IIC
https://doi.org/10.1007/s40319-020-00974-3

ARTICLE

Towards an Access Regime for Mobility Data

Peter Georg Picht

Abstract (Forced) access to digital resources requires a legal framework which is at least partly sector-specific. Regarding the important sector of connected mobility, this paper tries to push the quest for such a framework. It analyzes data-specific market conditions in the sector and the need for intervention they generate, as well as potentially helpful legal tools in the GDPR (data portability) and core competition law (e.g. essential facilities doctrine, relative market power, pertinent EU Regulations, new tools in the 10th revision of the German Act Against Restraints of Competition). Based on these findings, the paper develops cornerstones for a regulatory, yet stakeholder-oriented approach, flexibly tuned with contract, competition and data protection law. Not least, participants of connected mobility markets should take up this idea, as they have a lot to contribute to its quality and a lot to lose if inappropriate rules came to be set.

Keywords Connected mobility · Autonomous driving · GDPR · Data portability · Essential facilities · Big data

1 Introduction

Access to resources is a key issue, not only in competition law but also in many other areas of the law, as evidenced by examples like rights of way in real estate law

Peter Georg Picht is Professor and holds a Chair for Business and Commercial Law, Center for Intellectual Property and Competition Law – CIPCO, University of Zurich, Zurich, Switzerland; and Affiliated Research Fellow, Max Planck Institute for Innovation and Competition, Munich, Germany.

P. G. Picht (✉)
Prof. Dr.; LL.M. (Yale); Chair for Business and Commercial Law, Center for Intellectual Property and Competition Law – CIPCO, University of Zurich, Zurich, Switzerland
e-mail: peter.picht@rwi.uzh.ch

Published online: 15 September 2020

or IP law provisions on (compulsory) licensing. Sometimes, the law forces access to a resource even though the resource owner does not consent to it. Competition law does so, in particular, where it perceives a degree of access to and use of a resource it considers to be below the level generating optimal static and dynamic efficiency.[1] When deciding about forced access, it must consider the downsides of the operation, such as the amount of resources necessary for generating the access, affected interests of third parties (e.g. incumbent holders of limited access rights), or a disincentivizing effect on the resource holder's future market activities.[2] Although the reasons for a suboptimal level of access and use can be manifold, transactional frictions – transaction costs, lack of information, etc. – or market (power) strategies[3] oftentimes loom large.

It seems plausible to assume, as a starting point, that these patterns – why do resource holders not grant sufficient access, why does (competition) law force access, and why ought it to carry out a careful effects analysis before doing so – are present with regard to "digital resources" as well, but that they take specific forms in strongly digitized markets. With certainty, we can say that several areas of the law are, at least potentially, involved in the organization of (forced) access to digital resources; hence there is a need to align their involvement towards a coherent approach. Contract law, data protection law, consumer protection law in general, competition law, intellectual property law, and fundamental rights provisions[4] are among the relevant fields. The involvement of other areas depends not least on the access system eventually chosen; new legal concepts may even be necessary. While numerous and truly excellent contributions[5] have been made on many of these building blocks, their intersections have, so far, been somewhat less in focus, in particular when it comes to specific sectors of the digital economy. As our reality is ever faster becoming a digital one, this lacuna must be filled, starting with sectors which loom particularly large in our economies and societies. While no single contribution – and certainly not the weak forces of the present author – can undertake to achieve this task alone, the present paper tries to contribute to a coherent, holistic legal framework for the (forced) access to digital resources as follows: the next part (2) reflects briefly on the fundamental components of such an access regime and describes the focus of the paper. The third and main part (3) assesses potential elements of a data access regime for connected mobility before the last part of the paper (4) summarizes and concludes.

[1] European Commission (2005), paras. 213, 222, 231 *et seq*., 240; MünchKommEUWettbR/Eilmansberger, Art. 82, paras. 388 *et seq*.; Immenga/Mestmäcker/Fuchs/Möschel AEUV Art. 102, para. 337.

[2] European Commission (2005), paras. 213, 222, 231 *et seq*., 240.

[3] Immenga/Mestmäcker/Fuchs/Möschel AEUV Art. 102, para. 331.

[4] For an overview on relevant fundamental rights and freedoms, *see* Drexl (2018), p. 7.

[5] *See*, for instance, Drexl (2018); Metzger (2019), p. 129; Anderson et al. (2016); Digital Competition Expert Panel (2019); European Commission (2017); Kerber (2019a); Crémer et al. (2019); Schweitzer (2019), p. 569; Graef et al. (2013); Drexl (2017); Schweitzer et al. (2018).

2 Components of an Access Regime to Digital Resources

Before delving into details of a sector-specific access regime, it seems worthwhile to briefly sketch the fundamental structure such a regime ought to display: on the most fundamental, first level of an access regime for digital resources, we locate the goals that the regime ought to serve. Among them are, for instance, static and dynamic efficiency as key means to further societal welfare, the protection of privacy as a vital need *inter alia* for individual happiness, and the enabling of free, informed communication as a cornerstone for the working of a democratic society.[6] On the second level, we consider the forms of access which, we hope, help to further these goals. Between the poles of complete access and no access at all, we find an entire range of forms of limited or "qualified" access. The access may, for instance, be restricted to part of a resource or to a certain group of persons ("accessors"). Thinking about further access qualifications makes us realize the connection between access to and use of a digital resource – you can, for instance, have access to read but not to copy, to copy but not to disseminate, or to share in a private but not in a business context. Specific entitlements to use an accessed resource are present most obviously in cases of qualified access. But full and no access imply them, in a sense, as well because an access can hardly be called complete without the right to use the accessed resource and, on the other hand, refusal of access does usually reserve the resource's use for the resource holder.

Close as the relationship between access and use is, it is also intricate. For one thing, only in a limited number of settings do the modalities of access fully regulate the modalities of use. One may, for instance, say that unrestricted use can be brought about by granting unrestricted access. Granting specific persons access to, say, a certain set of data, however, does not necessarily ensure that these data are not passed on to other persons or used only for non-commercial purposes. In such cases, a workable access regime must contain an additional regulatory element, addressing the use of the resource once access is granted. It has then become an access *and use* regime. On the third level range the pertinent fields of law, with the provisions and principles they respectively contain, as the "tools" with which to engineer the regime of access and use. As said before, contract law, data protection law, consumer protection law in general, competition law, intellectual property law, and fundamental rights provisions are certainly relevant, but other fields of the law or even new legal concepts can come into play as well. Progressing thus, as it were, from the desired results to the law intended to achieve them and not, the other way round, from given legal structures to the results they may or may not produce seems helpful in the attempt to gain a fresh view on the access question and to organize the interworking of the involved parts of the law without too much heed to seemingly unalterable axioms.

One way to classify the provisions and principles encompassed by these areas of the law is to look at their function in a regime of access and use. Some are necessary

[6] *Cf.* also the fundamental purposes of an access regime as formulated in Drexl (2018), p. 5: establishing a functioning and competitive market for the data economy; promoting innovation; protecting consumer interests with a particular focus on protecting the privacy of natural persons; and promoting additional public interests.

to make a digital resource an object the law can handle, for instance by defining what non-personal data are in the sense of the law. Other provisions assign a resource to a person by giving that person some form of entitlement. Some define the conditions under which access ought to be granted and others the modalities (accessors, extent of access, etc.) of the access. Some provisions help to administer the access, for instance by stipulating duties to document or encrypt, others allow accessors to enforce their access rights, some order the post-access use of the resources, others protect third-party interests (e.g. by way of rights to object, to audit or to employ protective "digital butlers"), and some allow resource holders to enforce limitations of access and use upon accessors. The functional classification is a helpful one as it reminds us that the modalities of each element on this third level must be checked against and justified by the function of this element in bringing about the desired access regime on level two and, ultimately, the fundamental goals on level one.

From the plethora of digital resources and of legal issues related to their access and use, this paper selects as its focus digital data[7] generation in the mobility sector, brought about in particular by the increasing use of digital communication infrastructures (internet, mobile communication, etc.) for operating mobility devices, mobility services, and traffic systems as a whole (connected mobility). This development makes connected mobility devices (not only cars) a prime example for the so-called "Internet of Things".[8] This includes not only primary data, for instance on the movements of a single car, and meta-data generated by processing such primary data, but also the algorithms and further digital tools which conduct the handling of the data. Automated cars are an important[9] but not the only component of connected mobility as, for instance, public transportation or (un-)manned drones belong to the sector as well. As to the question what a regime of access to and use of these digital resources might look like, the paper can address only a few components of the "third level" sketched above, namely selected aspects of contract and competition law,[10] data portability, and cornerstones of a potential regulatory framework. Importantly, this paper's focus is on data access, not on the broader context of interoperability between mobility devices or systems, although data access can be a vital component in allowing for such interoperability.

[7] On categories of digital data in general, *see*, from a competition law perspective, Schweitzer (2019), p. 571.

[8] Kerber and Gill (2019), p. 6.

[9] On the empirics of autonomous car driving, *see e.g.* Anderson et al. (2016).

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – GDPR), OJ 2016 L 119/1.

3 An Access Regime for Connected Mobility

3.1 Some Data-Specific Characteristics of the Sector

Connected mobility produces multifarious types of digital data potentially relevant to a broad range of stakeholders. Data on vehicle performance instruct repair, maintenance and development efforts, data on movement in traffic help to run cooperative intelligent traffic systems, and data on accidents serve to assign liability or calculate insurance conditions.[11] The range of potential access contenders includes makers of vehicles and their corresponding aftermarket products/services, distribution partners, insurance companies, telematic service providers, mobility service providers (e.g. car sharing), road and toll companies, drivers' employers, but also academia and communal or other state entities.[12]

Although the present discussion focuses almost entirely on initial data, these are not the only potential access objects in connected mobility which deserve a closer look. Control over meta-data and data-processing algorithms is a competitive factor at least as important as control over initial data. In fact, the products and services marketed in the connected mobility sector – allowing for exceptions like initial data brokers – rest heavily on these two components. Opening access to them may, therefore, be a much more powerful way to enhance competition than opening access merely to initial data. An approach that limits access to initial data may claim this access to be sufficient if, and as far as, the meta-data and related algorithms have been developed from the initial data.[13] Furthermore, adverse effects on dynamic efficiency may be stronger when digital resource holders have to grant access to resources they did not merely collect but generated. On the other hand, important parts of the initial data in connected mobility are not that easy to collect unless the collector operates its own mobility ecosystem, for instance as a large car maker. Furthermore, a substantial part of the market-relevant patterns which can be read from initial mobility data have probably already been "reaped" by early controllers of such initial data and turned into market-relevant meta-data. This process may be replicated by follow-on accessors but such replication may be too late or impeded too much by exclusionary rights on data-based products/services or structures barring market access (for instance, know-how protection through confidentiality obligations on transaction partners) to effectively challenge the market leaders without access to their meta-data.

Stand-alone digital data are, of course, not the only potential objects of access in the connected mobility sector. Access to physical objects can loom large as well and it will, in a connected world, frequently intertwine with access to data, for instance where remote repair and maintenance services require access to both a vehicle and its data.[14] Although this paper cannot explore them in detail, the interaction between aspects specifically relevant for access to data and to physical mobility devices

[11] On these and other data categories and uses, *see* Metzger (2019), p. 130.

[12] On these and other access aspirants, *see* Metzger (2019), p. 130.

[13] *Cf.* also Louven (2018), p. 27.

[14] On this example, *see* Kerber (2019b), p. 25.

respectively may require a context-specific adaptation of the legal framework to such "combined-access constellations".

Thinking back to the time when people started to use pack animals or hire porters makes us realize that mobility markets are very old. Even markets for automotive mobility have been present for more than a century. Markets relating to the collection, distribution and use of digital data generated by consumers are much younger, but even Facebook and its antecedent Facemesh have been up and running for more than 15 years.[15] Compared to these roots, the markets relating to digital data from connected mobility are in a relatively early,[16] developing phase. Certainly, core players in these markets – such as car makers or ICT big shots – are well-known, sometimes very powerful incumbents in their traditional fields. But in connected mobility, the cards are, to a certain extent, being dealt anew,[17] with traditional market and power relations not necessarily translating into this new reality. For an access regime in connected mobility, this has at least two consequences: First, previous assessments of the market position and market conduct of specific players should be extended to connected mobility only after critical re-assessment. Car makers, for instance, may be the customary strong guys on traditional car-based mobility markets. As this mobility becomes increasingly connected, though, ICT companies will challenge their position. Second, experts have found markets based on digital data prone to the quick establishment of concentrated equilibria that give large players a lasting advantage based on network effects and data access.[18] In the developing connected mobility markets there seems, at present, still to be time to prevent some such equilibria or at least their negative effects.[19] While this may call for early intervention (cf. in detail below), the dynamic, innovative potential of evolving connected mobility markets caution, at the same time, against intervention excess.[20]

In setting the course for legal intervention, one important switch is the question whether the legal framework should be technology-neutral. As to data generated by connected vehicles, an important element of technological neutrality is the compatibility of the legal framework with either of the three main technical solutions debated today,[21] viz. the Data Server Platform (DSP), the In-vehicle Interface (IVI) and the On-board Application Platform (OAP) solutions. As described by the respective EU Working Group,[22] it is characteristic for the DSP solution that "the data from the vehicle is sent to a back-end server where it can be

[15] *Cf.* Kaplan (2003).

[16] On concrete, market-oriented programs for automated driving, starting in the first decade of the 21st century, *see* Anderson et al. (2016), p. 18 *et seq*.

[17] *Cf.* also Kerber and Gill (2019), p. 7, with the references cited there.

[18] Digital Competition Expert Panel (2019), p. 4.

[19] Digital Competition Expert Panel (2019), p. 4.

[20] In favour of careful, consumer welfare-oriented balancing, *see also* Digital Competition Expert Panel (2019), p. 5.

[21] On their respective technical advantages and disadvantages, *see* European Commission (2017), p. 8 *et seq*.

[22] On the following, *cf.* European Commission (2017), p. 6.

made available. Therefore, both the vehicle data and the application using the data are outside the vehicle system". There are at least three variants of the DSP solution: the "Extended Vehicle" concept organizes access "via an ISO-standardised interface from the vehicle manufacturers' back end servers". Under the "Shared Server" concept, data can be accessed "from a server controlled by a consortium of stakeholders (rather than the vehicle manufacturer) with an equivalent link to the vehicle". The "B2B Marketplace" concept envisages "an additional layer between the vehicle and the service providers, which would be fed by vehicle manufacturers' back end servers but be maintained by a service provider that would facilitate access by the market". In an IVI solution, however, data access "is enabled via an upgraded OBD (on-board diagnostic) interface inside the vehicle; any application using data would run outside the vehicle system, either on an external device or on a layer on the interface itself". An OAP solution "would allow access to vehicle data and the execution of applications inside the vehicle environment", thereby enabling real-time interaction with the vehicle, in particular for the purposes of collecting real-time data and providing real-time services.[23] According to an EU study, "Extended Vehicle/Neutral Server" solutions are likely to become the predominant technical solution, alongside proprietary on-board application platforms, if no legal intervention takes place.[24] Some authors even contend that this is already the case.[25]

3.2 The Need for Legal Intervention

Experts have diagnosed digital markets with an overall lack of competition and a pronounced winner-takes-most feature of their competitive dynamics.[26] Digital data are found to have the potential of "a driver of concentration and barrier to competition in digital markets".[27] Although such catch-all findings should be treated with caution, they provide an argument for a competition-enhancing intervention in the digital side of the mobility sector. Many suggest that, at least if the extended vehicle model were to prevail, legal tools are needed to correct market failures in the form of insufficient access by other players than the OEMs.[28] Complex mobility devices, and cars in particular, can generate pronounced lock-in scenarios which are, however, different from the type of lock-in experienced in the context of social networks. Dependence of high-quality repair and maintenance on data and other input from the OEMs, for example, can tie providers of such services, as well as car users, to the OEM and its digital resources. The link connectivity creates to the ICT sector and, in particular, to ICT standards adds – as evidenced by the "smartphone wars" – another layer of complexity, potential distortion of

[23] On this advantage of OAP over other approaches, *see* Kerber and Gill (2019), p. 18 *et seq.*

[24] European Commission (2017), p. 13.

[25] Kerber and Gill (2019), p. 8.

[26] Digital Competition Expert Panel (2019), p. 8.

[27] Digital Competition Expert Panel (2019), p. 9.

[28] *See* Kerber (2019a); Kerber and Gill (2019), pp. 9, 17, with references to and an overview on the respective discussion.

competition, and potential market inefficiencies. Markets shaped by digital platforms seem more prone to tip in favour of a single, then dominant winner than other markets.[29] During the early stages of connected mobility, each player may try to collect, protect, and offer the data generated by its business model individually. Over time, however, it is likely that groups of players assemble to manage and offer their data on a joint platform[30] or that many players are acquired by their more successful rivals. In a word, early intervention may be required now to prevent the need for heavier intervention later, when the competitive processes in connected mobility have already been distorted.[31] In addition, there seems to be a good degree of caution, even mistrust between the players.[32] These misgivings may well result in a general reluctance to grant data access, even where more interoperability could further the data holders' business interests, for instance by way of collaborative innovation. A balanced, jointly accepted access framework may help to overcome such "misaligned incentives"[33] and the resulting disadvantageous equilibria.

While the sum of these aspects corroborates the need for a specific data access regime in connected mobility,[34] state intervention as a remedy should be applied with caution. Recent studies on digital markets in general and connected mobility markets in particular appear rather pro-interventionist, willing to err on the side of over- rather than under-enforcement.[35] To a considerable extent, this approach is probably driven by a focus on the (GAFAM[36]) big shots and the arguably problematic nature of some of their business practices. Justified as stronger intervention may be in the fields of search engines, mobile communication ecosystems, social media or consumer goods distribution platforms, these sectors do not represent the entirety of digital markets. At least in many of the markets related to connected mobility, GAFAM-like giants have not yet formed, markets have arguably not yet tipped, and the range of market players and business models is broadening rather than consolidating.[37] At the same time, the risk to inadvertently hamper competition and innovation in rapidly changing markets by premature restrictions is obvious. In such an environment, a thrust towards creating more data access via immediate state intervention should be subject to at least one empirical exercise: by way of a sector inquiry,[38] authorities should establish that there indeed

[29] Digital Competition Expert Panel (2019), p. 8.

[30] An example is the "NEVADA-Share & Secure" concept advertised by the German Association of the Automotive Industry (VDA), *see* https://www.vda.de/en/topics/innovation-and-technology/data-security/what-is.html.

[31] *Cf.* also European Commission (2017), p. 8.

[32] *Cf.* also European Commission (2017), p. 10, on typical stakeholder positions regarding the technical solution to be implemented regarding in-vehicle data.

[33] Digital Competition Expert Panel (2019), p. 5.

[34] In favour of regulatory approaches, Kerber (2019a), p. 22.

[35] *Cf.*, for instance, Crémer et al. (2019), pp. 3, 126 *et seq.*

[36] Google, Apple, Facebook, Amazon and Microsoft.

[37] European Commission (2017), p. 6 *et seq.*

[38] Schweitzer (2019), p. 576.

exist, and on a substantial scale, concrete requests or general needs for access to mobility data which are not being satisfied on reasonable terms. If this is the case and immediate state intervention seems necessary to overcome the deadlock, the inquiry will provide precious guidance on the priorities for such intervention. If, however, the inquiry reveals an access situation that is, for the moment, both on the move and satisfactory on the whole, the establishment of clear but general legal principles in favour of an appropriate access regime may be wiser than heavy encroachment on the sector by way of micro-managing state intervention.

3.3 GDPR-Data Portability and User Rights for Co-generating Data Subjects

When assessing whether new legal tools are required for a connected mobility data access regime or whether the existing elements of the law suffice, data portability according to the GDPR is of particular relevance.

3.3.1 Content and Rationale of GDPR Data Portability

Article 20 GDPR, the Regulation's core provision on portability, stipulates a new right for data subjects.[39] Important guidance on this right is provided by the Art. 29 Working Party's[40] paper "Guidelines on the right of data portability".[41] Article 20(1) GDPR entitles the data subject to receive her personal data as previously provided to and collected by the "controller" (prototypically identical with the "resource holder" in the sense of the word used here), as well as to transmit those data to another controller without hindrance (technical, legal, or otherwise).[42] Article 20(2) GDPR adds a right to have – if technically feasible – the data transferred directly from the controller to another controller/resource holder. Technical feasibility depends on the objective and subjective circumstances of the case, in particular on factors such as the technical state of the art, the resources needed to realize the transfer, as well as the resources available to the controller.[43] Absent technical feasibility, the data subject still has the right to receive her data according to Art. 20(1) GDPR.[44] Where data transfer takes place, the receiving data controller must make sure that the data are relevant and that no excessive data processing takes places after the data transfer.[45] If these requirements are not met, the receiving controller has to take appropriate measures, including the erasure of received data.[46]

[39] The legal framework preceding the GDPR contained no similar provision, *see* BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20, para. 2 *et seq*.

[40] The Art. 29 Working Party is the independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018, *see* https://ec.europa.eu/newsroom/article29/news-overview.cfm.

[41] Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233.

[42] BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20, para. 80.

[43] Ehmann/Selmayr/Kamann/Braun DS-GVO Art. 20, para. 29 *et seq*.

[44] BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20, para. 90.

[45] Rücker and Kugler (2018), para. 674.

[46] Art. 29 Working Party's Guidelines on the right of "data portability", p. 6.

Data portability merely applies where the data processing is based on consent[47] or on a contract,[48] and where the processing is carried out by automated means (Art. 20(1)(a), (b) GDPR). It extends, in principle, only to personal data provided to the controller by the respective data subject.[49] Where data refer to several data subjects in such a way that they cannot be split up into data packages referring to only one of the subjects respectively, it is debated whether each of the data subjects (or none) holds a portability right with regard to that data, or whether portability rights ought to be assigned on a case-by-case basis, depending on the main focus of the respective data and on potential protective interests of non-focal data subjects.[50] Importantly, where a controller generates data ("meta-data" in the terms of this paper) based on personal data falling under the portability right, the generated data is said to be the controller's data and, hence, not subject to portability.[51]

The controller must provide the data "in a structured, commonly used and machine-readable format" (Art. 20(1) GDPR).[52] This open wording can accommodate various formats and developing technology.[53] Application programming interfaces (APIs) allowing for the download and transfer of data will certainly play an important role in the realization of portability.[54] The Guidelines on the right of data portability allow for trusted third-parties to hold and store personal data and grant access as framed by Art. 20 GDPR.[55] This may, for instance, be relevant to "shared server solutions" in connected mobility. According to Recital 68 GDPR, "Data controllers should be encouraged to develop interoperable formats that enable data portability". This creates an interesting link to the world of technical standard-setting.[56] "Transfer" of data according to Art. 20 GDPR does not necessarily imply that the controller erases the data from its own storage and processing systems.[57]

According to Art. 20(3) GDPR, data portability rights "shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", nor shall the exercise of portability rights affect a data subject's "right to be forgotten" under Art. 17 GDPR. According to Art. 20(4) GDPR, portability rights "shall not adversely affect the rights and freedoms of others", including, in particular, the others' rights to their own data. This can place a hefty burden on controllers as they will, for instance, have to make sure that data rightfully requested by one data subject is not

[47] Art. 6(1)(a), Art. 9(2)(a) GDPR.

[48] Art. 6(1)(b) GDPR.

[49] Drexl (2018), p. 3 *et seq*., also on anonymization.

[50] For details, *see* Ehmann/Selmayr/Kamann/Braun DS-GVO Art. 20, para. 15 *et seq*.

[51] Rücker and Kugler (2018), para. 668; Art. 29 Working Party's Guidelines, p. 8 *et seq*.

[52] The concept is reflected in the Car Approval Regulation, *see e.g.* Art. 61(1) CAR.

[53] Gola/Piltz DS-GVO Art. 20, paras. 22, 24.

[54] Art. 29 Working Party's Guidelines, p. 5.

[55] Art. 29 Working Party's Guidelines, p. 5.

[56] *Cf.* Graef et al. (2013), p. 9, on a potentially disincentivizing effect of excessive portability on joint standard-setting by data collectors.

[57] But the data subject can demand erasure, on details *see* Sydow (2018), Art. 20, para. 11 *et seq*.

"contaminated" with personal data of other subjects, data that would then be ported without the other data subjects' consent.

Regardless of whether Art. 20 GDPR dogmatically belongs to competition law, to data protection law, or to both fields,[58] the provision is functionally – and purposefully[59] – placed at the intersection between data protection, consumer protection and competition law.[60] It relates to the typical data protection law goals and tools because it aims at strengthening the control of data subjects over their own data (cf. also recital 68 GDPR)[61] and contains a specific form of a claim to information.[62] While the data portability right does not establish a full-fledged property right regarding one's own personal data which is in the hands of a controller, it does enlarge the data subject's rights to dispose over her data and, correspondingly, limits the controller's freedom to dispose over the data.[63] At the same time, Art. 20 attempts to further the goals of competition law, mainly by enhancing the potential for competition between data collectors through the reduction of lock-in and network effects.[64] When data subjects have an option to "shoulder their data backpacks",[65] walk away to another collector and enable this collector to offer them, with the help of the ported data, a similar level of performance, they should dread less their parting from the previous collector. And in case a receiving collector manages to attract numerous portings, it has a (better) chance to rival the network benefits offered by the transferring collector, if and because these benefits relate to the number of personal data packages stored by a controller.[66]

3.3.2 The Solution for an Access Regime?

It remains to be seen how the impact of recently introduced GDPR-portability on data markets will enfold. There are severe, structural doubts regarding the aptitude of portability rights to order data access in connected mobility. Data portability legislation was made with a view mainly to social networks.[67] What works for such networks does not automatically suit other settings. For one thing, while the delineation between personal and non-personal mobility data is debated,[68] at least

[58] On this discussion, *see* BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20, para. 6 *et seq*.

[59] Albrecht (2016), p. 93.

[60] Drexl (2018), p. 28.

[61] Rücker and Kugler (2018), para. 664.

[62] BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20, para. 7.

[63] *Cf*. Klug (2011), p. 133; Schätzle (2016), p. 75; BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20, para. 8.

[64] Graef et al. (2013), pp. 2, 5 *et seq*.

[65] As an example for the use of the term "data backpack" (*Datenrucksack*), *see* the German Government's overview on the GDPR, https://www.bundesregierung.de/breg-de/aktuelles/persoenliche-daten-besser-geschuetzt-1008076.

[66] Roßnagel et al. (2013), p. 107.

[67] Graef et al. (2013), p. 9.

[68] *Cf*. Drexl (2018), p. 3 *et seq*.

part of the relevant mobility data are non-personal. Overall traffic patterns, for instance, are likely not personal under the GDPR. The same is true for data so well anonymized that relating them back to the subject that generated the data is no longer possible.[69] The patterns of using brakes and throttle, on the other hand, seem to be so individual that they permit identification of the respective driver and qualify, hence, quite clearly as personal data in the sense of Art. 4(1) GDPR.[70] All data revealing the identity of a data subject through the subject's preferences or customs, be it infotainment or daily routes to work, qualify as personal as well.[71] Nonetheless, authors estimate that a large part of mobility data is either non-personal or, more frequently, a "hybrid" mix of personal and non-personal components.[72] Meta-data and data processing digital tools (mainly algorithms) are not subject to GDPR-portability in any case. In consequence, and wherever to draw the line between personal and non-personal mobility data, the GDPR with its focus on personal data provides neither a comprehensive nor a very reliable porting mechanism for the sector.

Where GDPR-portability rights do apply, they need not result in a sufficiently intense porting activity. As Art. 20 GDPR does not include a right to port in real time,[73] it cannot support uses of mobility data which require access to real-time data, such as traffic management or emergency relief systems.[74] The use of connected mobility, especially by consumers, does not result in the sort of comprehensive, portable data set that is generated through Facebook profiles and similar social media identities. Where consumer use of connected mobility does produce extensive personal data profiles, for instance a portfolio of data on characteristic car buyer/user patterns collected by a car manufacturer, it is not clear to what extent such data relate to (only) one data subject who would, in consequence, be the assignee of a portability right. And even where this assignment appears clear, the respective data subject will probably have a much lower incentive to request porting of her data to another connected mobility supplier than in other areas. We care about our photos, followers, and fairy-tale weddings, but many people will let rational apathy have the upper hand regarding data on their driving patterns. As a result, the porting which happens may be too slow and fragmentary for data-based business models. This is all the more so since mobility data is frequently generated through the use of a hardware mobility item, such as a car or an e-bike. Switching – at least with regard to products/services that use such data for improving the performance (in the broadest sense) of or offering additional features to the respective mobility device – from the incumbent mobility data collector to a competitor can, in such scenarios, require customers to not only port their data but

[69] Metzger (2019), p. 131.

[70] In fact, researchers from the University of Washington and the University of California at San Diego managed to identify drivers based only on data collected from a car's brake pedal during a short (90% correctness after 15 min, 100% correctness after 90 min) driving interval. *See* Enev et al. (2016).

[71] For more details, *see* Metzger (2019), p. 131.

[72] Kerber (2019a), p. 10 *et seq*.

[73] Schweitzer (2019), p. 574 with further references.

[74] Kerber (2019a), p. 27.

also switch to the competitor's device. Investments in the incumbent's device would then be lost as sunk costs, and the lock-in effect created by these and other switching costs,[75] create an additional barrier to GDPR porting.

Finally, even a relatively intense porting activity would not guarantee intense ensuing competition. Since porting does not engender a duty to erase, network effects based on continued control over a large data portfolio may well turn out to stabilize the incumbent's market position. Where an incumbent holds a large, unilaterally collected data set of its own, a competitor may have to convince an unrealistically large number of data subjects to port within a short period, in order to get a sufficiently attractive rival business model up and running.[76] And where mobility data sets are distributed over a number of holders (e.g. the providers of car sharing, public transportation, e-bikes and telecommunication networks), an incumbent is likely to have established a cooperative network based on long-term contracts which a competitor cannot duplicate simply by having individual users port their data. Furthermore, as it keeps track of its users' porting activities, an incumbent undertaking can devise response strategies,[77] such as strategic mergers, the removal of features that trigger porting or selective incentives for users otherwise likely to port.

Partly similar to these portability-related concerns are the reservations regarding a non-exclusive right, proposed by some authors,[78] for data subjects to use data in the production of which they have contributed. Although connected mobility would probably generate such rights in great density, as all subjects do, in some sense, contribute to the data their mobility produces, their practical relevance in establishing an access regime may be much more limited. Technical and legal details of this new type of assignment remain, as yet, unclear. Lack of information or rational apathy is likely to prevent a substantial part of data subjects from exercising their "co-producer" rights and the piecemeal data available from those who exercise it may not be sufficient for the needs of many a data-based business model.

The sum of these reflections suggests that user-driven portability, as envisaged by the GDPR or a new right to data co-use, can hardly serve as the main access motor.[79] Nonetheless, they may form components of a broader, regulatory framework (cf. also below).

3.4 Core Competition Law

3.4.1 Lack of Context-Specific Rules

Data are a factor in market performance and control over data (access) can convey market power. Furthermore, exchange of data between competitors and their

[75] On switching costs and lock-in regarding mobility device/data packages, *see also* Kerber (2019b), p. 6.

[76] *Cf.* also Gal and Aviv (forthcoming), p. 31.

[77] Kerber and Gill (2019), p. 20.

[78] Drexl (2017), p. 344, albeit reticent on whether such a right would fit connected mobility in particular.

[79] For a more positive, but not enthusiastic view, *see* Schweitzer et al. (2018), p. 135.

agreeing on a joint strategy for ordering the use of their data may fall foul of Art. 101 TFEU, although this paper does not focus on this aspect.[80] Hence, competition law is an evident candidate for establishing a data access regime in connected mobility. However, such a regime must address a broad range of potential access cases. Differences between these scenarios can be substantial, which suggests context-specific rules.[81] For instance, the law cannot apply identical considerations when answering the questions whether, on the one hand, providers of aftermarket products/services ought to get access to anonymized vehicle performance data and whether, on the other hand, mobility app sellers ought to receive non-anonymized vehicle user data for marketing purposes. Core competition law has not yet established a set of rules sufficiently context-specific even for prototypical connected mobility constellations. This raises the question whether general competition law doctrines are apt to tackle the issue.

3.4.2 Essential Facilities Doctrine and Variants

One of the competition law doctrines discussed in the context of data access is the "essential facilities doctrine".[82] According to this doctrine, a dominant undertaking has – roughly speaking – to grant access on competition-law-compliant terms to a facility if (i) the facility cannot (reasonably) be duplicated, (ii) exclusive control over the facility permits to control adjacent markets and prevent competition thereon, and (iii) there is no objective justification for refusing access to the facility.[83] Although the doctrine is well established in EU competition law, enforcers have applied it with caution, for one reason because the forced access constitutes a severe, regulation-style encroachment upon the dominant undertaking's freedom to do business.[84] Closely linked to the traditional essential facilities doctrine is a set of cases dealing with access not so much to physical resources than to intellectual property. Some of these cases consider it a prerequisite for a competition-law-based right of use that the IP owner refuses to grant a licence without objective justification, thereby preventing a new product for which there would be consumer demand, and blocking competition on a downstream market.[85] In its *Microsoft* decision, however, the CFI has declared these criteria to be only one subset of "exceptional circumstances" which can justify the competition-law-based obligation to license IP.[86] And the court's decision in *Huawei v. ZTE* has introduced yet another prong of this case law,

[80] For some initial thoughts on the matter, *see* Kerber (2019b), p. 36 *et seq*.

[81] Schweitzer et al. (2018), p. 129.

[82] For an overview, *see* Immenga/Mestmäcker/Fuchs/Möschel AEUV Art. 102, para. 331 *et seq*.

[83] Whish and Bailey (2015), p. 742 *et seq*.

[84] Schweitzer et al. (2018), p. 131.

[85] Joined Cases No. C-241/91 P and No. C-242/91 *RTE and ITP v. Commission ("Magill")* [1995] ECR I-743 = ECLI:EU:C:1995:98; Case No. C-418/01 *IMS Health* [2004] ECR I-5039 = ECLI:EU:C:2004:257.

[86] Case No. T-201/04 *Microsoft v. Commission* [2007] ECR II-3601 = ECLI:EU:T:2007:289.

focussing mainly on conduct obligations in negotiations about the licensing of standard-essential patents.[87]

The application of the essential facilities doctrine to primary mobility data raises issues regarding practically all of the doctrine's requirements: access aspirants which are not undertakings in the sense of competition law, for instance public administration bodies, do not have legal standing to claim access under the essential facilities doctrine.[88]

In the developing connected mobility sector, many collectors of valuable data are unlikely to be dominant on the primary markets for connected mobility devices/services (yet) and, hence, the doctrine cannot address them in the first place. Things look different on markets for products/services complementary to a primary product if (1) the buyer of the primary product is, following its primary acquisition, locked into a "product ecosystem" and forced, or at least very likely, to demand the complementary product/service as well; if (2) primary and secondary products/services do not form a combined "systems market" on which there is competition between several system providers; and if (3) competition for the primary product/system does not effectively limit market power on the secondary market.[89] Even though connected mobility is likely to generate multiple product ecosystems,[90] these conditions – and the ensuing possibility to apply the essential facilities doctrine – will exist only in a subset[91] of the relevant cases.

In order to qualify as a physical essential facility or its IP derivative, mobility data would have to be indispensable for a successful activity on the respective adjacent (up- or downstream) market and impossible to duplicate with tolerable effort. While a right to access and use IP-protected subject matter is, by definition, indispensable for any lawful activity on markets for products/services based on this subject matter, mobility data are, largely, not protected by IP which would, by its very existence, grant them "essential" status. Duplicability thresholds under the essential facilities doctrine are high, determination of markets sufficiently clear and close to the markets on which the data collector is active can be challenging,[92] and mobility data (insights) may be more easy to duplicate than digital data generated in other areas.[93] It seems much harder to replace the personality of a human being displayed in a Facebook profile by another person's profile, or to piece it together

[87] CJEU, 16 July 2015, Case No. C-170/13 *Huawei/ZTE*. On subsequent case law, *see* Picht (2018b).

[88] Drexl (2017), p. 419.

[89] *See*, in detail, Schweitzer et al. (2018), p. 140 *et seq*.

[90] For digital transformation in general, *see* Schweitzer et al. (2018), p. 140 *et seq*.

[91] For data-based services, in particular, cross-system interchangeability and adaptability (*e.g*. by way of programming different app settings compatible with different systems) may be greater than for traditional secondary market products. As another example, transactions over data generated by a particular type/brand of vehicle may constitute a distinct market where demand cannot substitute such data by data generated through another type/brand of vehicle, for instance because they relate to repair/maintenance particularities of the respective brand/type; Kerber (2019b), p. 18. But such data may also form only part of a larger market, for instance where the information on mobility patterns they convey could also be gained from another set of vehicle data and the two data sets are, hence, substitutable.

[92] In detail on this aspect, Schweitzer (2019), p. 579 *et seq*.

[93] On modalities of duplicating data in access refusal scenarios, *see* Schweitzer et al. (2018), p. 133.

from information otherwise publicly available, than to detect traffic patterns from a portfolio of user data relating to vehicle type A instead of type B. As a result, an access regime based on the criteria of indispensability and duplicability in the sense of the essential facilities doctrine may funnel market participants into duplicating primary data although the data are already available from another collector and the resources spent on duplicative collection would have a more beneficial effect if invested in follow-on innovation.

Furthermore, if the "new product requirement" developed in the compulsory licensing prong of the essential facilities doctrine were to be applied to data access because of the intangible, non-rival nature of digital data,[94] it would be hard to apply this requirement in a sector developing as rapidly as connected mobility today. Who is to say which future products/services a particular set of data will provide the basis for and whether a product/service will not reach the market based on other data even if access to one data portfolio is refused? At least for an individual data collector it would seem an excessive burden to have to answer these questions and decide whether the essential facilities doctrine establishes an obligation to fulfil a concrete access request.[95]

Finally, even if the access applicant manages to establish all other requirements under the essential facilities doctrine, the data collector may well be able to refuse access because the data subjects' consent required by data protection laws for such access is missing.[96] The essential facilities doctrine itself cannot replace such consent[97] and it would contradict the protective ratio of data protection consent requirements to establish an obligation on the data collector to induce consent at any cost.[98]

Certainly, difficulties in applying traditional criteria of the essential facilities doctrine could be overcome by doing away with these criteria, essentially lowering the threshold of the doctrine's applicability. There are, for instance, recent tendencies in literature,[99] case law[100] and legislature[101] to establish a duty of dominant undertakings to grant competitors (technical) interoperability – including access to the data, ports/interfaces, etc. necessary for achieving this outcome – which seems to be going well beyond the traditional essential facilities doctrine. However, such approaches arguably amount to creating a new, more regulatory doctrine, an operation that should not be concealed under the essential facilities

[94] Apparently against the (rigid) application of a new product requirement: Schweitzer et al. (2018), p. 136 *et seq*.

[95] Schweitzer (2019), p. 577.

[96] Schweitzer et al. (2018), p. 133 *et seq*.

[97] In particular, Art. 6 GDPR contains no rule that would render the processing of personal data lawful just because it takes place in an essential facilities context.

[98] Schweitzer et al. (2018), p. 134 with further references.

[99] *Cf*., for instance, Kerber (2019b), p. 35 *et seq*.

[100] *See*, for instance, the far-reaching 2018 Swiss decision on granting interoperability in financial markets for dynamic currency conversion, German Federal Administrative Court (*Bundesverwaltungsgericht – BVerwG*), 18 December 2018, Case No. B-831/2011, E. 775 *et seq*.

[101] On the draft 10th revision of the German Act Against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen – GWB*), *cf*. below.

disguise.[102] Furthermore, they are, on the one hand, still limited to dominance scenarios while, on the other hand, the sweeping breadth they could acquire by doing away with the traditional requirements of the essential facilities doctrine seems, as yet, insufficiently founded on a thorough (economic) analysis of their market effects, including detrimental effects on the dynamic efficiency generated by large market players.

3.4.3 Conduct Requirements Not Tied to the Dominance Threshold

Difficulties in establishing a position of market power sufficient to trigger the essential facilities doctrine, and concerns over whether this threshold is too high to establish a sensible access regime, are reduced by the application of concepts imposing pro-competitive conduct requirements on undertakings holding market power below the dominance threshold.

German law, for instance, extends part of the conduct requirements for dominant undertakings to firms holding relative market power vis-à-vis other market players,[103] including a duty to do business and/or grant access to resources.[104] The relative market power can, *inter alia*, result from the economic dependence of a firm's business model on another firm's product, either as the consequence of a contractual relationship between the two firms or because of the dependent firm's unilateral decision to focus its market performance on the other firm's product.[105]

In a similar vein, the recent "Furman Report" from the UK suggests obligations for the handling of digital data whose application does not necessarily depend on the presence of market dominance in the sense of traditional competition law. Without going into great detail, the report proposes the institution of a "digital markets unit" which would then develop, together with the stakeholders, a code of competitive conduct to "be applied only to particularly powerful companies, those deemed to have 'strategic market status', in order to avoid creating new burdens or barriers for smaller firms". One goal the authors seem to have in mind for the code of conduct is to overcome obstacles to data portability resulting from "misaligned incentives" of data-controlling companies. The report does not limit such data openness to personal data in the sense of the GDPR but includes non-personal or anonymized data "where access to [them] will tackle the key barrier to entry in a digital market, while protecting privacy".

The automotive sector is known to generate scenarios of relative market power[106] and connected mobility will produce them as well. The existing body of law on

[102] More positive towards an application of the essential facilities doctrine with lowered thresholds: Schweitzer et al. (2018), p. 139.

[103] Hitherto, the relative market power doctrine in German competition law protected only SMEs. As part of the impending 10th GWB revision, however, this limitation is likely to be removed.

[104] Sec. 20 GWB.

[105] For details of these and other variants of relative market power, *see* MüKoGWB/Westermann GWB Sec. 20, para. 27 *et seq*.

[106] *Cf*., as one recent example, German Federal Supreme Court (*Bundesgerichtshof – BGH*), 6 October 2015, Case No. KZR 87/13 – *Porsche-Tuning*.

vertical production, distribution and service relationships in the mobility sector[107] contains, so far, no specific rules for mobility data access. Hence, the general rules for below-dominance conduct requirements apply. As part of them, the balancing of interests required under the relative market power concept for deciding whether business must be done, or access granted,[108] will have to be keyed to the particularities of mobility data access. It has already been suggested that it should loom large, in this exercise, whether data were collected as a by-product or as a key product, whether the dependent aspirant could organize access to similar data from other sources, how important the data are to the business models and innovation incentives of both parties, and how substantial the innovative contribution of the dependent undertaking will be once access is granted.[109] Even if these considerations point towards a competition-law-based right to data access,[110] however, the effectiveness of a data access regime based on the concept of relative market power can be hampered by several limitations. Traditionally, at least, conduct requirements under the concept of relative market power depend on a pre-existing business relationship or at least pre-existing market transactions over the respective resource because they are all about establishing or maintaining the aspirant's access to the relationship/transactions.[111]

In pioneer settings of connected mobility, however, such a pre-existing context may be lacking.[112] Economic theory takes a rather sceptical view on whether competition law enforcement is justified in cases of relative market power, except for scenarios in which a lock-in exists prior to the stronger party's conduct at issue.[113] Broadly extending the relative market power doctrine to settings lacking a pre-existing market and, hence, usually also a pre-existing lock-in risks neglecting these economic concerns about detrimental over-enforcement. In view of the reflections on GDPR data portability (cf. above), it seems naïve to expect customers of the undertaking holding relative market power to play a catalytic role in the enforcement of competition-law-based access obligations.[114] Dependent

[107] Results of this experience are, for instance, Regulation (EC) No. 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJ 2007 L 171/1; Commission notice, Supplementary guidelines on vertical restraints in agreements for the sale and repair of motor vehicles and for the distribution of spare parts for motor vehicles, OJ 2010 C 138/16. Commission Regulation (EU) No. 461/2010 of 27 May 2010 on the application of Art. 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices in the motor vehicle sector, OJ 2010 L 129/52.

[108] On this balance in general, *see* Immenga/Mestmäcker/Markert GWB Sec. 20, marginal note 57.

[109] Schweitzer et al. (2018), p. 146 *et seq*.

[110] Some authors contend, though, that this would largely have to be done through the development of a new subcategory of the relative market power doctrine as its established tiers might not sufficiently cover the new settings, *cf*. Kerber (2019b), p. 31.

[111] Schweitzer et al. (2018), p. 156.

[112] *Ibid*.

[113] Kerber (2019b), p. 29 with further references.

[114] For an apparently differing view, Schweitzer et al. (2018), p. 149.

undertakings will enforce access case-by-case, usually not regarding real-time data access,[115] and only if they deem the advantages of such a strategy to be higher than the costs and risks,[116] including the danger to inflict permanent damage upon their business relationship with the data holder. Unless they are overcome in the framework of a holistic access regime, data protection issues (e.g. lack of valid consent declarations), traffic security concerns (in particular regarding aspirants not previously in a business relationship with the data collector), risks to competition (e.g. exchange of sensitive information embodied in the accessed data),[117] and legitimate confidentiality interests of the data collector[118] may come into play with regard to relative market power constellations as well. Furthermore, conduct requirements for undertakings holding relative market power are known to the competition laws of some EU Member States, but not to EU-level competition law,[119] let alone to all major competition law jurisdictions worldwide. As long as the concept has not spread at least into EU law, this fact severely curtails its force to tackle the global phenomenon of connected mobility. The sum of these qualms regarding the appropriateness of an access regime based on the concept of relative market power points, again, towards a specific, regulatory *ex ante* framework.

Last but not least, provisions against anti-competitive agreements (e.g. Art. 101 TFEU) prohibit such agreements not only if the parties to them hold some sort of market power. With this tool, competition law could therefore target "mobility data cartels" engaging, for instance, in a joint refusal to deal with data access seekers or in the alignment of conditions for granting such access.[120] Data (access) cartels are, however, largely uncharted terrain as well. It remains to be seen, for instance, how data safety and traffic security aspects play out in the framework of the Art. 101(3) TFEU justification for conduct which would otherwise violate Art. 101(1) TFEU. In any case, anti-collusion law cannot remedy data access issues based on unilateral conduct.

[115] Schweitzer (2019), p. 577. Contrary to the position taken there, however, conduct rules for undertakings with relative market power are not categorically unable to enforce real-time data access – even if a violation of these conduct rules is initially claimed ex post, the remedy may well be to grant future real-time access. .

[116] Kerber (2019b), p. 33.

[117] Not only human collusion but also algorithmic collusion should be taken into consideration here because the porting of data and, more generally, the access of undertakings to each other's algorithms and digital data will, to a large extent, be realized using algorithmic systems. As digitization proceeds, as algorithms increasingly develop towards an "artificially intelligent", "deep learning" state, and as, consequently, mutual access to digital resources may become a phenomenon that gets ever broader and ever less directly steered by humans, collusive cooperation between algorithmic access systems should concern competition law and trigger further research.

[118] For the relevance of these considerations, *see also* Schweitzer et al. (2018), pp. 147, 153.

[119] MüKoEuWettbR/Eilmansberger/Bien AEUV Art. 102, para. 74 *et seq*.; Lee (2019).

[120] Kerber (2019b), p. 4.

3.4.4 The 10th Revision of the German Act Against Restraints of Competition

As to German law, the 10th revision of the German Act Against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen – GWB*)[121] attempts to mitigate some of the deficiencies highlighted heretofore. The draft revision envisages, in particular, to:

- explicitly list access to data of competitive value as a source of market dominance (draft Sec. 18(3)(2));
- include data as a potential essential facility to which its holder must grant access under the traditional conditions of the essential facilities doctrine (draft Sec. 19(2)(4));
- establish conduct rules for undertakings of preeminent, cross-market relevance for competition which are stricter than the conduct obligations for "ordinary" market-dominant undertakings (draft Sec. 19a). Not least because data access is, again, one factor relevant for the finding of a "super-dominance" in this sense, the GAFAM five are the most likely early addressees of the provision. *Inter alia*, the German Federal Cartel Office (*Bundeskartellamt*) will be able to prohibit them – by way of an ex-ante ruling and subject to objective justifications to be proven by the respective undertaking – from (i) disfavouring their competitors when intermediating access to a market; (ii) impeding competitors in markets in which the super-dominant undertaking does not presently hold but may quickly acquire a dominant position; (iii) using collected data to establish or raise market entry barriers, to otherwise impede other market players, or to introduce contract clauses permitting such a use of data; (iv) impeding competition by obstructing the interoperability of products, services or data;
- acknowledge that relative market power can exist where a market player depends on the access to data controlled by another undertaking and that refusal of access to such data may inappropriately impede the respective market player even if a business relationship concerning the data has not hitherto been established (draft Sec. 20(1a));
- prohibit undertakings with superior market power on multi-sided and/or network markets from substantially endangering effective competition by impeding competitors from generating positive network effects (draft Sec. 20(3a)). This provision is intended to timely prevent the tipping of markets prone to network effects;
- facilitate the issuance of interim measures by the competition authority through a lowering of the threshold for such measures.

At present, it seems uncertain, though rather likely, that most of these propositions actually enter into force. Still, they would form part of only one EU Member State's competition law, and it remains to be seen how much change they inspire on the level of EU law or in other Member States. Much could depend, in

[121] Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz), Referentenentwurf des Bundesministeriums für Wirtschaft und Energie, 24 January 2020, https://www.bmwi.de/Redaktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.pdf.

this respect, on the detailed agenda of recently re-designated Margrethe Vestager, now Commissioner not only for competition but also for the "digital age".

Looking at the prospective German legal framework, the prominence it attributes to data as a competitive factor looms large for the connected mobility sector, just like its fortified toolbox for controlling the conduct of undertakings holding (a certain) market power. While, in developing connected mobility markets, the overwhelming majority of players is unlikely to possess super-dominance, draft Sec. 19a GWB may be employed to curtail strategies by juggernauts from other sectors to capture these markets. Access claims based on the essential facilities doctrine should have somewhat higher prospects of success when the law expresses more clearly that theoretical duplicability does not prevent data from qualifying as essential under the doctrine. At least in multi-sided and/or network markets, lack of pre-existing data transactions will no longer block provisions on relative market power. As to the "anti-tipping" provision in draft Sec. 20(3a), there will be much initial uncertainty and need for case law to clarify, for instance, how a "superior" market position is different from dominance and relative market power or which acts exactly impede competitors from generating positive network effects. Eventually, the provision may become a useful tool in some contexts of data access in connected mobility markets, while other settings are likely to escape its reach. For the success of a car-sharing platform, for instance, network effects are paramount, and one could imagine Sec. 20(3a) to ensure access to mobility data necessary for generating such effects. When it comes to repair, maintenance or traffic stream prediction data, on the other hand, the network effects dimension seems much less evident.

3.4.5 Conclusion

The previous *tour d'horizon* has shown that core competition law contains several elements which are potentially helpful in creating an appropriate mobility data access regime. Each of them has, however, at least in its present form, boundaries and weaknesses which prevent it from constituting the stand-alone, ready-to-apply solution for the issue. In addition to their individual limitations, the pertinent competition law doctrines share some overarching problems. One of them is the fundamentally unclear interplay between competition law and data protection law. In the *Facebook* case, the German Federal Cartel Office, the Düsseldorf Court of Appeal (*Oberlandesgericht – OLG*) and – presently to a lesser extent – the EU Commission are in a discourse on whether GDPR violations can constitute a breach of competition law as well.[122] It will take a long time before the Düsseldorf court in the main proceedings (so far, it has issued only an interim decision), the German Federal Supreme Court, and potentially the CJEU have handed down their rulings on the case. And even then, the GDPR/competition law interplay is unlikely to be resolved.

[122] *Cf.* Bloomberg, "Germany's *Facebook* Order Will Be Studied by EU, Vestager Says", 8 February 2019, https://www.bloomberg.com/news/articles/2019-02-08/germany-s-facebook-order-will-be-studied-by-eu-vestager-says; Düsseldorf Court of Appeal (OLG), 26 August 2019, Case No. VI-Kart 1/19 (V).

Remedies are a second overarching problem: traditionally at least, competition law remedies have been case-by-case and after the fact, sometimes very much so at the end of lengthy proceedings. An easier access to interim measures and, more generally, a speeding up of proceedings can help competition law enforcement to provide more timely relief. Nonetheless, it seems uncertain whether competition law remedies will soon be in a position to appropriately order data access in the entire connected mobility sector, providing for outcomes such as continuous real-time access to repair and maintenance data[123] on a broad scale or the complex, non-static, stakeholder-driven data stewardship proposed in this article.[124]

All this is not to mean that core competition law will prove unable to develop answers, but at the least this process will take a period of time (and probably a substantial amount of case law)[125] during which legal uncertainty and piecemeal enforcement may slow down market dynamics or allow competition to be harmed.

3.5 EU Regulation on Access to Car Repair and Maintenance Service Information

For a few aspects of connected mobility EU law does not have to revert to general rules since it contains specific provisions of a regulatory nature. The most important ones[126] form part of the – recently recast – EU Regulation on the approval and market surveillance of motor vehicles[127] (hereinafter: Car Approval Regulation – CAR) as this Regulation also addresses the mandatory access to data for car maintenance and repair (repair and maintenance information – RMI). The Regulation establishes an obligation of car manufacturers (hereinafter: Original Equipment Manufacturers – OEMs) to grant such access,[128] based mainly on the rationale that the purchase of a car locks a customer into obtaining repair and maintenance services for the car (as well as the products necessary for them) and that exclusive possession by OEMs of the data necessary to perform such services would allow them to control the aftermarkets for the repair and maintenance of their cars[129] and, hence, the entire "system" of a car and its aftermarket products/services. Unless there is sufficiently vivid competition between several car-

[123] Kerber and Gill (2019), p. 7.

[124] *Cf.* also, regarding the example of an interoperable telematic system, Kerber (2019b), p. 26.

[125] *See also* Kerber (2019b), p. 42, pointing out the delays and legal uncertainties incurred by a case-by-case adaptation of core competition law.

[126] Another example would be Art. 6 Regulation (EC) No. 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJ 2007 L 171/1.

[127] Regulation (EU) No. 858/2018 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, OJ 2018 L 151/1. This revised version of the Regulation applies from 1 September 2020, *see* Art. 91 CAR. On the implications of the recast Regulation for Connected Mobility, *see* Kerber and Gill (2019).

[128] Art. 60 *et seq.* CAR.

[129] Kerber and Gill (2019), p. 4.

aftermarket systems,[130] the ensuing lack of competition within such systems risks generating adverse effects on static and dynamic efficiency.[131] Hence, CAR is very much about controlling a specific form of relative market power,[144] a dimension the Regulation should spell out more clearly.

The CAR access regime is perceived to have, hitherto, been working rather well[132] and the Regulation's most recent version adds some[133] components addressing connected mobility. In particular, OEMs must grant unrestricted access to RMI[134] in a format standardized through technical specifications[135] and in a non-discriminatory fashion.[136] In principle, all businesses providing aftermarket products or services can request access,[137] albeit only against the payment of "reasonable and proportionate fees" based on the extent of use of the data,[138] a stipulation evidently close to the FRAND concept known from SEP licensing.[139] Last but not least, as an important reaction to changing OEM business models, the right to access RMI no longer depends on whether the OEM has made the respective information available to authorized dealers but merely on the nature of the data themselves.[140]

In spite of these adaptations, however, the Car Approval Regulation clearly does not present the regulatory solution for data access in connected mobility, even with regard to RMI. To name only two shortcomings, the Regulation puts much emphasis on the OBD (on-board diagnostic) port and the access to data collected through this port.[141] Today, however, collection and transmission of data through the OBD as a

[130] Doubting sufficient systems competition in the automotive sector: Kerber and Gill (2019), p. 4 *et seq.* with further references.

[131] For additional details, *see* Kerber and Gill (2019), p. 4.

[132] For details on this and, in particular, the pertinent EU evaluation study, *see* Kerber and Gill (2019), p. 3.

[133] On the genesis of the recast regulation, including its focus on emissions and the European Parliament's access-oriented initiative, *see* Kerber and Gill (2019), p. 10.

[134] Recital (50), Art. 61(1) CAR.

[135] *Inter alia*, "[i]nformation shall be presented in an easily accessible manner in the form of machine-readable and electronically processable datasets" (Art. 61(1) CAR), a stipulation evidently close to the requirements for GDPR data portability. Art. 61(2) CAR indicates that the EU Commission aims at establishing a pertinent standard "through the work of the European Committee for Standardisation (CEN) or a comparable standardisation body". "Details of the technical requirements for access to vehicle OBD information and vehicle repair and maintenance information, in particular technical specifications on how vehicle OBD information and vehicle repair and maintenance information are to be provided, are laid down in Annex X" to the Car Approval Regulation (Art. 61(4) CAR). "The Commission is empowered to adopt delegated acts in accordance with Article 82, amending Annex X to take account of technical and regulatory developments", Art. 61(11) CAR.

[136] Art. 61(1), (7), (8), Annex X, Art. 2 CAR.

[137] The Regulation uses the broad term "independent operators" (*e.g.* Recital (52), Art. 61(1), (2), (5) CAR) and Art. 61(2) CAR evidences the breadth of the concept by speaking of "other operators than repairers". *Cf.*, to the same effect, Kerber and Gill (2019), p. 5.

[138] Art. 63(1) CAR.

[139] Kerber and Gill (2019), p. 5.

[140] For details, *see* Kerber and Gill (2019), p. 13.

[141] *Cf. e.g.* Arts. 3(49), 61 CAR.

central hub is technically no longer necessary and OEMs seem, in fact, to be shifting their data streams away from the OBD channel.[142] Furthermore, the Regulation contains no obligation to provide direct, real-time access to the data and IT systems of vehicles, thereby practically barring independent operators from providing remote diagnostic and maintenance services.[143] Nonetheless, CAR indicates rather clearly that regulation can be a workable and helpful instrument in the mobility sector.[144]

3.6 Cornerstones of a Regulatory Framework

3.6.1 The Relationship Between Access-granting Obligations and Market Strength

The described shortcomings of existing legal rules, and the reflections about the presently appropriate level of intervention, point towards sector-specific ex ante rules for connected mobility[145] which aim not so much at implementing immediate intervention but at establishing goals and guidance for a stakeholder-developed access regime, while providing for the option of state intervention in case stakeholders do not live up to the task. As one of its most fundamental elements, such a framework must define the market position that triggers access-granting obligations – should they be imposed on dominant firms only, depend on some form of strategic or relative power, or target every collector of relevant data? Contrary to what has hitherto been proposed,[146] the legal community should at least discuss a broad, non-discriminatory[147] access-granting obligation regarding primary connected mobility data, encompassing all collectors of such data, save maybe very small, start-up-style companies for which the technical and financial burdens of such an access regime could be suffocating.

An obligation to grant broad access to meta-data, to digital tools for processing data, and to goods/services based on primary connectivity data should, on the contrary, be much more limited. The same goes for an obligation to generate operative interoperability,[148] for instance through interface data and access to a digital platform, because such an obligation is much closer to a duty to permanently integrate an unwanted partner into one's own business model. Its ramifications must be subject to ongoing economic research as the sector unfolds; over-enforcement concerns may be mitigated by limiting general access obligations to essential digital infrastructure and/or dominant undertakings, and by adequately compensating[149]

[142] Kerber and Gill (2019), p. 8.

[143] For details, *see* Kerber and Gill (2019), p. 15 *et seq*.

[144] Kerber and Gill (2019), p. 6.

[145] Generally in favour of a regulatory approach, Kerber and Gill (2019), p. 5; Kerber (2019b), p. 43, considers connected driving a sector particularly well suited for sector-specific regulation.

[146] *Cf*. however, for an arguably similar tendency, Kerber and Gill (2019), p. 19.

[147] *Cf*. also Art. 61(1) CAR. Non-discriminatory is, however, not the same as "equal for all" because it implies treating differing constellations differently.

[148] *Cf*. also the concept of "full protocol interoperability" used by Crémer et al. (2019), p. 8.

[149] *Cf*. also Louven (2018), p. 27.

(cf. below) resource holders for the granting of access; an obligation to grant access to specific, dependent market players ought to depend on the presence of relative/strategic power vis-à-vis these dependent players. For both primary data and secondary digital resources, the access regime should not exclusively focus on market players horizontally or vertically related to the resource holder but include the public sector, science and civil society.

At least seven reasons – besides general notions of a free flow of (primary data) information in digitized societies[150] – speak for such a grid of access granting obligations:

First, traditional competition law notions of market dominance appear too high a threshold in handling a developing sector that ought – broadly speaking – to be prevented from tipping in favour of a few large players, since dominance-based intervention could likely take place only after the tipping, and thereby the creation of dominance, has already happened. Postulating a "strategic market status", which is not limited to cases of dominance, as the prerequisite for conduct obligations on digital markets[151] is a step in the right direction. But the formula in itself does not clarify the criteria for such a "strategic" status. The concept of relative market power – which equally applies below the dominance threshold – has gained clearer contours through case law but its traditional categories cannot easily grasp the constellations relevant in connected mobility. All current formulae relating to some form of market power, hence, threaten to create either legal uncertainty or under-enforcement.

Second, lawmakers, courts, and others active in the development of the law cannot know which technical solution for the collection, storage and distribution of connectivity data turns out to yield the best innovation dividend to society. Arguably, not even technical experts can be sure about this as the relative advantages of different solutions may change over time and new solutions may arise. Furthermore, the law and its enforcers can easily lag behind in their attempt to tackle the latest technical or business methods with which market players may try to circumnavigate the delineations of any given, limited access obligation. A legal framework that is technologically neutral therefore deserves preference over the backing of a specific technical solution by legal authorities[152] and a generic access requirement may be best suited to allow for technology-neutrality and avoid hare-and-tortoise races between enforcers and market players.

Third, the market strength of a data collector is not necessarily related to the quality of the data it collects. Strong players may be able to collect more data and, statistically, the large portfolios thus acquired are very likely to contain some valuable data. But smaller portfolios collected by weaker players may also harbour primary data which is of great relevance to other inventors. Precisely because the

[150] On this general consideration, *see* Drexl (2018), p. 16 *et seq.* In the EU, (cross-border) access to mobility data and the business opportunities it creates also matter from the perspective of fostering the EU internal market, *cf.* Recital (50) CAR.

[151] Digital Competition Expert Panel (2019), p. 10.

[152] *Cf.* also Kerber and Gill (2019), p. 9, arguing that rules which are technology-neutral tend to remove firms' incentives to choose a solution suboptimal in terms of static and dynamic efficiency, only because it helps protect market power.

data collector is in a weak market position, lacking for instance the necessary financial resources, it may not be able to reap the full potential of its data. This potential can then neither help the player to catch up with its stronger competitors – a prospect which might, if certain, justify an exemption from access-granting obligations to foster competition – nor can other players reap it if the collector does not want or have to grant access. If the small player remains unsuccessful, the data will either be lost or end up, by way of asset acquisition or merger, in the hands of a larger player which is itself subject to access-granting obligations. Access is then, finally, possible but it comes at the cost of deadweight losses in the form of time delay and the unnecessary investment of resources. Better it seems, from this perspective, to enable data access regardless of the market strength of the data collector,[153] letting the market decide which data appear promising enough to pay for access (on the non-gratuitous nature of access, see below).

Fourth, the fact that control over data is (at least so far) not protected by an (intellectual) property right or a similar form of ownership suggests, from a legal perspective, a low threshold for limiting such control by way of access obligations.[154]

Fifth, the multiple collection by different market players of data sets with similar information value can be economically unreasonable even where the primary collection was not dominance-enabled. Where, for instance, the data are a by-product of the main, income-generating business activity or where they have built up over an entire use history,[155] competitors of even small firms may refuse to engage in (long-term) business activity that is not, as such, relevant to them, merely to collect the by-product/historical data. Furthermore, even where duplicative collection takes place, it can be suboptimal from the viewpoint of overall economic efficiency and societal concerns such as environmental protection.[156]

Sixth, not only, but also, in connected mobility, the generation and accumulation of data frequently engage several players,[157] yet such group efforts may be disincentivized if it becomes the standard outcome that their results benefit only one or very few of the players.

And *seventh*, regarding secondary digital resources, the collecting, ordering and storing of primary data in a usable form require investments by the collector. It is the generation of meta-data and the development of products/services based on primary and meta-data, however, where the main innovative effort takes place. Forcing access to this level of a collector's business model bears, therefore, a much higher risk of harming the collector's incentives and overall dynamic efficiency than access to the level of primary data. This suggests limiting access to meta-data and data-based products/services to dominant collectors, which can typically recoup

[153] Potentially in the same vein, European Commission (2017), pp. 14, 153, 172, proposing a "requirement that a reasonable request for data could not be rejected by *any* vehicle manufacturer" (emphasis added).

[154] Schweitzer (2019), p. 577.

[155] *Cf.* on these factors as obstacles to multiple data collection, Gal and Aviv (forthcoming), p. 27.

[156] *Cf.* Drexl (2017), p. 416 *et seq.*

[157] Kerber (2019b), p. 22.

investments more easily and whose innovation incentives may be triggered rather by increased competition than by increased exclusivity, or to access seekers which are dependent on the owner of the meta-data or data-based product/service in a way that refusing access would have substantial and lasting anti-competitive effects.

3.6.2 A Stakeholder-Based Approach

While state law will – subject to other empirical results, for instance from a sector inquiry – probably prove necessary to set the guardrails on broad access to primary mobility data and on limited access to secondary digital resources, the working out of details and the management of the access regime should be left, as far as possible, to market participants and other stakeholders. This corresponds to the complex, cross-jurisdictional (cf. below) and developing nature of connected mobility, an environment in which state-driven micromanagement risks, at least presently, harming dynamic efficiency by over-enforcement in some areas, while lacking the resources or the legal capacity for appropriate enforcement in others.

A stakeholder-based approach seems particularly promising for organizing the concrete modalities of access once it is clear that access has to be granted.[158] Contracts are the tool of choice here, as their flexibility permits tailoring of the access to the individual use.[159] Considering the general rules on an appropriate data access regime to be limitations for the permissible content of such contracts and requiring stakeholders to make the contracts accessible[160] – except for business secrets and similar confidential content – for oversight purposes will help to keep this contractual, case-by-case approach in line with the overall system. The EU Commission has already formulated some guiding principles for data-related contracts, such as transparency on the scope and purpose of data access, protection of legitimate confidentiality interests, and a porting-friendly approach for data generated as by-products.[161] Clearly, these aspects are not exhaustive and it seems doubtful whether – as already suggested[162] – their enforcement only via Member State contract laws would be of sufficient timeliness and efficiency. However, an augmented collection of guiding principles for stakeholder contracts could form part of a future, binding regulatory framework. Additionally, the law on intellectual property rights provides an essentially stakeholder-based grid for balancing access and exclusivity, in particular through (compulsory) licence contracts and statutory rights to use protected subject matter.

[158] The Car Approval Regulation takes a different approach by making very detailed technical stipulations in its Annex X and mandating the European Commission to keep the Annex abreast of technical and regulatory developments. For the reasons given in this contribution, it seems doubtful whether this concept is suitable for an access regime covering broader areas of connected mobility. In favour of the CAR approach, however: Kerber and Gill (2019), pp. 11, 17.

[159] In favour of a contractual approach and on concrete examples implemented by BMW and Tesla: Metzger (2019), pp. 130, 133 *et seq*.

[160] Similar: Metzger (2019), p. 135.

[161] European Commission (2018).

[162] Schweitzer et al. (2018), p. 148; similar, but more critical on whether this generates a sufficient contract control: Drexl (2017), p. 420.

Data pooling is another element suitable for a stakeholder-based approach. Large pools of relevant data not only help foster innovation (e.g. machine learning)[163] and transaction efficiency, they can also mitigate the risks posed to competition by unilateral control over large data portfolios.[164] Having such pools run by stakeholders, in the framework of legal rules which safeguard their secure, pro-competitive, and otherwise compliant management,[165] seems preferable over pools whose data are subject to direct state control (and potentially abuse). From a technical perspective, stakeholder collectives should be in a much better position than public administration to determine "structured, commonly used and interoperable formats" (cf. Recital (68), Art. 20(1) GDPR) allowing for an efficient transfer of data to be accessed.

As to the bodies that should work out, implement and control the details of an access regime, specialized state agencies and collective stakeholder organizations, such as SSOs[166] or mobility providers' associations, are among the obvious candidates. Some form of cooperation between these two types of protagonists seems helpful in any case, but who is in the driver's seat? The Furman Report favours, with regard to digital markets in general, the creation of new agencies which are supposed to cooperate with stakeholders but also to play the decisive part in working out rules of conduct for such markets.[167] It states that "it is clear that a voluntary approach would be insufficient – businesses' natural incentives do not line up with delivering these functions".[168] However, it does not seem self-evident that a less gloomy view on the ability of stakeholders to create a workable access regime themselves would prove naïve. With the help of sufficient guidance on the general principles they ought to implement and the expectation of state intervention as a result of failure to perform the task, stakeholder organizations can be quite good at finding workable solutions.[169] They may, in fact, outperform state agencies which, typically, possess less hands-on experience and resources than the stakeholders collectively. Moreover, additional administrative bodies can show a tendency to justify their existence by generating activity that is not strictly necessary while a stakeholder-driven framework setting promises greater restraint. Where additional state enforcement resources prove necessary,[170] the same reflection points towards the creation of specialized units within existing agencies, to be staffed at least with

[163] Schweitzer et al. (2018), p. 152.

[164] Favourable also Kerber (2019b), p. 40.

[165] This may include a "trustee" overseeing the grant of access, not least because this solution would prevent data holders from recording access patterns and developing anti-competitive strategies based on these insights, *cf.* Kerber and Gill (2019), p. 16.

[166] *Cf.* also Recital (54), Art. 61(2) CAR, envisaging the setting of standards for vehicle data exchange by the European Committee for Standardization (CEN).

[167] Digital Competition Expert Panel (2019), p. 10 *et seq.*

[168] Digital Competition Expert Panel (2019), p. 10.

[169] *See*, for instance, on reforming ETSI policies in cooperation with the EU Commission and stakeholders, Fröhlich (2008), especially p. 214 *et seq.*

[170] For an example of an enforcement regime combining stakeholder self-responsibility and oversight by a specialized agency, *see* Art. 64 *et seq.* CAR, which stipulates that OEMs must proactively submit proof of compliance while the agency in charge checks compliance where indicated.

legal experts in the fields of competition law and data (protection) law, technical experts and economists, instead of creating entirely new agencies with their own administrative overheads and search for legitimacy.[171]

Besides state legal guidance, oversight by state authorities, and an appropriate organizational structure, a stakeholder-based approach must include a robust dispute resolution mechanism, effective in its procedural framework, customized to the sector-specific needs (e.g. regarding panel structure), and generating enforceable decisions. This is a lesson we can learn from the "Smartphone Wars", fought mainly via extensive state court litigation over the licensing of standard-essential ICT patents.[172] Alternative Dispute Resolution proposals for this sector[173] may prove helpful for the connected mobility sector as well.

3.6.3 The Role of Data Subject Consent

Which role should the consent of data subjects play in an access regime for connected mobility data? As far as personal data in the sense of the GDPR are concerned, the Regulation's consent requirements[174] form a sort of lower threshold for the grant of access to such data. Previous experience with formally consented data collection hauls,[175] however, and the complex range of cases of potential data use raise doubts over the consent principle's aptitude to serve as a flexible, specific and – where necessary – restrictive mechanism for establishing a data access regime. General critique that the resources (to be) invested into fulfilling GDPR consent requirements may not result in an adequate increase in protection and self-determination[176] seems, therefore, likely to apply to connected mobility as well.

Whether consent declarations provide meaningful guidance on when access should be granted appears doubtful given that data subjects can feel forced into consenting in order to be able to properly use an acquired connected mobility device or service; that they may be unaware of what a consent declaration extends to if it is shown only briefly on the screen of their mobility device; or that they are likely to systematically underestimate the value of the data "given away" for free by their consent.[177] Shortcomings in the consent mechanism can, however, lie not only in the excessive breadth of consent declarations or the lack of awareness of what the subject consents to. Consent declarations whose wording is too narrow, or which are

[171] The Furman Report discusses both options but leans towards a stand-alone digital market authority, *see* Digital Competition Expert Panel (2019), p. 10.

[172] For a case-law overview, *see* Picht (2018b); Picht and Habich, "FRAND: The German case law" (forthcoming).

[173] *See*, for instance, the Munich IP Dispute Resolution FRAND ADR Case Management Guidelines. On further proposals and soft law, *see* Picht (2019).

[174] *Cf.* Art. 6 *et seq.* GDPR.

[175] A recent example is the *Facebook* case of the German Federal Cartel Office, *see* https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.

[176] Metzger (2019).

[177] On these and further consent issues, *see* Weichert (2014), p. 242 *et seq.*; Lüdemann (2015), p. 253; Acquisti and Grossklags (2003), especially pp. 7, 11, 12, 14; Metzger (2019), pp. 131 *et seq.*, 134 *et seq.*

lacking altogether because data collectors overlooked or avoided the need to invest in requesting them, can block beneficial data use. Even the very addressee of a consent requirement can be uncertain, for instance where a mobility device changes hands and the acquirer is not a party to the contract between the original owner and the seller of the device, or where the subject generating data by way of a mobility device is not the device owner but a mere user, potentially unknown to the data collector.[178] The right of data subjects to revoke, in principle, their consent (Art. 7(3) GDPR) could endanger the use of entire data portfolios or data-based products/services into which data had been integrated that are now subject to the revocation. The development of user-friendly standard procedures for granting or refusing a consent keyed to the case of use at issue[179] may help to improve things. At least for the time being, though, the law will have to ensure an appropriate access regime even where and when the consent mechanism fails. This arguably applies not only to consent requirements under data protection laws but also to the consent mechanisms envisaged for the OAP access to connected vehicles.[180] A legal framework to this effect will have to include provisions which limit the rights of primary data collectors to grant other market participants (e.g. providers of products/services on aftermarkets) access to personal data even if data subjects have generically consented to the passing on of their data, but also provisions which allow for the granting of access[181] to anonymized or otherwise not clearly personal data even though specific data subject consent is lacking and the applicability of data protection rules to such data may be unclear.[182]

3.6.4 Compensating Access

As a general rule, access to mobility data should be compensated rather than for free. This enables market mechanisms to play, for instance by shifting investment in and the realization of access to data to those market players who are able to make use of the data at the best cost/return ratio and, hence, in a way favourable to the economy and society as a whole.[183] Furthermore, access compensation can be adapted to the investments necessary for collecting the respective data and to the role the data play – e.g. as a by-product or key product – in the collector's business model, thereby safeguarding the collector's incentives to engage in beneficial data collection and data-based innovation.[184]

[178] *Cf.* Metzger (2019), p. 134.

[179] Digital Competition Expert Panel (2019), p. 13.

[180] Favouring user selection and user consent in an OAP arrangement as the best solution at least for RMI access – as do, for instance, Kerber and Gill (2019), p. 18 *et seq.* – may, therefore, prove too optimistic.

[181] Metzger (2019), p. 130.

[182] An example is provided by Arts. 35, 36 Payment Services Directive, under which providers of digital payment services can request access to bank account data of their customers from the respective bank for the purpose of processing a payment, *see* Drexl (2018), p. 29.

[183] Picht (2018c), p. 55 *et seq.*; Metzger (2019), pp. 130, 134.

[184] Schweitzer et al. (2018), p. 131.

This immediately suggests transfer of the F(air)R(easonable)A(nd)N(on-)D(is-criminatory) concept, developed mainly for the licensing of ICT SEPs, to the "licensing" of connected mobility data as a new field of application.[185] In fact, CAR already champions this concept for the scope of its application. It should be noted, though, that FRAND is far from a finalized, smoothly working concept.[186] In spite of the doctrine's high beneficial potential, the remaining problems even in the ICT-SEP area are legion. Numerous contributions from scholars, probably case law, and potentially the law-makers will be required to work out a FRAND framework for access to connected mobility data, as provisions like Art. 63(1) CAR, stating that data holders "may charge reasonable and proportionate fees", are of little guidance value for this quest.

This paper makes two remarks: First, for FRAND to become more than a euphonious label it is necessary to establish principles on how to determine what FRAND access conditions are in a given setting. This includes specifying a range of cases of use and their corresponding access conditions.[187] In ICT-SEP licensing, the breaking down of an appropriate cumulative royalty for all relevant SEPs into shares depending on the number of SEPs held by the respective patentee ("top-down method") and the assessment of comparable licences ("comparables") form the two most prominent determination methods at present.[188] Both are intricate to apply in connected mobility. The number and diversity of relevant data, as well as the multifarious business models which may be based on access to them, render the determination of an appropriate overall "access price" and its breaking down into shares to be paid for the access to a certain subset of data in the context of a certain business model much more difficult than in the ICT-SEP context. Comparables will also be hard to find as long as the licensing of mobility data is still in an early phase. FRAND determination in connected mobility may therefore have to revert, at least initially, to methods other than top-down or comparables, for instance to model licence conditions defined by stakeholders' associations.

Second, to a certain extent FRAND shifts the determination of licence conditions from market forces to regulative, market-ordering rules. This forms a strong concept for the licensing of ICT-SEPs, not least because it is limited there to a large but finite number of patents on a universally needed infrastructure. "FRANDialization" of entire sectors, however, implies the risk of an excessive curbing of market dynamics, together with the static and dynamic efficiencies that the free, intense working of market forces can bring about. In some respects, for instance core primary data and/or key data collectors, FRAND access to mobility data will

[185] Schweitzer (2019), p. 576.

[186] Rather supportive of transferring FRAND to connected mobility: Kerber and Gill (2019), pp. 19, 21.

[187] On use-case-based vs. application-based access, *cf.* also European Commission (2017), p. 7 *et seq.* For a pricing example – a maximum of EUR 5 per car and month – implemented by the car maker BMW, *see* Metzger (2019), p. 133.

[188] For a comparison and their application in two high-profile cases, *see* Picht (2018a).

probably be beneficial nonetheless. But one should be cautious in making it the general solution across all constellations of connected mobility.[189]

3.6.5 Limitations

An appropriate access regime must respect, or at least pay close attention to, the reasons and interests which speak against unfettered access. In connected mobility, they form a multifarious pattern which is by no means necessarily identical to those in other sectors of the economy. This paper limits its reflections to only two concerns, namely "privacy" in the sense of the (rules for the) protection of personal data and "traffic security" in the sense of a safely working mobility system which protects the lives and goods of all stakeholders involved. Many contributions to the discussion about data access have an explicit or underlying focus on personal data collected via the internet by companies such as the big GAFAM five,[190] hence their focus on the privacy concern.[191] In connected mobility, however, traffic security is paramount as well.[192] Personal and non-personal traffic data transferred into hands that do not, for instance, adequately protect them, use them for ill purposes, and/or make them the basis for unsafe products or services can become very dangerous. Two groups of stakeholders who would likely bear the brunt of such risks, and whose interests in traffic security should therefore loom large, are the traffic participants whose health and fortune are at immediate stake, but also mobility providers (car makers, public transportation companies, etc.) which may be held liable[193] – at least primarily or jointly – for the damage caused by mobility goods/services (e.g. spare parts, apps) they did not even originate.

To safeguard data protection and traffic security, substantive legal rules, technical solutions[194] and an appropriate agency structure[195] will have to join hands. Mandatory differential privacy that prevents de-anonymization of previously personal data,[196] tagging and blockchain-based tracking of the fate of accessed data packages, as well as safety standards and checks for data or data-based

[189] Similarly, the establishment of only one platform for data sharing, as suggested by the EU Commission experts, has the downside of eliminating systemic competition between several data platforms; *cf.* European Commission (2017), p. 15.

[190] Google, Apple, Facebook, Amazon and Microsoft.

[191] *Cf.*, for instance, Digital Competition Expert Panel (2019), p. 6, which talks, even regarding non-personal data, only about "protecting privacy".

[192] Drexl (2018), p. 14 *et seq.*

[193] On this risk and its implications especially for OAP solutions, European Commission (2017), p. 13.

[194] On technical standards as a component of data access regimes, *cf.* also Digital Competition Expert Panel (2019), p. 128.

[195] Art. 66 CAR provides an interesting example by entrusting the "Forum on Access to Vehicle Information regarding access to vehicle OBD information and vehicle repair and maintenance information" with developing rules and procedures for the access to sensitive vehicle data.

[196] On the workings, chances and limitations of differential privacy, *see* D'Orazio et al. (2015); Bambauer et al. (2014).

products/services which are fed back into connected mobility[197] represent important technical contributions. "Data austerity", meaning that access should be limited to the data truly necessary for a particular case of use,[198] has an important technical component as well since it is, in the first place, a technical question which data are required for providing a particular data-based product/service. A range of pre-defined access/use cases for typical constellations could provide safe harbours and guide companies on how they should structure their pertinent transactions. If there are doubts over whether the legal framework ensures an appropriate access regime irrespective of the technical solution implemented for storing and accessing data, a general rule that primary data ought to be stored on neutral servers could prove helpful, at least until OAP solutions are safe and workable enough to be implemented.[199]

As to agency structures, it seems – again – doubtful whether state agencies have the resources to perform these technical tasks as well as, let alone better than, stakeholders. Instead, primary stewardship could lie with the stakeholders, in particular with providers of key components in connected mobility, such as car makers or ICT infrastructure providers, while state authorities exercise oversight. Stakeholder groups could designate a neutral entity that carries out the stewardship as a sort of fiduciary, in cooperation with a board of stakeholders.[200] State oversight, together with standards[201] set by collective stakeholder bodies, would also mitigate the risk that the stewards of such an access regime use their position to harm competition – be it by colluding or by abusing market power conferred on them – or to undermine the very goals they are mandated to achieve.

3.6.6 Relation Between New Regulation and Other Elements of the Law

It seems unlikely that the legislature would design a new access regulation to immediately and completely replace all existing regulatory elements – CAR in particular – in the mobility sector.[202] Such self-restriction may prove wise given that it can be difficult to predict the ramifications of new regulatory tools. However, new and incumbent regulation must be made to interact coherently. CAR, for instance, should probably take precedence over new regulatory provisions with regard to

[197] *Cf.* Kerber and Gill (2019), p. 15, who underline that security issues – and defensive OEM strategies based on them – are not new to the mobility sector and that appropriate certification systems can go a long way towards resolving them. It seems uncertain whether one certification mechanism will suffice for the entirety of connected mobility, but area-specific certifications should prove helpful.

[198] European Commission (2017), p. 9.

[199] European Commission (2017), p. 13.

[200] For an example, *see* European Commission (2017), p. 50. *See Facebook* case of the German Federal Cartel Office, https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html, on the SERMI Association.

[201] CAR, for instance, does already envisage standardization, although with an outdated focus on OBD solutions, *cf.* Kerber and Gill (2019), p. 5.

[202] Kerber and Gill (2019), p. 8.

vehicle repair and maintenance information for independent operators.[203] In a – very advisable – assessment of the new regulatory system's workability, such interactions should be a focus point.

What would be the interrelation between specific rules – including specific regulation – on connected mobility data access and general competition or data protection law? Some argue for a parallel application of core competition law,[204] and it is true that competition law should remain available as a subsidiary watchdog[205] for constellations not foreseen by the more specific (regulatory) framework. Multiple layers of legal requirements and sanction regimes can, however, lead to a compliance overstrain, resulting in a lack of legal certainty and coherence, over-enforcement, and suboptimal dynamic efficiency due to the fear of getting caught in a compliance trap. This could be avoided by a principle of competition law subsidiarity, according to which core competition law ought to step in only where more specific rules prove structurally or practically unfit to do the job. In general, compliance with the sector-specific (regulatory) rules should, therefore, create a safe harbour from general competition law or, at least, prevent fines for acts found to be violating general competition rules. Conversely, access regime regulations could step back to the extent portability rights or potential data subjects' rights to use co-generated data manage to generate an appropriate access regime.

One development strengthening such a priority role for data portability rights could be their extension to non-personal data, as already undertaken in France.[206] To realize such a flexible fine-tuning, the bodies implementing a data access regime will have to establish resources enabling them to empirically ascertain, on an ongoing basis, the extent to which portability rights or other mechanisms complementary to the core data access regime are realizing data access in a way that enables the core regime to step back. There is, save in exceptional settings, no such thing as a general (intellectual) property right to primary connectivity data.[207] Nonetheless, existing IP access rules may inform connected mobility regulation, for instance when it comes to the shaping of compulsory "licences" to data. As an example, the primarily contractual and remunerated nature of compulsory licences under Art. 31 TRIPS, as well as the dependency of their duration and scope on the purpose for which they are required, appears worthy of transfer to a data access regime. Conversely, if certain data are protected by intellectual property rights, for instance because they form part of a secondary digital resource, data access regime requirements are likely to impact existing IP provisions (e.g. on protectability or

[203] *Cf.* also Recital (51) CAR: "Technical progress introducing new methods or techniques for vehicle diagnostics and repair, such as remote access to vehicle information and software, should not weaken the objective of this Regulation with respect to access to vehicle repair and maintenance information for independent operators".

[204] Digital Competition Expert Panel (2019), p. 8.

[205] Following an arguably similar approach: Kerber (2019b), p. 43.

[206] Art. L224.42.1 *Code de la consommation* (French Consumer Code), *see* Drexl (2018), p. 16.

[207] On the discussion about property or other assignments of rights to data, *see* Drexl (2017), p. 340 *et seq.*; Metzger (2019), p. 135, also on database rights as a relatively important exception; Schweitzer et al. (2018), p. 153 *et seq.*

compulsory licensing), or even induce the creation of new IP protection limitations.[208]

3.6.7 The Cross-jurisdictional Level

Markets for specific connected mobility products or services can well be national or regional. But the tasks of a corresponding access regime are, in part, global. Access to data resulting from and helpful to coordinating the use of a road in the US Midwest are of little interest to public transportation providers in the Chinese city of Chengdu. But a provider of world-wide map and road directions may wish to access these data and, to the extent they show safety issues related to a brake system built into various car brands all over the world, they are potentially important to authorities, as well as to several players along the chain of production and distribution. Even today, many legal elements of a future data access regime would, essentially, be national or regional, lacking homogeneity with parallel legal elements in other nations/regions of the world and oftentimes thereby creating data security gaps or deadweight losses in the form of resources required to conform with differing legal regimes. In such instances, the territorial tradition of legal regimes clashes with the global nature of the tasks they have to solve. Worldwide law on a data access regime for connected mobility, for instance in the form of a UN-induced treaty, is unlikely to be set any time soon. However, from the side of state authority, a close cooperation between the – already existing – mobility and data protection agencies of important regions (North America, China, EU, Japan, etc.) and, from the stakeholder side, best practice models developed by ICT SSOs or associations in the traditional mobility sector[209] could serve as an, albeit piecemeal, starting point. Reputed international organizations, such as the World Intellectual Property Organization or the International Competition Network, could adopt a coordinating and driving role.

4 Conclusion

Digitization requires a legal framework which is at least partly sector-specific. Regarding the important sector of connected mobility, this paper has tried to push the quest for such a framework one step further. The cornerstones for a regulatory, yet stakeholder-oriented approach, flexibly tuned with contract, competition and data protection law, presented here, are probably not the only workable solution. Given the advantages, though, it deserves further research, discussion and, potentially, implementation. Participants in connected mobility markets should join this exercise as they have a lot to contribute to its quality, and a lot to lose if inappropriate rules come to be set.

[208] Drexl (2017), p. 420 *et seq.*

[209] *Cf.*, for instance, the "NEVADA-Share & Secure" concept, developed by the German Association of the Automotive Industry (VDA), https://www.vda.de/en/topics/innovation-and-technology/data-security/what-is.html.

References

Art. 29 Working Party (2017) Guidelines on the right of data portability, 27 October 2017. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

Acquisti A, Grossklags J (2003) Losses, gains, and hyberbolic discounting: an experimental approach to information security attitudes and behavior. 2nd Annual Workshop on "Economics and Information Security", UC Berkeley. http://people.ischool.berkeley.edu/~jensg/research/paper/acquisti_grossklags.pdf

Albrecht JP (2016) Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung. CR: 88–98

Anderson JM, Kalra N, Stanley KD, Sorensen P, Samaras C, Oluwatola TA (2016) Autonomous vehicle technology, a guide for policymakers. RAND Corporation. www.rand.org/t/rr443-2

Bambauer JR, Muralidhar K, Sarathy R (2014) Fool's gold: an illustrated critique of differential privacy. 16 Vanderbilt Journal of Entertainment & Technology Law 2014:701–755. http://www.jetlaw.org/wp-content/uploads/2014/06/Bambauer_Final.pdf; and Arizona Legal Studies Discussion Paper No. 13-47. https://ssrn.com/abstract=2326746

BeckOK DatenschutzR/von Lewinski DS-GVO Art. 20

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

D'Orazio V, Honaker J, King G (2015) Differential privacy for social science inference. 24 July 2015. Sloan Foundation Economics Research Paper No. 2676160. https://ssrn.com/abstract=2676160; or https://doi.org/10.2139/ssrn.2676160

Digital Competition Expert Panel (2019) Unlocking digital competition, March 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf

Drexl J (2017) Neue Regeln für die Europäische Datenwirtschaft? NZKart 2017:339–344 (part 1), 415–421 (part 2)

Drexl J (2018) Legal challenges of the changing role of personal and non-personal data in the data economy. Max Planck Institute for Innovation and Competition Research Paper No. 18-23, 7 November 2018. https://ssrn.com/abstract=3274519

Ehmann/Selmayr/Kamann/Braun DS-GVO Art. 20

Enev M, Takakuwa A, Koscher K, Kohno T (2016) Automobile driver fingerprinting. De Gruyter Open – Proceedings on Privacy Enhancing Technologies (1):34–51. http://www.autosec.org/pubs/fingerprint.pdf; or https://doi.org/10.1515/popets-2015-0029

European Commission (2005) DG Competition discussion paper on the application of Article 82 of the Treaty to exclusionary abuses, December 2005. http://ec.europa.eu/competition/antitrust/art82/discpaper2005.pdf

European Commission (2017) Access to in-vehicle data and resources, final report. https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf

European Commission (2018) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Towards a common European data space", COM/2018/232 final. https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-232-F1-EN-MAIN-PART-1.PDF

Fröhlich M (2008) Standards und Patente – Die ETSI IPR Policy. GRUR 205–218

Gal M, Aviv O (forthcoming, manuscript on file with the authors) The competitive effects of the GDPR. https://doi.org/10.1093/joclec/nhaa012

Graef I, Verschakelen J, Valcke P (2013) Putting the right to data portability into a competition law perspective. The Journal of the Higher School of Economics, Annual Review 2013:53–63. https://ssrn.com/abstract=2416537

Gola/Piltz DS-GVO Art. 20

Immenga/Mestmäcker/Fuchs/Möschel AEUV Art. 102

Kaplan K (2003) Facemash creator survives ad board. The Harvard Crimson, 19 November 2003. https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/

Kerber W (2019a) Data governance in connected cars: the problem of access to in-vehicle data. 9 (2019) JIPITEC:310. https://www.jipitec.eu/issues/jipitec-9-3-2018/4807/citation

Kerber W (2019b) Data-sharing in IoT ecosystems from a competition law perspective. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3445422

Kerber W, Gill D (2019) Access to data in connected cars and the recent reform of the motor vehicle type approval regulation, 7 June 2019, MAGKS Joint Discussion Paper Series in Economics No. 15-2019. http://www.uni-marburg.de/fb02/makro/forschung/magkspapers

Klug C (2011) Revision des EU-Datenschutzrechts aus Unternehmenssicht. RDV 129–139

Lee S (2019) Economic dependence on online intermediary platforms and its exploitative abuse. LL.M. dissertation, Faculty of Law, University of Amsterdam. https://ssrn.com/abstract=3343370

Louven S (2018) Zugang zu Daten – Kartellrecht als Lösung? GRUR Newsletter 2/2018:26–27. http://www.grur.org/uploads/media/2018-02_GRUR_Newsletter_02.pdf

Lüdemann V (2015) Connected Cars – Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück. ZD 247–254

Metzger A (2019) Digitale Mobilität – Verträge über Nutzerdaten. GRUR 129–136

MüKoEuWettbR/Eilmansberger/Bien AEUV Art. 102

MüKoGWB/Westermann GWB Sec. 20

MünchKommEUWettbR/Eilmansberger Art. 82

Munich IP Dispute Resolution, FRAND ADR case management guidelines, version 1.0. http://www.ipdr-forum.org/guidelines/

Picht PG (2018a) FRAND determination in TCL v. Ericsson and Unwired Planet v. Huawei: same same but different? Max Planck Institute for Innovation & Competition Research Paper No. 18-07. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3177975

Picht PG (2018b) FRAND wars 2.0. WuW 2018:234 (part I), 300 (part II)

Picht PG (2018c) Vom materiellen Wert des Immateriellen. Mohr Siebeck, Tübingen

Picht PG (2019) Schiedsverfahren in SEP/FRAND-Streitigkeiten – Überblick und Kernprobleme. GRUR 11–25

Roßnagel A, Richter P, Nebel M (2013) Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der DS-GVO. ZD 103–108

Rücker D, Kugler T (eds) (2018) New European General Data Protection Regulation – a practitioner's guide. C.H.Beck/Hart/Nomos, Munich/London/Baden-Baden

Schätzle D (2016) Ein Recht auf die Fahrzeugdaten – Das Recht auf Datenportabilität aus der DS-GVO. PinG 02(16):71–75

Schweitzer H (2019) Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung. GRUR 569–580

Schweitzer H, Haucap J, Kerber W, Welker R (2018) Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 29 August 2018. https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&v=15

Sydow G (ed) (2018) Europäische Datenschutzgrundverordnung – Handkommentar, 2nd edn. Nomos/Manz/Dike, Baden-Baden/Vienna/Basel

Weichert T (2014) Datenschutz im Auto – Das Kfz als großes Smartphone mit Rädern. SVR 6:201–207 (part 1), 241–248 (part 2)

Whish R, Bailey D (2015) Competition law, 8th edn. Oxford University Press, Oxford