the lack of interoperability, also be an abusive behavior of a dominant firm according to Art. 102 TFEU? This problem can be discussed here only briefly and would need a much deeper analysis. However, impediments to such a "vertical interoperability" can be an abusive behavior of dominant firms.[80] Although in the public and academic discussion there is a wide-spread opinion that especially in the digital economy we should move much more into the direction of more interoperability and open standards, the economic analysis of these issues calls for more caution and the need for case-specific analyses of the benefits and costs of interoperability (see section 2). Although there can be no doubt that behavior that impedes (vertical) interoperability in the case of IoT ecosystems can be abusive behavior, this always requires a careful analysis of the costs and benefits.[81]

However in the case of connected cars the preliminary studies about the "extended vehicle" concept have not shown important benefits of such closed systems. The only and main argument of the car manufacturers, namely safety and security reasons, why such a closed system is necessary, is very controversially discussed among technical experts. Therefore it might not be easy for OEMs to justify their technically closed systems with its presumably significant negative effects on competition and innovation on secondary markets.[82] The main problem of using Art. 102 TFEU for solving these interoperability problems might be on the side of the remedies, because so far the alternative technical option of an open interoperable telematic system has not been sufficiently developed, and would require considerable investments and presumably a longer process of standardization. It is therefore very unclear whether manufacturers can be obliged via Art. 102 TFEU for developing open interoperable telematic platforms. It might however be possible to impose obligations on the OEMs to develop safety and security systems

---

[78] See Kerber/Gill (2019, 15), who also show that this problem is not solved by the recent reform of the type approval regulation.

[79] The problem of repair and maintenance services for connected devices and IoT ecosystems will emerge in many contexts. In the U.S., this is usually also discussed under the heading of "right to repair". See, e.g., Determan/Perens (2017, 29) and, in the context of the aftermarket discussion, OECD (2017, 39).

[80] See Kerber/Schweitzer (2017, 52). In the Microsoft case the refusal to grant access to interface information that was indispensable for competition on the downstream work group server market was seen as an abusive behavior of Microsoft, who was dominant on the market for operating systems.

[81] See for an overview (also on the economic discussion) Kerber/Schweitzer (2017, 52-54)

[82] On the contrary, the EU Commission promotes manifold industry-wide standardisation activities for its long-term objective of an integrated mobility system (EU Commission 2018a).

for the technical remote access to their connected cars, which allows independent service providers to perform certain services (as, e.g., remote repair and maintenance services) directly in the car.[83]

Conclusions

The discussion in this section 4.2.1 showed that the refusal of a manufacturer of a connected device to grant access to certain sets of data produced by the connected device and which are necessary for offering aftermarket and other complementary services to the users of the connected device can be an abusive behavior according to Art. 102 TFEU, leading to an obligation of granting access to these data. However, it is first necessary that the manufacturer is a dominant firm, at least for the separate markets for aftermarket and complementary services, which might require an analysis of the effectiveness of systems competition. Additionally, a comprehensive analysis of the benefits and costs of such an obligation for data access is necessary, whose outcome might also depend much on the specific sets of data for which data access is demanded. Particularly complex problems might arise with regard to the demand for real-time access to data as well as in those cases, in which interoperability with the connected device is necessary for performing aftermarket or other complementary services. However, one of the most important additional problems for solving data access problems in that way is that Art. 102 TFEU proceedings often take a long time. Therefore they can clarify the rules for the necessary conditions for access to certain sets of data in IoT contexts and suitable remedies only in a step-by-step process through a sequence of case decisions. This might be a cumbersome and a very costly process, which especially for small- and medium-sized firms might not offer a realistic perspective for solving their problems. In that respect, much of the scepticism in the literature about solving access problems in IoT contexts through Art. 102 TFEU is justified.[84] However, the analysis also showed that this provision might offer more possibilities for finding suitable solutions than previously thought. If competition authorities would try to develop with regard to certain IoT ecosystems precedent cases with appropriate remedies, and, e.g., also develop guidelines for helping to identify under what conditions the refusal to grant access to data can be abusive according to Art. 102 TFEU, the law of abuse of dominant firms might be flexible enough for developing new case groups, in which data access and data-sharing problems in IoT ecosystems might be solved, at least to some extent.[85]

---

[83] Such an obligation does already exist in the old (and new) type approval regulation with respect to the access to safety and security-relevant functions, but only at the premises of repair shops (and not for remote access). See in much more detail Kerber/Gill (2019, 14-16).

[84] See, in particular, Furman et al (2019, 55).

[85] For a discussion whether the German law of abuse of dominant firms (§ 19 GWB) should be amended in that respect, see Schweitzer/Haucap/Kerber/Welker (2018, 170).

4.2.2 Abusive behavior of firms with "relative market power" ("economic dependence")

Despite our result in the last section that data access problems in IoT ecosystems might be solved through the control of abusive behavior of dominant firms, it is not clear whether the application of Art. 102 TFEU will be as flexible as it would be necessary, and whether some of the problems, especially with regard to proving dominance and the definition of separate markets for aftermarket and other complementary services within an ecosystem, can be overcome in a sufficient way. Therefore also with regard to IoT ecosystems it can be discussed whether it might be necessary to control abusive behavior of firms in the digital economy also below the threshold of market dominance.[86] In the already mentioned consultation of the EU Commission about the Communication "Building a European data economy", many concerns were raised that often firms, particularly small and medium-sized enterprises, have large difficulties for getting access to data in "unequal bargaining power" situations between firms. Therefore the EU Commission claimed "unequal bargaining power" as one of the main problems for insufficient access to data.[87] Although problems through "unequal bargaining power" situations between firms can be attempted to solve also in the law of "Unfair Trading Practices", situations that one firm is bilaterally dependent from another firm (without the latter being a dominant firm) can also be addressed in a number of competition law regimes. In German competition law the concept of so-called "relative market power" can be found in § 20 (1) GWB. According to this provision a firm with "relative market power" is not allowed to abuse its power vis-à-vis small or medium-sized companies, which are bilaterally dependent from this firm, because they do not have sufficient and reasonable possibilities for switching to other firms[88] (outside options).[89] In the recent policy discussion about the challenges of the digital economy, the German report about "Modernising the law of abuse of firms with market power" recommended to use this provision

---

[86] For a discussion about the question of a general lowering of the threshold for antitrust intervention below market dominance see Schweitzer/Haucap/Kerber/Welker (2018, 54-76). This is not discussed in the EU report (Crémer/de Montjoye/Schweitzer 2019).

[87] See EU Commission (2017a, 10-12); for a critical discussion Kerber (2017, 124-128).

[88] § 20 (1) GWB: "§ 19 (1) in conjunction with paragraph 2 no. 1 [prohibition of abusive behavior by dominant firms, WK] shall also apply to undertakings and associations of undertakings to the extent that small or medium-sized enterprises as suppliers or purchasers of a certain type of goods or commercial services depend on them in such a way that sufficient and reasonable possibilities of switching to other undertakings do not exist (relative market power)." (English translation of the German legal text; available at: http://www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf).

[89] For a general analysis of this provision see Nothdurft (2015, 2018); for a brief overview see Schweitzer/Haucap/Kerber/Welker (2018, 63-70).

much more actively for helping firms that are dependent on specific platforms (P2B-problems) or have problems of getting access to data from other firms.[90]

The basic idea of the German concept of "relative market power" is that firms can also have "market power" vis-a-vis certain dependent firms below the threshold of market dominance, which they can use for unreasonably foreclosing these firms or treating them differently without justification. This provision does not only protect firms in "unequal bargaining power" situations against abusive behavior but also protects the competitive process.[91] In German competition law it is explicitly seen as an extension of the prohibition of abusive behavior of dominant firms below the threshold of market dominance,[92] but this protection is so far limited to small and medium-sized firms which are dependent on another firm, who then is deemed to have "relative market power". Such an additional control of abusive behavior based upon bilateral dependency of firms does not exist in EU competition law, but can also be found in a number of other countries as, e.g., France and Japan.[93]

From an economic perspective the concept of bilateral "economic dependence" is a difficult and perhaps dangerous (i.e., potentially overinclusive) concept, because in competition processes situations, in which one of the involved firms seems to be very dependent on another firm due to the lack of close (and therefore satisfactory) options to switch to another buyer or seller, can emerge in many normal negotiation processes between firms on markets, without being abusive behavior or a problem for competition. Therefore the application of such a concept requires a cautious and clear approach, under what conditions a problematic "unequal bargaining power" situation can be identified, and what the criteria are for assessing a certain behavior as abusive.[94] Although the analysis of bilateral bargaining situations is a topic of research in economics, com-

---

[90] See Schweitzer/Haucap/Kerber/Welker (2018, 64). In the Furman report it is explicitly mentioned that "economic dependence" and "relative market power" can be considered as aspects of market power that might be important for determining whether a company holds a "strategic market status", which then is subjected to the regulatory powers of the proposed "digital market unit" (Furman et al 2019, 81).

[91] See Schweitzer/Haucap/Kerber/Welker (2018, 65); this provision is not meant for protection against pure exploitative abuse (see Nothdurft, 2015, 8).

[92] The German rules about the prohibition of abusive behavior of dominant firms can be found in § 19 GWB, and § 20 (1) explicitly refers to the general prohibition of § 19 (1) and (2) S.1 GWB (see fn.86).

[93] See for an analysis of the dependence concept and its interpretation in different competition law regimes, Lee/Schißler (2019).

[94] For the analysis of "unequal bargaining power" situations in the context of the buying power discussion and under what conditions an abusive behavior in situations with "relative market power" (§ 20 (1) GWB: formerly: § 26 (2) S.2) can be identified, see Kerber (1989, 489 – 505, 523-549).

petition economics has so far been reluctant in addressing these issues in a competition policy setting. The main opinion in competition economics is that relevant problems only exist, if a firm has a traditional market power position on a specific market, which is supposed to be analysed as a question of market dominance. There are however two notable exceptions in the economic competition policy discussion, where bilateral bargaining power plays an important role. One is the discussion about buying power, where it is broadly accepted that bilateral bargaining power plays a crucial role and where outside options have to be analyzed also in competition cases.[95] The second exception are cases, in which bilateral hold-up problems between firms lead to an "unequal bargaining power" situation. This concept was introduced in economics by Williamson in his transaction costs approach, in which one firm can be bilaterally dependent on another due to transaction-specific investments (with sunk costs) for the other firm.[96] In the meantime, this hold up-concept has been used in many other contexts, as, e.g., standard-essential patents, and it is suggested here that it also can play an important role with regard to data access problems in IoT contexts.

For a better understanding of the German provision about abusive behavior of firms with "relative market power", a brief overview about the currently existing case groups might be helpful.[97] A first important case group ("sortimentsbedingte Abhängigkeit") refers to the problem that retailers in their competition vis-à-vis the consumers might be dependent on having certain strong brands in their range of products, leading to a bilateral dependence from those firms with very strong brands,[98] and a refusal to supply might be deemed as an abusive exclusionary behavior.[99] Directly related to Williamson's "transaction-specific investment" reasoning is the case group of a firm-specific dependency ("unternehmensbedingte Abhängigkeit"), in which one firm has invested specifically into the relationship with another firm (as, e.g., in cases of "authorised dealerships"), and therefore can be seen as bilaterally dependent from the other firm after this investment ("lock-in" situation).[100] The third important case group are "buying power-related dependencies", in which, e.g., suppliers might be bilaterally dependent on large retail chains, because the latter might have a "gatekeeper position" to a large group of customers and/or buy a large share of the production of the supplier. Both reasons might give the retail chain a large bilateral bargaining power vis-à-vis this supplier. The abu-

95 See for the relevance of bilateral bargaining approaches for the analysis of buying power Inderst/Mazzarotto (2006).

96 See Williamson (1979) and Kerber (1989, 137).

97 See for a broad analysis and overview of court decisions Nothdurft (2015, 31-74); for a brief overview Schweitzer/Haucap/Kerber/Welker (2018, 66-70.)

98 This is called „Spitzenstellungs- und Spitzengruppenabhängigkeit".

99 See Nothdurft (2015, 36-43).

100 See Nothdurft (2015, 44-49).

sive behavior refers usually to “excessive” demands for rebates or other favorable conditions for the buyer.[101] [102] All of these case groups are well-established and broadly accepted as a useful complement to the rules against abusive behavior of dominant firms. The broad acceptance of this provision of § 20 (1) GWB in Germany might be explained by its careful and cautious application in German competition law.

In the following, it will be discussed whether this concept and the German provision of § 20 (1) GWB can be used for solving data access problems. First it has to be emphasized that so far there have been no cases with applications to the new challenges of the digital economy (as, e.g. to platforms) or to the problem of data access. Again, it is focused on data access problems in IoT contexts, in which the manufacturer of an IoT device (as, e.g., the car manufacturer) has exclusive control of the access to the data (and to the connected device). Particularly important is the question whether this concept can close gaps that might be difficult to solve with Art. 102 TFEU (or § 19 GWB as the German prohibition of abusive behavior of dominant firms). The first clear advantage of § 20 (1) GWB is that the manufacturer of the device as data holder need not be deemed as dominant according to Art. 102 TFEU (or § 18 GWB in German competition law), i.e. it is not necessary to analyze the effectiveness of systems competition between the manufacturers for deciding whether separate markets for aftermarket and other complementary services within the ecosystem exist. The relationship between independent service providers, who would like to have access to data for being able to compete on these secondary markets within the ecosystem, and the manufacturer who has exclusive control of these data can be much more directly investigated. One possibility is that the independent service providers are already bilaterally dependent on this manufacturer, because they have made firm-specific investments for providing these services in this ecosystem. Then such a case would directly fit into the existing case group of “firm-specific dependence”. This might be relevant for repair and maintenance service providers who have specialized themselves for providing services on the secondary markets for connected devices (primary products) of certain manufacturers. Similarly to the problem of getting access to brand-specific spare parts as a precondition for offering certain repair and other services,[103] specific sets of data might be deemed as

[101] See Nothdurft (2015, 49-54). This group is also important in the new discussion about B2P-problems between dealers and online platforms, from which they can be bilaterally dependent. See for solving these problems with § 20 (1) GWB Schweitzer/Haucap/Kerber/Welker (2018, 94).

[102] There is a fourth case group (“mangelbedingte Abhängigkeit”), which was only important in the oil crisis in the 1970s.

[103] See, e.g., the decision of the German Bundesgerichtshof “Porsche-Tuning” (BGH, 6.10.2015, KZR 87/13), and Schweitzer/Haucap/Kerber/Welker (2018, 177-180).

necessary for offering these services, and the refusal to grant access to them might be a prohibited abusive behavior of this manufacturer with “relative market power”.[104]

However, in many cases the independent service providers in these ecosystems might not fit directly into this case group, because they have not invested in a firm-specific way for this manufacturer.[105] One way of solving this problem is to develop a broader interpretation of this case group. Another perhaps more consequent option is to develop within this provision of § 20 (1) GWB a new case group, which encompasses directly all those cases, in which one firm (usually the manufacturer), who controls exclusively the access to the data produced by a connected device, might abuse its “relative market power” vis-à-vis other firms, who need these data for offering products or services to the users of this device (and are therefore “dependent”), if it does not grant access to these data. Again, it is the fact that the manufacturer with its exclusive control of the data is a gatekeeper for the independent service providers to the secondary markets of these ecosystems that makes the independent service providers bilaterally dependent on this exclusive holder of data. This can be characterized as a hold up-situation, which can be exploited by the firm with the gatekeeper position. The dependency is therefore determined by the exclusive control of certain sets of data (“data dependency”). Again it is an important precondition of the dependency of an ISP that these data cannot be acquired via other channels, and that they are non-substitutable for providing these services, because otherwise there would be sufficient and reasonable alternative options.

For our example of connected cars this would imply that independent service providers that would like to offer aftermarket or other services in the ecosystem of connected cars, for which they need access to certain sets of data, can be seen as dependent from the OEMs with their exclusive control of the data, and might therefore claim access to these data based upon this new case group (data dependency) in § 20 (1) GWB. From an economic perspective it is also no problem to extend this kind of dependency concept also to those cases, in which an ISP needs technical access to the connected device itself for performing certain services, as, e.g. remote repair services, as we have discussed it also with regard to Art. 102 TFEU (interoperability problem).[106]

In a similar way as in the case of market dominance, also in cases of “relative market power” the question, whether a refusal to grant access to a certain set of data is abusive, requires a comprehensive balancing of benefits and costs of granting data access.

---

[104] The case group of “firm-specific dependency” might also fit for the data access problems of farmers vis-a-vis the manufacturers of smart farm machinery.

[105] It has additionally to be taken into account that the case group of firm-specific dependency might only grant a time-limited protection due to the limited duration of a firm-specific investment.

[106] However the term “data dependency” would not fit any more for these cases.

Again, as in the previous section, we focus here entirely on those cases, in which one firm (as usually the manufacturer of a connected device) controls exclusively the access to the data of this device or the access to a digital ecosystem, and independent firms would like to offer their products and services on secondary markets within this ecosystem, and need access to the data or the connected device.[107] As in the case of balancing in the Art. 102 TFEU cases, it is also here very important to distinguish between different types of data, because the legitimate interests, e.g. with regard to personal data and business secrets, as well as the conditions, costs, and incentives for producing, storing, and processing of the data in these connected devices might be very different. At the same time, also the value of the additional services that might be created within this ecosystem through innovative new services for the users of the connected device can be taken into account as well as the positive effects of more competition on these secondary markets. Again it might be a relevant criterion whether and to what extent other stakeholders in this ecosystem (and especially also the users of the connected device) have participated in the production of the respective data. All of these considerations can and should be taken into account in such a balancing for determining whether a refusal is an "unfair impediment" ("unbillige Behinderung") and therefore a prohibited abusive behavior according to § 20 (1) GWB. Without being able here to discuss this in detail, the so far existing results of the analysis of the data access problems in the connected car example would suggest that this balancing of benefits and costs of mandating data access for independent service providers would also offer good chances for claiming access to data from OEMs according to § 20 (1) GWB.[108]

The main advantages compared to Art. 102 TFEU lie in not needing to prove dominance, the existence of separate secondary markets,[109] as well as avoiding the uncertainty about the necessary high flexibility in the application of Art. 102 TFEU for solving these data access problems. It cannot be excluded that with a sufficiently large flexibility (and creativity) in the application of Art. 102 TFEU (or § 19 GWB), it might not be necessary to use this concept of "relative market power" for solving the data governance problems of digital ecosystems in IoT contexts. But it is highly speculative whether such a legal development within the Art. 102 TFEU will happen in the future. Therefore it can be recommended to use additionally this concept of "relative market power", e.g. the

[107] We do not focus on other cases, in which firms outside the ecosystem would like to have access to these data for offering products and services unrelated to these connected devices and ecosystems.

[108] Of course, also here the questions of reasonable fees for data access as well as compliance with the GDPR as a precondition in the case of personal data have to be solved.

[109] Is it a problem that in § 20 (1) GWB no filter is used with regard to the effectiveness of systems competition? This need not be a problem, because if systems competition works well enough, then no significant positive effects of granting access to data can be expected in the "balancing" part of the application of this provision.

provision of § 20 (1) GWB of German competition law, for solving data access problems in IoT contexts. This can be done in Germany to some extent by using the already existing case group of "firm-specific dependency" but would primarily require also the development of new case groups, as, e.g., a new case group about "data dependency". The development of such a new case group will need time, in which in a step-by-step process the conditions and criteria both for data dependency and for the abusive behavior have to be clarified. However, for this specific group of data problems in IoT ecosystems with competition problems on secondary markets, the academic discussion is, in the meantime, far enough developed for allowing the drafting of a consistent framework with clear assessment criteria, although this might still need more experience and research.

Introducing new case groups in § 20 (1) GWB of German competition law might not be easy. Therefore it should not be relied on private litigation through small- and medium-sized companies for initiating new precedent cases for enforcing access to data in IoT contexts, because this might be too difficult, risky, and costly for these firms. Therefore the German report on "Modernising the law of abuse of market power" recommends (for the planned 10th amendment of German competition law) a much broader approach for activating this old and well-established provision of German competition law in that respect. First, it recommends, also in respect to P2B problems on platform markets (as, e.g., Amazon), that in § 20 (1) GWB the limitation of the protection to small- and medium-sized firms should be abolished, because also larger firms can be dependent on platforms or on certain sets of data. This step would also strengthen generally the importance of § 20 (1) GWB in the German competition law regime.[110] Secondly, due to the difficulties of interpreting § 20 (1) GWB and to help triggering a more active application to data access problems in these IoT contexts the report also recommends to clarify with an addition to § 20 (1) GWB "that a relevant form of dependency may also result from an undertaking being dependent, in order to achieve a substantial value creation within a value creation network, on access to automatically generated machine or service usage data that is exclusively controlled by another company; and denial of access to data can constitute an unreasonable exclusionary conduct, even if markets for such data do not yet exist."[111] Such or a similar addition to § 20 (1) GWB by the German

[110] See Schweitzer/Haucap/Kerber/Welker (2018, 73-76). Additionally, such specific protections of SMEs in competition law are seen today generally hard to defend and outdated (see also Nothdurft, 2015, 54-62).

[111] Schweitzer/Haucap/Kerber/Welker (2018, executive summary, 6); the term "value creation network" was chosen as a more general technical term instead of IoT ecosystems. The specific emphasis on the last part that dependence can also exist, if markets for such data do not exist so far, refers to a specific requirement of the German Bundesgerichtshof in former court decisions about access to input resources in § 20 (1) GWB, which stipulated that the input resource, to which a third-party claimant wants access, should be "normally accessible" in market transactions ("üblicherweise zugänglicher Geschäftsverkehr"), which is usually not the case for these

legislator might help considerably to trigger new cases for access to data in IoT contexts and digital ecosystems that can lead to new case groups.[112] In addition to these legislative amendments for facilitating data access solutions via the concept of "relative market power" in German competition law, it can also be recommended that the German Bundeskartellamt develops an active policy for applying § 20 (1) GWB in cases of refusal to grant access to data in digital ecosystems. This can also include guidelines about principles and criteria for dependency and the balancing of benefits and costs of data access and data-sharing in such case groups.

In Germany § 20 (1) GWB might therefore provide additional options for solving data access problems in IoT ecosystems, especially in the case of an appropriate amendment of this provision by the German legislator. It is not possible here to discuss the question whether similar solutions are possible in other EU Member States as, e.g., in France, where also specific provisions about bilateral "dependencies" between firms exist, or whether also the European law on unfair trade practices can be used in that respect, because it also tries to deal with "unequal bargaining power" situations.[113]

4.3. Preventing the exclusive control of data through competition law

4.3.1 Overview

The analyses in the last section 4.2 have shown that general competition law provisions about abusive behavior of firms with market power can offer much more possibilities to solve access to data and interoperability problems than commonly thought. This does not imply that these provisions are the best way of solving these problems. What other competition law provisions can be used for dealing with these problems of data access and interoperability within IoT ecosystems? In the previous section, it was always assumed that one firm has exclusive control of the data and the technical access to the connected device, and the question was about how other stakeholders in this ecosystems can get access to the data from this firm. However, it also can be asked whether competition law can also be used for preventing that one firm gets into such a position of exclusive control of certain data sets. Under what conditions can the obtaining of such an exclusive control be the result of anticompetitive behavior and therefore a violation of competition law? It is not possible here to provide a comprehensive discussion of this issue. Therefore section 4.3 will encompass only a brief overview and, additionally,

---

sets of exclusively held data in these IoT ecosystems (see Schweitzer/Haucap/Kerber/Welker 2018, 191).

[112] The German Ministry of Economic Affairs and Energy is right now preparing a proposal for the 10th amendment of German competition law.

[113] See for the latter also Lee/Schißler (2019).

a preliminary analysis of a case study, namely the question whether the "extended vehicle" concept of the car manufacturers can itself be viewed as an anticompetitive horizontal agreement that restricts competition with regard to technological innovation and data governance.

One possibility how firms could get exclusive control of certain sets of data and of IoT ecosystems are mergers, i.e. that a merger (e.g., by combining the data sets of these firms) can lead to a monopolistic position with regard to certain non-replicable or substitutable sets of data. This is a question, which has already been investigated as part of merger reviews. In that respect, merger control can be (and in fact is already) used for preventing the emergence of exclusive monopolistic control of data sets that can lead to impeding competition on other (up/downstream or adjacent) markets.[114] Another much larger case group refers to all kinds of unilateral strategies of firms with market power to foreclose other firms for acquiring access to certain kinds of data, which might help them to defend their exclusive control. This can encompass well-known strategies as bundling strategies, exclusivity agreements or other predatory strategies that makes it harder or even impossible for others to get access to certain kinds of data. As far as these firms are dominant, these strategies might be abusive behavior according to Art. 102 TFEU. Another group of strategies might refer to the exclusive technical control of IoT ecosystems in terms of impeding interoperability and openness of IoT ecosystems. Also the question whether and to what extent manufacturers of connected devices should be allowed to design technically closed ecosystems that grants them exclusive technical control and makes interoperability impossible can be seen as a strategy that can be subject to the law of abuse of market power (as this has already been discussed to some extent in section 4.2.2). Also additional obstructive strategies with regard to interoperability, with which a manufacturer of a device tries to impede unilateral solutions by other firms for achieving interoperability (as, e.g., through adapters) can be an abusive behavior according to Art. 102 TFEU.[115] This can be relevant for strategies of car manufacturers in the ecosystem of connected driving but also with regard to technological decisions of manufacturers of many other connected devices in IoT contexts.

A third group of cases refers to the possibilities to use horizontal or vertical agreements between firms for either gaining exclusive control of data or for helping to defend such an exclusive position (Art. 101 TFEU). In that respect many kinds of strategies might be possible. In the following, this article will focus only on one strategy, namely horizontal agreements between manufacturers of connected devices about technological and con-

[114] See, e.g., Graef (2015), and Kadar/Bogdan (2017).

[115] A very interesting way of solving interoperability problems might be the unilateral development of so-called adapters (or converters) by independent service providers. For these strategies see Farrell/Simcoe (2012, 46). See with regard to all these strategies from a competition law perspective Kerber/Schweitzer (2017, 54-56).

tractual decisions that restrict competition between these firms in order to help them to obtain or defend such exclusive gatekeeper positions with regard to the ecosystems of the devices and the data. This can refer to technological collusion (closed systems / lacking interoperability) but also collusions about the governance of the data, e.g. with the contractual relationships with the consumers as the owners of these devices, or the conditions for allowing other firms access to these exclusively held data. In the next section 4.3.2 we will therefore ask – as a case study - whether the "extended vehicle" concept of the car manufacturers can be seen itself as an anticompetitive collusive behavior with regard to technological decisions and data governance, which might violate Art. 101 TFEU. But similar questions can also be raised with regard to many other connected devices as, e.g., smart farm machinery or smart TVs. This is an issue that also can touch standardisation questions and new discussions about data pools and data-sharing agreements.

4.3.2 Case study: Is the "extended vehicle" concept an anticompetitive horizontal agreement between OEMs in the automobile industry?

In the EU horizontal agreements between competitors are generally prohibited (Art. 101 (1) TFEU), but can be exempted according to Art. 101 (3) TFEU, if certain conditions are fulfilled. This provision about horizontal agreements does not only refer to price collusion but also to agreements about technology as well as contractual conditions. The relevance of Art. 101 TFEU for technological decisions also in the automobile industry has recently been emphasized by the investigation of the EU Commission about technological collusion between German car manufacturers with regard to emission cleaning technology.[116] The argument in this case was that the technological collusion has impeded competition between car manufacturers with regard to reducing emissions and innovation. In the following, it will be asked (1) whether the extended vehicle concept itself can be seen as an anticompetitive horizontal agreement between car manufacturers, and (2) whether such an agreement might fulfill the criteria for an exemption. In that respect, also the Guidelines about the horizontal co-operation agreements have to be considered (EU Commission 2011). As to my knowledge, this question has not emerged so far in the discussion about access to data in connected cars.[117] In this subsection this question can only be analyzed in a limited, brief, and preliminary way, partly due to limited space but partly also due to the need for thorough investigations about the behavior of the OEMs.[118]

---

[116] See the investigation of the EU Commission against German car manufacturers with regard to emission cleaning technology (EU Commission 2019).

[117] See briefly Kerber (2018, 324, 329).

[118] This can only be done by a competition authority.

The “extended vehicle” concept was developed by European car manufacturers and has been for several years the official approach of the European automobile industry how to deal with the problem of the “access to in-vehicle data and resources”. The European and the German association of car manufacturers have published detailed position papers about the “extended vehicle” (ACEA 2016a, 2016b; VDA 2016) and are defending it in the recent policy discussions about access to in-vehicle data.[119] As far as the European car manufacturers are already offering connected cars, they use the basic principles of the extended vehicle concept, although the exact extent of its application should be subject to a more thorough investigation. As far as the car manufacturers stick to this joint concept of the “extended vehicle”, it can be seen as a horizontal agreement between competitors. As already described in section 3, the basic principles of this concept are that the OEMs have exclusive technical access to the car, and have exclusive control of the in-vehicle data through transmitting all in-vehicle data to proprietary servers of the OEMs, leading to a de facto appropriation of these data and their value. Beyond these basic principles, the concept also entails a number of rules about additional aspects of the governance of these in-vehicle data, esp. with regard to their access and commercialisation. This encompasses, on the one hand, agreements about the exceptions with regard to access to these data, e.g., for public authorities, for repair and maintenance services (as required by the type approval regulation), and about the protection of personal data (according to the GDPR). These rules however also encompass principles about the commercialisation of in-vehicle data (as, e.g., anonymised sets of in-vehicle data), the classification of data, and the principle that access to in-vehicle data for independent service providers is only possible by using freely negotiated B2B arrangements.[120]

To what extent can horizontal agreements between OEMs about these principles restrict competition between car manufacturers in the ecosystem of connected cars? The policy discussion, esp. in the C-ITS platform discussion (C-ITS 2016) about “access to in-vehicle data and resources” has shown clearly that different technological design options besides the extended vehicle concept (with its “external server” solution) exist. In the ensuing discussion it became increasingly clear that the main alternative technological solution of the on-board application platform (as an open interoperable telematics platform), which allows the storage of the data in the car and a direct choice of the car owners whom they want to give access to these data, might be a superior technological solution, esp. also with regard to competition and innovation within the ecosystem of connected cars.[121] This alternative concept has the advantage that it does not lead

[119] See ACEA (2016a, 2016b), VDA (2016).

[120] See ACEA (2016a, 2016b), VDA (2016).

[121] See section 2.2, and esp. also the results of the TRL study (2017) that was commissioned by the EU Commission.

directly to an exclusive control of the in-vehicle data by the OEMs. In addition, an open interoperable telematics platform combined with a sophisticated multi-layered safety and security system would also allow the direct access of independent service providers to the connected car, allowing the car users to choose freely between all service providers (that fulfill the requirements of a safety and security certification). With the agreement on the extended vehicle concept the car manufacturers might have restricted technological and innovation competition, because they jointly reject to pursue other technological solutions, as, e.g. the development of open interoperable telematic platforms, which might lead to less consumer harm. Therefore it also can be interpreted as a horizontal agreement about jointly choosing closed ecosystems for connected driving with locked-in consumers and without interoperability, which deprives the consumers from choosing between more open and more closed ecosystems of connected driving.

However the collusion might also extend to their behavior with regard to the governance of the data. Most important is that the horizontal agreement about the extended vehicle concept also leads to the result that each of the car manufacturer obtains exclusive ("monopolistic") control of the in-vehicle data and can de facto "appropriate" the value of these data (through their commercialisation). The "extended vehicle" concept therefore might eliminate also competition between OEMs with regard to the governance of the data, because all OEMs use the same basic design of data governance, and the car owners have no possibility to choose between different ones. It is subject to deeper investigations to what extent the "extended vehicle" concept does also lead to a collusion about the specific contractual terms and conditions between OEMs and the car owners, especially also with regard to giving consent to the use of in-vehicle data (including personal data according to the GDPR).[122]

Therefore a preliminary assessment leads to the result that the "extended vehicle" concept might be viewed as a horizontal agreement between the OEMs that can impede their competition and innovation with regard to the technological design and the governance of the data that are collected and produced in the connected car. The expected negative effects on competition and innovation within the ecosystem of connected driving as well as "lock-in" of consumers and reduction of consumer choice, have been discussed earlier. The next important assessment step is whether the extended vehicle concept can fulfill the requirements for an exemption according to Art. 101 (3) TFEU. Most important for this question is what the benefits of these agreements in terms of

[122] Especially interesting in that respect is the question, whether and to what extent the OEMs might have agreed on the same rules about the granularity of the decisions of car users for giving consent to the processing and use of personal data. See for the problem of car owners whether they have to give a general all-or-nothing permission or can decide in a more "granular" way, whether they give consent to the use of what kinds of data and for what purposes Specht/Kerber (2019, 189-191) as well as the first C-ITS guiding principle about consent of the data subjects in the connected car (C-ITS 2016, 75).

advantages for efficiency or innovation are, and whether these restrictions of competition are necessary for achieving these benefits. In the following, we only can offer some preliminary reasonings from an economic perspective, why there might be serious doubts that these conditions are fulfilled in this case. A thorough analysis would require to take into account the EU Guidelines on horizontal co-operation agreements (EU Commission 2011), and here especially also the rules about standardisation agreements, because there are also standard-setting processes with regard to the “extended vehicle” concept (ISO 20077, 20078). Since these standard-setting processes can be intransparent and opaque, it is necessary to investigate also thoroughly about the contents of these standardisation processes, and whether are not misused for restricting competition.[123]

From an economic perspective it is very unclear what the benefits of such a horizontal agreement between OEMs for efficiency and innovation might be. The main argument of the OEMs for defending the extended vehicle concept has always been the need for maximum safety and security of the vehicle. However we have already seen that this claim of the OEMs is heavily disputed by technological experts and is therefore presumably not sufficient for fulfilling the criterion of contributing to efficiency and innovation. More important is that even if this claim were true, it is not clear at all why a horizontal agreement between the OEMs is necessary for achieving this level of safety and security. Therefore from a competition and a consumer welfare perspective, it would be preferable that car manufacturers decide independently and in competition with each other about the extent of the closedness or openness of their brand-specific ecosystem and/or whether it might be better to participate into the development of open, interoperable telematics systems and the necessary safety and security solutions. Since there are also good arguments that the proprietary closed ecosystems of the OEMs, which follow from the application of the extended vehicle concept, might not be future-proof in the upcoming transition to an integrated mobility system in the automobile sector with its need for direct V2X communication, it can even be argued that a technological collusion that favors the extended vehicle concept might be in the medium and long term detrimental for innovation in the automobile sector.

The other important question is whether the agreement on the second important element of the extended vehicle concept, i.e. the exclusive control of the in-vehicle data, which leads to the de facto appropriation of these data by the OEMs and their ability for their free commercialisation, has any benefits for efficiency and innovation. So far the OEMs have not put forward any specific argument about the benefits of their exclusive control of these data in terms of efficiency and innovation from a social welfare perspec-

[123] See for more information <https://www.iso.org/standard/66978. html>, TRL (2017, 46), and from a broader perspective Kerber/Gill (2019, 17-20).

tive.[124] It was already shown that safety and security arguments cannot be used for justifying the de facto appropriation of these data by the OEMs (see above section 3). One possible line of reasoning from the new discussions about data economy and data-sharing would be that the transmitting of all in-vehicle data to their servers can lead to advantages due to the aggregation of these data on their brand-specific servers, e.g. for data analytics, AI applications, and training algorithms. It is one of the important new insights of the economics of data that the aggregation of data in larger data pools can increase the quality of data analytics results and can lead to more efficiency and innovation. This argument however does not support the brand-specific proprietary data silos which are the consequence of the extended vehicle concept. This reasoning rather leads to very different data governance solutions, which emphasize the sharing of these data for many other interested parties. From that perspective, it would be more interesting to develop concepts of data pooling and data-sharing agreements that encompass the in-vehicle data from all car manufacturers, but this is not the approach of the "extended vehicle" concept.

4.3.3 Conclusions

The question whether the "extended vehicle" concept of the car manufacturers in Europe is itself an (non-exemptible) anticompetitive collusion about technology and data governance according to Art. 101 TFEU cannot be answered here thoroughly. However, the above presented preliminary reasonings justify the raising serious concerns, which might warrant competition authorities for taking a deeper look into this matter. The objective of this subsection, however, is to raise generally the awareness that impediments to competition and innovation through the exclusive control of non-replicable and non-substitutable data sets in IoT ecosystems can also be the result of horizontal collusion between the manufacturers of connected devices, both with regard to technological decisions and decisions about the governance of data. In that respect, also other connected devices and ecosystems should be analysed from this perspective.

The advantage of applying Art. 101 TFEU on such questions is that this provision allows competition authorities to develop criteria and lay down more specific rules for the exemption of these agreements according to Art. 101 (3) TFEU, either through guidelines or even the initiation of block exemption regulations. In this context also the innovative analysis in the EU report about the efficiencies and competition concerns of data pools and data-sharing agreements are very interesting.[125] A different institutional approach

[124] In ACEA (2016b) reasonings of car manufacturers can be found that might be interpreted as industrial policy arguments with regard to their "competition" with the large US tech firms. See Specht/Kerber (2018, 179).

[125] See for the efficiencies and competition concerns of data pools Crémer/de Montjoye/Schweitzer (2019, 92-98).

has been proposed in the UK report, in which the new proposed “digital market unit” could develop in cooperation with the stakeholders (here: OEMs and independent service providers) solutions about technological and data governance problems, with the explicit option of mandatory regulatory solutions if voluntary solutions fail.[126] A further option would be direct sector-specific solutions along the lines of the PSD2-Directive, which wants to help Fintech companies to enter the market for digital payment services by implementing a far-reaching regulatory solution for opening the access to bank account data (“Open Banking”). This however already leads to the broader discussion of other solutions outside of competition law.

5. Conclusions and Perspectives

This article has dealt with the data access and data-sharing problems that emerge in many IoT contexts, in which connected devices are generating huge amounts of data that are often under the exclusive control of one firm, usually the manufacturers of the devices. Through the exclusive control of these data and often also of the technical access to these connected devices through the design of closed systems, one firm can control entire ecosystems with many complementary services that need either access to these data or technical access to the connected devices for offering their services. This can lead to an impediment of competition on these secondary markets with less competition, innovation, and consumer choice. But such IoT ecosystems can also lead to an under-utilization of these data and inefficient technological decisions about the optimal level of interoperability and standardisation. After having presented an overview in section 2 about the basic economic reasonings that are relevant for such IoT ecosystems, the example of connected cars with the unsolved problems of “access to in-vehicle data and resources” were analyzed in section 3. It was shown that the application of the “extended vehicle” concept leads to the exclusive control and therefore the monopolistic gatekeeper position of the car manufacturers allowing them to foreclose independent service providers and control the secondary markets in the ecosystem of connected driving. The connected car example also shows that alternative technological solutions, as open interoperable telematic systems, are possible and presumably superior (due to fewer problems for competition and innovation on these secondary markets) but might need regulatory solutions for their implementation. Therefore connected cars are also a good example for the necessity of solving both data access/sharing and interoperability problems.

The main focus of this article was on the question whether and to what extent general competition law can help to solve these data access and interoperability problems in IoT

126 See Furman (2019, 64-82).

ecosystems. With regard to the possibility to solve data access problems for independent service providers through the control of abusive behavior of firms with market power, it is an important result that the refusal to grant access to exclusively held data by a manufacturer of a connected device (as, e.g., the OEMs in the connected car example) can be an abusive behavior of a dominant firm. Proving separate markets for aftermarket or other complementary services in an ecosystem might not be an easy task, and, in any case, also a comprehensive balancing of benefits and costs of such a data access is necessary, which might also lead to different results for different types of data. In addition, compliance with GDPR is always necessary. However, the scope for granting access to data via Art. 102 TFEU seems to be much larger than in the traditional "essential facility" cases with access to physical facilities or IPRs. Presumably still more possibilities exist, if the control of abusive behavior is extended to situations, in which one firm is dependent from another, as in the concept of "relative market power" (§ 20 (1) GWB in German competition law). Especially an amendment of this provision through the German legislator could facilitate the solving of data access problems of independent service providers in IoT ecosystems. Another approach of solving data access and data-sharing problems in IoT ecosystems would more directly challenge the position of exclusive control of data through the manufacturers by asking such a position can itself be the result of anticompetitive behavior. Merger control, the control of abusive behavior for foreclosing other firms from acquiring data or obstructing interoperability, as well as the challenging of horizontal collusive behavior about technological and data governance decisions are instruments than can be used in that respect. Also for other connected devices than connected cars the question can emerge whether the manufacturers successfully collude with regard to technology and data governance for establishing closed ecosystems with exclusive control of the data and a lack of interoperability.

Despite our conclusions that general competition law can offer a number of options for solving problems of data access and data-sharing in IoT ecosystems, these solutions might not be easy to achieve or sufficient for solving existing and future data access and interoperability problems. One group of problems lie in the always difficult case-by-case development in the law of controlling abusive behavior, and in the difficulties and uncertainty of the development of entire new case groups. An active policy of competition authorities with regard to data access problems could however support the development of such case groups, which can also include the publication of guidelines, e.g., with regard to refusal to grant access to data in Art. 102 TFEU cases (or § 20 (1) GWB cases in Germany). Despite such efforts still large problems might remain, esp. also with regard to solving interoperability problems. Therefore it is also necessary to ask for other solutions beyond general competition law. The direct introduction of data (access) rights, the use of the data portability right of Art. 20 GDPR, the law of Unfair Trading Practices and other contract law provisions might be used for solving certain kinds of problems. Par-

ticularly interesting are also policy efforts for promoting standardisation (for solving interoperability problems), and, in some contexts, direct sector-specific regulations which allow for more tailor-made solutions. Both are especially interesting for the complex ecosystem of connected driving. However, all these other solutions have their own (often difficult) problems, which require also much more research. But from an economic perspective it is important to keep in mind that the necessary balancing between the benefits and costs of different data governance solutions (incentives, benefits of wide data use, privacy and business secret concerns etc.) and benefits and costs of closed or open (and interoperable) systems will be similar whatever kind of policy solutions and legal instruments are used. Due to the different economic and technological conditions of, it can however be expected that for different IoT ecosystems also different legal and regulatory solutions might be the most appropriate. In the discussion there is a broad consensus that “one size fit all” solutions are not the appropriate answer to the complexities of the data access and interoperability problems.

What does this imply for the discussion in competition law? (1) One should not expect that general competition law might be capable of solving all or most of these problems, i.e. often additional solutions will be necessary and sometimes they might be much better suited for solving the problems. (2) At the same time, competition law should not rely on the implementation of effective solutions through other instruments, as, e.g., sector-specific regulations or the future application of the data portability right, because it is neither clear whether such sector-specific regulations are introduced nor whether these or other solutions are effective enough for solving the problems for competition and innovation. (3) Therefore competition law should try to solve these problems also within general competition law for offering fallback solutions, if the other solutions fail or are not implemented in an effective way. Finally, it should also be kept in mind that general competition law and enforcement through competition authorities also have a lot of advantages in comparison to many of these other instruments for finding well-balanced solutions for competition problems, particularly also through their experience of applying sound economic reasonings and methods.

References

ACEA (2016a). Access to vehicle data for third-party services. ACEA Position Paper. Brussels, December 2016.

ACEA (2016b). ACEA Strategy Paper on Connectivity. Brussels, April 2016.

AFCAR (2018) Manifesto for fair digitalization opportunities. Available at: https://www.direct-access.eu/policy-event-2018

Alonso Raposo et al. (2017) The r-evolution of driving: from Connected Vehicles to Co-ordinated Automated Road Transport (C-ART). Available at: doi:10.2760/225671.

Anderson et al. (2016), Autonomous Vehicle Technology – A Guide for Policymakers.

Article 29 Data Protection Working Party (2017), Guidelines on the right to data portability, (revised version: 5 April 2017), 16 EN, WP 242 rev.01.

Autorité de la Concurrence/Bundeskartellamt (2016), Competition Law and Data.

Bell, R. / Kramer, J. (2015), Competition / Antitrust Challenges in Technology Aftermarkets, available at: https://eu-competitionlaw.com/category/abuse-of-dominance/

Borenstein, S. / MacKie-Mason, J.K. / Netz, J.S. (2000) Exercising Market Power in Proprietary Aftermarkets. Journal of Economics & Management Strategy, Volume 9 (2), 157-188.

Bourreau, M. / A. de Streel (2019) Digital Conglomerates and EU Competition Policy, abrufbar unter https://ssrn.com/abstract=3350512

Choi, S./Whinston, A. (2000), Benefits and requirements for interoperability in the electronic marketplace, Technology in Society 22, 33-44.

C-ITS Platform (2016) Final Report. Available at: https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf [last accessed 22.03.2019].

Crémer, J./Y-A. de Montjoye/ H. Schweitzer (2019), Competition policy for the digital era, available at: http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf

Determann, L., Perens, B. (2017) Open Cars. Berkeley Technology Law Journal, 915-988.

Drexl, J. (2017a), Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 8 Journal of Intellectual Property, Information Technology and E-Commerce (JIPITEC) 8, 257 – XXX.

Drexl., J. (2017b), Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz, Neue Zeitschrift für Kartellrecht (NZKart), 339–344 (part 1) und 415–421 (part 2).

Drexl. J. (2018), Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC, Brussels.

Duch-Brown, N. / Martens, B. / Mueller-Langer, F. (2017), The Economics of Ownership, Access and Trade in Digital Data, JRC Digital Economy Working Paper 2017-01, available at https://ssrn.com/abstract=2914144

EU Commission (2011), Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (2011/C 11/01).

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

EU Commission (2017a), Building a European data economy, 10.1.2017, COM(2017) 9 fin.;

EU Commission (2017b), Annex to the Synopsis report. Detailed analysis of the public online consultations results on "Building a European data economy".

EU Commission (2018a), On the road to automated mobility: An EU strategy for mobility of the future, 17.5.2018, COM(2018) 283 fin.).

EU Commission (2018b): Communication "Towards a common European data space", COM(2018) 232 final (25.4.2018).

EU Commission (2018c): Commission Staff Working Document, Guidance on sharing private sector data in the European data economy, SWD(2018) 125 fin.

EU Commission (2019), Antitrust: Commission sends Statement of Objections to BMW, Daimler and VW for restricting competition on emission cleaning technology, Press release (5 April 2019).

Farrell, J. /Simcoe, T. (2012), Four Paths to Compatibility, in: Peitz, M. / Waldfogel, J. (eds.), The Oxford Handbook of the Digital Economy, 34-58.

Farrell, J./Weiser (2003), Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age, Harvard Journal of Law and Technology 17, 85.

FIA (2016) Policy Position on car connectivity. Available at: https://www.fiaregion1.com/policy-position-on-car-connectivity/ [last accessed: 22.05.2019].

FIGIEFA (2016). Commission Communication on "Free Flow of Data". Input from the Independent Automotive Aftermarket (23 December 2016).

Furman, J./D. Coyle/A. Fletcher/ P. Marsden/ D. McAuley (2019): Unlocking digital competition. Report of the Digital Competition Expert Panel, available at: https://www.gov.uk/government/ publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel

Gasser, U. (2015), Interoperability in the Digital Ecosystem, 9-17; available at SSRN: <http://ssrn. com/abstract=2639210>.

Graef, I. (2015), Market Definition and Market Power in Data: The Case of Online Platforms. World Competition 38, 473-506.

Hawker, N.W. (2011) Automotive aftermarkets: A case study in systems competition. In: The Antitrust Bulletin: Vol. 56, No. 1/Spring 2011, 57-79.

Inderst, R. / Mazzarotto, N. (2006), Buyer Power in Distribution, in: Collins (ed.), Issues in Competition Law and Policy (ABA Antitrust Section Handbook), 2006, 1953.

Kadar, M. / Bogdan, M. (2017): “Big Data” and EU Merger Control – A Case Review, Journal of European Competition Law & Practice 8, 479-491.

Kerber, W. (1989), Evolutionäre Marktprozesse und Nachfragemacht: das Nachfragemachtproblem im Rahmen einer evolutionären Spielraumanalyse und Kritik seiner bisherigen wettbewerbspolitischen Behandlung, Baden-Baden 1989.

Kerber, W. (2016), A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, Gewerblicher Rechtsschutz und Urheberrecht - Internationaler Teil (GRUR Int.), 989–998.

Kerber, W. (2017), Rights on Data: The EU Communication „Building a European Data Economy" from an Economic Perspective, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Trading Data in the Digital Economy: Legal Concepts and Tools, Baden-Baden 2017, 109–136.

Kerber, W. (2018), Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, in: Journal of Intellectual Property, Information Technology and Electronic Commerce Law JIPITEC 9(3), 2018, 310-331.

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

Kerber, W. / Gill, D. (2019), Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, forthcoming in: Journal of Intellectual Property, Information Technology and Electronic Commerce Law JIPITEC 2019; available also at SSRN: http://ssrn.com/abstract=3406021.

Kerber, W., / Schweitzer, H. (2017). Interoperability in the Digital Economy, in: Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 8(1). 2017, 39 - 58.

Körber, T. (2016), "Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht, NZKart, 303-310 (part 1) and 348-356 (part 2).

Lee, S. / Schißler, J. (2019), 'Economic Dependence on Online Intermediary Platforms and Its Exploitative Abuse', mimeo.

Leveque, F. (2005), Innovation, Leveraging and Essential Facilities: Interoperability Licensing in the EU Microsoft Case, World Competition 28, 2005, 71-91.

Martens, B. / F. Mueller-Langer (2018), Access to digital car data and competition in aftersales services, Digital Economy Working Paper 2018-0X, JRC Technical Reports, 7-10.

McKinsey (2016) Automotive revolution – perspective towards 2030: How the convergence of disruptive technology-driven trends could transform the auto industry. Available at: https://www.mckinsey.com/~/media/mckinsey/industries/high tech/our insights/disruptive trends that will transform the auto industry/auto 2030 report jan 2016.ashx

Nothdurft, J. (2015), Relative Marktmacht: Gutachten zu Grundlagen, Bedeutung, Wirkung und Praxis der deutschen Missbrauchsverbote gegenüber relativ marktmächtigen Unternehmen, available at http://www.faire-importpreise.ch/pdf/gutachten.pdf

Nothdurft, J. (2018), § 20 GWB Unternehmen mit relativer oder überlegener Marktmacht, in: Langen, B., Bunte, H.J. (ed.) Kartellrecht: Kommentar. Band 1, Deutsches Kartellrecht, 13. A.. Köln: Luchterhand, 660-715.

OECD (2017), Competition Issues in Aftermarkets, DAF/COMP(2017)2.

OECD/ ITF (2015), Automated and Autonomous Driving. Regulation under uncertainty. Corporate Partnership Report.

Palfrey, J. / Gasser, U. (2012), Interop. The Promise and Perils of Highly Interconnected Systems, Basic Books: NewYork.

Prüfer, J. / Schottmüller, C, Competing With Big Data, TILEC Discussion Paper 2017-006, 2017, available at: https://ssrn.com/abstract=2918726.

PwC (2017), Cross-cutting Business Models für IoT. Final report (SMART number 2017/0027), Brussels.

Quantalyse Belgium, Schönenberger Advisory Services (2019) The automotive digital transformation and the economic impact of existing data access models, Technical Report. Available at: https://www.fiaregion1.com/wp-content/uploads/2019/03/The-Automotive-Digital-Transformation_Full-study.pdf.

Regulation (EC) No 715/2007 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. Official Journal of the European Union, L 171/1, 29.06.2007.

Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC. Official Journal of the European Union, L 151/1, 14.06.2018.

Schweitzer, H. (2018), Ein neuer europäischer Ordnungsrahmen für Datenmärkte?, Neue Juristische Wochenschrift (NJW), S. 275–280.

Schweitzer, H. (2019), Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, forthcoming in GRUR.

Schweitzer, H. / Peitz, M. (2017), Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?, ZEW Discussion Paper No. 17-043, 2017, abrufbar unter http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf.

Schweitzer, H. / Peitz, M. (2018), Ein neuer Ordnungsrahmen für Datenmärkte? Neue Juristische Wochenschrift, 275-280

Schweitzer, H./Haucap, J./Kerber, W./Welker, R. (2018), Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Baden-Baden: Nomos; also available at: https://www.bmwi.de/Redaktion/DE/Publikationen/ Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.html; an executive summary in English language is available at SSRN: https://ssrn.com/abstract=3250742

Shapiro, C. (1995) Aftermarkets and Consumer Welfare: Making Sense of Kodak, in: Antitrust Law Journal, Vol 63, No. 2, Winter 1995, 482-511.

Shapiro, C., Teece, D.J. (1994) Systems Competition and Aftermarkets: An Economic Analysis of Kodak, in: The Antitrust Bulletin, Spring 1994, 135-162.

Specht, L. / Kerber, W. (2018), Datenrechte – Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland – USA, abrufbar unter http://www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf.

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

VDA (2016) Position – Access to the vehicle and vehicle generated data. Available at: https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html.

Williamson, O.E. (1979), Transaction-Cost Economics: The Governance of Contractual Relations, Journal of Law & Econo9mics, 233-261.

Zech, H. (2016), A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data, Journal of Intellectual Property Law & Practic e, 460-470.