Paving the way for future reforms

From (horizontal and sectoral) data access solutions towards data governance systems

Wolfgang Kerber[*]

A. Introduction

The emerging data economy has triggered a broad and fast-evolving discussion about the governance of data. Whereas personal data are subject to the EU General Data Protection Regulation (GDPR), no clear legal framework exists for the increasing amount of other (non-personal or industrial) data that are collected and produced in the digital economy, e.g. sensor data in Internet of Things (IoT) contexts, anonymised data sets, or inferred data. After a brief debate about the need for a new exclusive right on those data, the discussion has shifted very fast to concerns that the huge amount of collected and produced data is not being used sufficiently to drive innovation and competition. This has led to a broad policy discussion about more data access and data-sharing.[1] From an economic perspective this is driven by the insights that (a) data are non-rivalrous in use, i.e. the same

* I thank the participants of the conference 'Verbraucherrechtstage 2019: Datenzugang, Verbraucherinteressen und Gemeinwohl' (12–13 December 2019 in Berlin) for valuable feedback. The author declares no conflict of interest.

1 See Herbert Zech, 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data' (2016) 11 Journal of Intellectual Property Law & Practice 460; Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 989; Wolfgang Kerber, 'Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Hart and Nomos 2017) 109; Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertization and Access' (2017) 8 Journal of Intellectual Property, Information Technology and ECommerce 257; Josef Drexl, 'Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz' (2017) 5 Neue Zeitschrift für Kartellrecht 339 (part 1) and 415 (part 2); Communication from the European Commission of 10 January 2017 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – Building a European Data Economy, COM(2017) 2 final; Heike Schweitzer and Martin Peitz, 'Ein neuer Ordnungsrahmen für Datenmärkte?'

data can be used by many firms, (b) data are a key input for innovation, and (c) the lack of access to data can have negative effects on competition and innovation. In the meantime, there is a broad consensus that – in addition to facilitating voluntary data-sharing between firms and opening public sector data – it might be necessary also to have mandatory solutions for access to (or sharing of) data sets that are held by private firms. Most prominent in that respect are the current discussions (and legislative proposals) about facilitating access to data, either directly through competition law or indirectly through improving data portability.[2]

In this general discussion about mandatory solutions for the access to privately held data sets, two basic questions can be distinguished: (1) Under what conditions should data-holding firms have obligations to grant access to these data? (2) What legal instruments should be used for implementing and enforcing those obligations? It is the first question which so far has been at the centre of the policy discussion. Despite a general heated discussion about the justification of mandatory data access solutions, in the meantime, a basic consensus seems to be emerging about the most important criteria that are relevant for deciding under what conditions data-holding firms might have such data access obligations. Benefits through more innovation and competition, incentives for the production of data, protection of business secrets and privacy (compliance with GDPR), whether data claimants have participated in the production of data (co-generated data, e.g. in value chains) or bargaining power imbalances between firms are important criteria that can be included in a comprehensive

---

(2018) Neue Juristische Wochenschrift 275; Communication from the European Commission of 25 April 2018 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – 'Towards a common European data space' COM(2018) 232 final; Heike Schweitzer, 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung' (2019) Gewerblicher Rechtsschutz und Urheberrecht 569; OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies* (OECD 2019); Communication from the Commission of 19 February 2020 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – A European strategy for data, COM(2020) 66 final.

2 See for competition policy Heike Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen* (Nomos 2018); Jacques Crémer, Yves-Alexandre de Montjoye, Heike Schweitzer, 'Competition Policy for the Digital Era' (2019) 91–107 <http://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 31 August 2020; Heike Schweitzer and Robert Welker, 'A legal framework for access to data – A competition policy perspective', in this volume.

balancing of the positive and negative effects of obligations for data access and data-sharing.[3] An important result of the discussion is that depending on the specific technological and economic conditions and the type of data a wide range of results is possible with regard to the extent that obligations for data access and data sharing can be recommended.

This article focusses on the second basic question: Assuming that certain obligations for data access and data-sharing can be recommended, how should these mandatory data access solutions be implemented? Therefore this article presents an analysis of the legal and regulatory instruments for solving data access problems in the data economy. Part B, which follows, gives an overview of the broad range of policy options that are under discussion (competition law, the data portability right of Article 20 GDPR,[4] contract law or unfair trading law). Data access claims against private firms can therefore be based upon general legal rules that apply to all sectors (horizontal data access solutions). However, they can also be the result of sector-specific regulations, as, e.g., the sectoral regulation for the access to bank account data in the Second Payment Services Directive (PSD2).[5] Such sector-specific solutions are also discussed for the data in connected cars or for data in energy markets. One of the main questions in this discussion is whether horizontal or sectoral access solutions might lead to better results. Therefore part B will also entail an analysis of the most important advantages and problems of both types of data access solutions.

The main thesis of this article, however, is that a narrow focus on the question whether data-holding firms might have an obligation to grant other firms access to data might not be sufficient for solving the problems for innovation and competition, and that therefore a broader approach for

3 See, for example, Schweitzer and others (n. 2) 158–162; Crémer and others (n. 2) 74; Schweitzer (n. 1); Wolfgang Kerber, 'Data-sharing in IoT Ecosystems and Competition Law: The Example of Connected Cars' (2019) 15(4) Journal of Competition Law & Economics 381, 400–402; and from a more general perspective Datenethikkommission, 'Gutachten der Datenethikkommission' (2019) 90–91, 145–147 <www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=427D953199879513E7B9E0C2544E921E.2_cid364?__blob=publicationFile&v=6> accessed 31 August 2020.

4 Regulation (EU) No. 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, [2016] OJ L119/1.

5 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the Internal Market [2015] OJ L337/35.

finding proper data governance solutions is necessary. Particularly the analysis of the sector-specific data access solutions shows (1) the need for a more comprehensive analysis of data governance problems which takes into account the working of entire sectors or ecosystems, as well as (2) the importance of additional regulations, eg on interoperability (and standardisation), and safety and security, for ensuring the effectiveness of data governance solutions (part C). The main part D offers a more systematic framework for the analysis and design of entire data governance systems, which at an abstract level refer to all rights and legal rules that are relevant for data in a certain system. After section I distinguishes between the general data governance system of the entire economy and specific data governance systems for certain sectors or parts of the economy, section II emphasises the need for a deep analysis of the working of (often interrelated) markets and entire ecosystems in the digital economy. Here the analysis should particularly focus on the effects of (sometimes multiple) market failures and the question which data governance solutions and additional regulations might be suitable and necessary for solving the problems. The final section III of this part offers an overview of instruments that can be very helpful in general and specific data governance systems. This encompasses consumer data rights, data trustee solutions, and complementary regulatory solutions for interoperability and standardisation as well as for safety, security, and privacy problems. The final brief part E on further perspectives emphasises the need for a more anticipatory approach to data governance solutions and discusses open institutional questions.

B. Horizontal vs. sectoral data access solutions

I. Horizontal data access solutions

Horizontal solutions for facilitating data access and data sharing refer to legal rules that apply to the general economy and not only to specific sectors. Proposals that intend to facilitate generally voluntary data-sharing and the development of well-functioning data markets, eg by reducing transaction costs, can also be seen as such horizontal solutions, but here our analysis will be limited to mandatory solutions for data access to data

that are held by private parties, usually firms.[6] In the general debate about data access a broad range of different horizontal solutions have been discussed. It cannot be the task of this chapter to analyse all of these solutions or even compare them with respect to their suitability, effectiveness, and specific problems. Instead we focus on the most important ones, i.e. on solutions based upon competition law, data portability rights, and some other solutions including, e.g., contract law. After a brief overview of these solutions, the general advantages and problems of horizontal solutions will be discussed.[7]

The most prominently discussed solutions are based upon competition law,[8] because the well-established 'essential facility' doctrine (EFD) seems already to offer a direct way in which firms might obtain access to data sets of dominant firms if they are essential for entering markets and/or for innovation. Despite a broad consensus that data sets can under certain conditions be such an essential facility, there has been broad scepticism in the literature concerning to what extent the EFD, which, e.g., in the EU (according to Article 102 TFEU) has been traditionally applied in a very restrictive way, can be used for solving competition problems that are caused by lack of access to exclusively held data of private firms. However, there are a number of proposals on making this approach, that the refusal to grant access to data can be seen as an abusive behaviour of a firm with market power, more effective. They range from proposing to apply the EFD more flexibly with regard to data (which can be justified from an economic perspective),[9] to develop a reasoning for such an abusive behaviour outside of the EFD (based, e.g., upon a leverage-of-market-power and foreclosure-of-competitors argument),[10] or to base such data access claims on the prohibition of abusive behaviour of firms with relative market power

6 See for ways to facilitate voluntary solutions, including through model contracts, Commission COM(2017) 9 final (n. 1); and most recently Bertin Martens and others, 'Business-to-Business Data Sharing: An Economic and Legal Analysis' (2020) JRC Digital Economy Working Paper 2020–05 <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc121336.pdf> accessed 31 August 2020; and for the problem of opening public sector data Heiko Richter, 'The law and policy of government access to private sector data ("B2G data sharing")', in this volume.

7 For this analysis we will assume that under certain conditions granting access to data can be recommended from a policy perspective according to a set of criteria that have to be applied for justifying the access to these data in particular cases.

8 See for the following Kerber (n. 3) 395–422; see, in particular, also Schweitzer and Welker (n. 2).

9 See Schweitzer and others (n. 2) 171.

10 See Crémer and others (n. 2) 98.

(dependency concept), which implies that the data-holding company does not need to be a dominant firm (according to Article 102 TFEU). In the current draft proposal of the 10th amendment of German competition law new provisions can be found for facilitating the access to data from firms with market power.[11] Despite general broad support for facilitating more data access through competition law, it is so far unclear to what extent these efforts will be successful and able to lead to effective solutions for the data access problems.[12]

In the recent discussion the data portability right according to Article 20 GDPR is viewed as a potentially very promising option for solving data access problems. The basic idea is that the consumers can exert their right to the portability of their personal data to give access to such data that are held by one firm (e.g. a social media platform) to other firms, either for easier switching of services or for allowing the offering of additional complementary services that require access to these personal data. It is important that this data portability right of the GDPR has always been seen as a potential vehicle for facilitating competition (through reducing lock-ins caused by high switching costs). However, there is also a broad consensus that so far this right has not led to effective solutions, because of an unclear (and also insufficient) scope of this right, large technical and other feasibility problems, and too high transaction costs for consumers. The data portability right encompasses neither the right to the portability of data in real time nor does it contain interoperability requirements for ensuring the technical feasibility of data portability. Therefore it is not surprising that the discussion is shifting to the question of how this data portability right in the GDPR can be made more effective.[13] However data portability rights can also play a role independent of Article 20 GDPR (and therefore

11 Bundesregierung, 'Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0' (8 September 2020) <www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&v=4> accessed 11 September 2020; see also Kerber (n. 3); Wolfgang Kerber, 'Datenzugangsansprüche im Referentenentwurf zur 10. GWB-Novelle aus ökonomischer Perspektive' (2020) 05 Wirtschaft und Wettbewerb 249.

12 See for the problems in competition law Kerber (n. 3) 403–407, 412–413, arguing that competition law solutions (even after legislative amendments like that in German competition law) can help, but only to a certain extent.

13 See for the discussion about the data portability right of the GDPR Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability as last revised and adopted on 5 April 2017' (16 EN, WP 242 rev.01) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233> accessed 31 August 2020;

outside of privacy laws), as is shown in the new discussion about consumer data rights.[14] It focusses on the question of what rights (especially with respect to access and portability) consumers should have regarding data that are collected as part of their role as consumers. Since the concept of consumer data can be independently (and more broadly) defined than the legal concept of 'personal data' in privacy laws, the consumer data rights approach allows for a much broader and open discussion on which of 'their' data consumers can make accessible in what form to other firms through exerting these rights against firms that hold their consumer data. Since however legislation on consumer data rights is still in its earliest stages, it is too early to make assessments about the effectiveness of such solutions.[15]

Commission Communication COM(2020) 66 final (n. 1) 10, 21 (about enhancing the data portability right under Art. 20 GDPR); for recent discussions see Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1356; Kommission Wettbewerbsrecht 4.0, 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft' (2019) 39–44 <www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/bericht-der-kommission-wettbewerbsrecht-4-0.pdf?__blob=publicationFile&v=12> 31 August 2020; Jan Krämer, Pierre Senellart and Alexandre de Streel, 'Making Data Portability more effective for the Digital Economy – Report' (Centre on Regulation in Europe 2020) <https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/> accessed 31 August 2020; and in particular Ruth Janal, 'Data portability under the GDPR: A blueprint for access rights?', in this volume, who is very sceptical that the data portability right according to Art. 20 GDPR can be a model for B2B data access solutions.

14 See for the discussion about consumer data rights OECD, 'Consumer Data Rights and Competition – Background Note' (OECD 2020) DAF/COMP(2020)1 <https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf> accessed 31 August 2020, which was triggered much by their introduction through legislation in Australia (see Louisa Specht-Riemenschneider, 'Data access rights – A comparative perspective', in this volume). Interesting in the Australian case is that it primarily adopts a horizontal approach that is however implemented step-by-step in a sector-specific way (hybrid of a horizontal and sectoral solution).

15 The consumer data rights approach is also very close to the proposal of Josef Drexl of nonwaivable data access rights for consumers with regard to data of connected devices. See Josef Drexl, 'Data Access and Control in the Era of Connected Devices' (2018) and Josef Drexl, 'Connected devices – An unfair competition law approach to data access rights of users', in this volume; see also Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's "Public Consultation on Building the European Data Economy"' (2017) <www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf> accessed 31 August 2020.

Beyond these two most discussed solutions a number of other options can also be found which might be applicable under specific conditions. For example, under certain conditions contract law might be capable of offering firms access to data as part of their contractual relationships with other firms, especially if the data claimant has participated in the generation of these data (co-generated data).[16] Also discussed is the option that data access claims might also be based upon unfair trading laws, especially in cases of unequal bargaining power between the data claimant and the data holder, i.e. the refusal to grant access to certain data sets might be seen as an unfair trade practice. However both solutions can only be applied in certain situations and are so far not developed. It is particularly unclear what the criteria are in these fields of the law, but it is important that such data claims might be based upon already existing laws. This is different for other data access/sharing proposals, such as, e.g., the opening of large sets of anonymised data for AI applications and the training of algorithms. Such a proposal can also be seen as a horizontal solution if it is applied to data from all sectors.[17] Particularly interesting are also proposals that combine different horizontal solutions, especially combinations between competition law and data portability rights. The idea of prohibiting the impediment of data portability as an abusive behaviour of firms with market power is a proposal that has emerged repeatedly and in different ways in the competition policy discussion about how to solve data access problems.[18]

16 See Schweitzer and others (n. 2) 181–183; Commission Communication COM(2018) 232 final (n. 1) 9–11 (key principles of B2B data-sharing that should be respected in contractual agreements); Datenethikkommission (n. 3) 28–30 (on unfair/inefficient B2B contracts about data and a legislative proposal for changing German contract law in that respect); for an analysis of data access solutions in general contract law see Axel Metzger, 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', in this volume, who is sceptical about such mandatory access solutions in B2B contexts outside of competition law; see also Michael Grünberger, 'Data access rules: The role of contractual unfairness control of (consumer) contracts', in this volume, about data access through contractual unfair control of consumer contracts.

17 The approach of the European Commission in its strategy for data focusses on a cross-sectoral governance framework. See Commission Communication COM(2020) 66 final (n. 1) 11–25.

18 See, e.g., the proposal of the German Kommission Wettbewerbsrecht 4.0 (n. 13) 6, 54–55 for an EU regulation for dominant platforms that would also entail an obligation of these platforms to enable the portability of user and use data in real time and to ensure interoperability with complementary services.

What are the general advantages and problems of horizontal solutions for data access? There is overall a broad consensus that general rules that can be applied to the entire economy are theoretically preferable over sector-specific rules, due especially to the manifold costs and distortions that can arise through establishing different data access solutions for different parts of the economy. However the academic discussion about data access and data-sharing issues has shown that it is not easy to identify and apply general criteria for granting access to data. Although a general set of relevant criteria is now emerging in the discussion, decisions on whether to grant access to data depend very much on the specific economic and technological context. It has always been one of the counterarguments against general data access rules that their application might not be capable of distinguishing precisely enough between cases in which data access should be granted, and other cases where this is not advisable. Wrong decisions would lead to welfare losses through type 1 and type 2 errors. However, theoretically a differentiated application to the specific conditions of cases is also possible with general rules if a clear set of criteria exists that can be applied to specific cases. Through a process of developing groups and subgroups of cases, the law can develop a differentiated approach with solutions that are sufficiently adapted to the different conditions of different sectors, markets, and technologies. But such a process might take a long time, and depend very much also on who the driving force is behind such a differentiation. Is it a competition authority, which also can make decisions on enforcement priorities and issue guidelines, or is it the result of a process that relies mostly on private litigation and the courts? This implies that also the institutional design of the enforcement of the horizontal rules for granting access to data can be important for the finding of proper solutions and their effectiveness.[19]

There are however a number of additional problems. One important problem that so far has not been discussed much is the question what ac-

19 From an economic perspective the same balancing problem between benefits and problems of data access exists independent of the question which horizontal solution is applied from a legal perspective. Due to the different dogmatic approaches of these different laws and the different enforcement systems, certain horizontal solutions might be better capable of leading to good decisions than others. Therefore, competition law, which is much more familiar with the application of economic reasonings and is primarily enforced by a competition authority, might have relative advantages over unfair trading law or the data portability right of the GDPR. However, different horizontal solutions might also specialise with regard to different kinds of data access problems.

cess to data really means. Does it imply that data are transmitted to other firms (and they are free to use them in any way, or only for specific purposes) or do they only receive access to a server, where their use of the data is monitored (perhaps at a neutral institution)? Depending on the specific conditions of how access to data is given (and what can be done with the data), the benefits and problems of data access can be very different, which implies that horizontal solutions should also be capable of finding suitable solutions for this question. Particularly important is also that data access often only works if (1) data are also made available in a common data format, (2) easy-to-use technical interfaces (such as APIs) are available for transmitting the data, (3) the problem of fees and other conditions for data access is solved, (4) safety/security issues and the compliance with privacy laws (in the EU: GDPR) are dealt with, and (5) the problem of too high (transaction) costs of using these horizontal solutions for the data claimants and/or the consumers (in case of data portability rights) is solved. In a number of important cases, such as in IoT contexts (including connected cars), also (6) additional interoperability problems (due to technically closed systems) might have to be solved. Although this cannot be discussed here in detail, it is very unclear whether horizontal data access solutions as general competition law, the data portability right (Article 20 GDPR), unfair trading law or contract law can solve these additional problems. Very often this will be not possible. Therefore it is right now an open question to what extent the discussed horizontal solutions will be capable of solving the data access problems in an effective way in the foreseeable future.

II. Sectoral data access solutions

Sectoral data access solutions are usually regulatory solutions that try to solve problems of access to data or the sharing of data in a targeted way for specific sectors. In the general discussion about data access solutions, the option of sector-specific regulation has often been seen as a possibly superior solution at least in certain sectors.[20] Before discussing the general advantages and problems of sector-specific regulatory solutions, we will analyse briefly two examples of sector-specific solutions. One example is the data

20 Particularly in the discussion of data access solutions in competition law, it was always acknowledged that in certain sectors a sector-specific regulatory solution can lead to better solutions. See, e.g., Crémer and others (n. 2) 107.

access regime to bank account data that has been established in the banking sector by the PSD2. The other example refers to the current discussion about access to the data of connected cars, in which also a sector-specific regulatory solution is currently on the political agenda and the topic of heated discussion.

1. Opening of bank account data (PSD2)

The basic idea of the opening of bank accounts through the regulatory regime of the PSD2 is to enable new innovative financial services for the customers of banks for their online bank accounts, especially through new Fintech companies.[21] It is about the access of two different types of independent financial service providers, namely payment service providers who offer payment services via the bank accounts of the customers (PIS: payment initiation services), and other providers of financial services who based upon the data from bank accounts can offer additional financial services (AIS: account information services) to the bank account owners. The regulatory regime tries to solve a market failure problem due to insufficient innovation competition between banks regarding new digital financial services and a lock-in problem of customers of traditional banks. Since Fintech companies have problems offering their new innovative services to consumers, because banks can refuse them access to the bank accounts of their customers, a sector-specific regulatory regime obliging banks to give access to the bank accounts has been viewed as necessary for triggering more innovation with regard to these financial services. The decisive problem is that banks have the exclusive control over both the bank account data and the possibility to initiate payments from these bank accounts. Independent financial service providers, who offer services in competition with the banks, are therefore not capable of offering the bank customers their services without the permission of the banks. Therefore this sectoral access

21 See Directive (EU) 2015/2366 (n. 4); for an overview see Heike Mai, 'PSD 2, Open Banking und der Wert personenbezogener Daten' (2018) Deutsche Bank Research <www.dbresearch.de/PROD/RPS_DE-PROD/PROD0000000000470556/PSD_2%2C_Open_Banking_und_der_Wert_personenbezogener.PDF> accessed 31 August 2020; Simonetta Vezzoso, 'Fintech, access to data, and the role of competition policy' in Vicente Bagnoli (ed.), *Competition and Innovation* (Scortecci 2018) 30–41; see also, in particular, Jörg Hoffmann, 'Safeguarding innovation in the framework of sector-specific data access regimes: The case of digital payment services', in this volume.

regime encompasses an obligation of the banks to grant independent financial service providers (with the permission of the bank account holders) access to bank account data as well as the possibility to directly initiate payments from the bank account of the customers. This implies that banks no longer have the right to refuse such access to these data and the bank account by these independent service providers. The basic ideas of the PSD2 are much influenced by the Open Banking initiative of the UK competition authority CMA,[22] and can be interpreted from an economic perspective primarily as an innovation policy measure.

Particularly important for our analysis here is that the PSD2 regulation goes far beyond a pure regulation of data access. It is rather a package of regulatory solutions that consists of a number of important elements:[23]

(1) The account information service providers (AISP) have a right to access the bank account data, and can use them for offering additional financial services.
(2) The payment initiation service providers (PISP) have the right to access the bank account of a customer and directly initiate payments from this account.
(3) Since both forms of access require direct technical access to the bank account, the banks must provide open interoperable interfaces for these service providers. Here some form of standardisation (eg APIs) is required.[24]
(4) The banks are not allowed to demand fees for the access of these financial service providers.
(5) For increasing the security of the bank customers (as part of consumer protection) the regulation also includes additional requirements: (a) strong authentification of the bank customers (double authentification), (b) licensing of the financial service providers, and (c) liability of the bank (for mistakes and fraud).

---

22 UK Competition & Markets Authority, 'Retail banking market investigation – Provisional decision on remedies' (2016) <https://assets.publishing.service.gov.uk/media/573a377240f0b6155900000c/retail_banking_market_pdr.pdf> accessed 31 August 2020; Open Banking <www.openbanking.org.uk/> accessed 31 August 2020.

23 See European Commission Fact Sheet, 'Payment Services Directive (PSD2): Regulatory Technical Standards (RTS) Enabling Consumers to Benefit from Safer and more Innovative Electronic Payments' (2017) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_17_4961/MEMO_17_4961_EN.pdf> accessed 31 August 2020.

24 There are still considerable problems regarding its practical implementation.

(6) The European Banking Authority has the regulatory oversight for this regulatory regime.

Since this Directive had to be transposed into national law, it is currently in different stages of implementation in the Member States. The pros and cons of this regulation for opening bank accounts in order to stimulate innovative financial services cannot be discussed here. But what is important is that it is widely seen as a regulatory model for supporting data-driven innovation through opening data. However there is also considerable criticism with respect to the details of the regulation and the question to what extent the regulation can achieve its objectives.[25]

2. *Access to data in connected cars*

The technological transition to connected cars (as an example of an IoT device), in which huge amounts of data are collected and produced in the car and directly transmitted to proprietary servers of the car manufacturers, has triggered a new regulatory discussion about 'access to in-vehicle data and resources'.[26] Independent service providers that want to offer aftermar-

---

25 See for a positive view and emphasis on its model character, e.g., Jason Furman and others, 'Unlocking digital competition – Report of the Digital Competition Expert Panel' (2019) 69 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf≥ accessed 31 August 2020. One of the important critical concerns is with the danger that large digital tech firms (e.g. Apple, Google) can use this data access for entering the market with potentially negative effects in the long term: See Miguel de la Mano and Jorge Padilla, 'Big Tech Banking' (2018) 14 Journal of Competition Law & Economics 494. Since these large platform firms do not have to open their data, demands for reciprocity of data access have emerged: See Fabiana Di Porto and Gustavo Ghidini, '"I Access Your Data, You Access Mine" – Requiring Data Reciprocity in Payment Services' (2020) 51 International Review of Intellectual Property and Competition Law 307; see also the critical analysis of Jörg Hoffmann, 'Safeguarding innovation in the framework of sector-specific data access regimes: The case of digital payment services', in this volume.

26 See as an overview: C-ITS Platform, 'Final Report' (2016) <https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf> accessed 31 August 2020; TRL, 'Access to In-Vehicle Data and Resources – Final Report' (2017) <https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf> accessed 31 August 2020; Commission Communication COM(2018) 232 final (n. 1); Wolfgang Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data' (2018) 9

ket and other new innovative complementary services in this new ecosystem of connected cars to the car users are very concerned that the car manufacturers can use their monopolistic gatekeeper position to the data and to the car for controlling all markets for aftermarket and other complementary services that need access to these data and/or access to the car (e.g. providing remote repair and maintenance services). This can lead to the foreclosure of independent service providers and the leveraging of market power to these secondary markets in this new digital ecosystem of connected cars. This gatekeeper position is the consequence of the application of the 'extended vehicle concept' by the car manufacturers, which implies that they have exclusive de facto control of (1) all data produced in the car and (2) the technical access to the car, ie without the permission of the car manufacturer no access is possible to these data or the car. An economic analysis of this situation comes to the clear result that the concerns of the independent service providers are justified, and that therefore this gatekeeper position can lead to serious problems for competition, innovation, and consumer choice on these secondary markets.[27] Since 2016, the independent service providers have been demanding a regulatory solution for this problem. The European Commission has acknowledged this problem but has not yet made proposals for solving it.[28]

Journal of Intellectual Property Information Technology and E-Commerce Law 310.

27 See for an economic analysis of this access problem Kerber (ibid), which is based upon a systematic analysis of market failures in the ecosystems of connected cars; see also from an economic perspective Bertin Martens and Frank Mueller-Langer, 'Access to Digital Car data and competition in aftermarket maintenance services' (2020) 16(1) Journal of Competition Law & Economics 116.

28 See for contributions to this policy discussion C-ITS platform (n. 26); TRL (n. 26); Kerber (n. 3, n. 26); Wolfgang Kerber and Daniel Gill, 'Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation' (2019) 10 Journal of Intellectual Property Information Technology and E-Commerce Law 244. See for position papers of stakeholders ACEA, 'Access to Vehicle Data for Third-Party Services – Position Paper' (2016) <www.acea.be/uploads/publications/ACEA_Position_Paper_Access_to_vehicle_data_for_third-party_services.pdf> accessed 31 August 2020, BEUC, 'Protecting European Consumers with Connected and Automated Cars – Position Paper' (2017) <www.beuc.eu/publications/beuc-x-2017-138_dve_beuc_connected_autonomous_cars.pdf> accessed 31 August 2020, FIGIEFA, 'Commission Communication on "Free Flow of Data." Input from the Independent Automotive Aftermarket' (2016) <www.figiefa.eu/wp-content/uploads/Free-Flow-of-Data-FIGIEFA-Input-2016_12_23.pdf> accessed 31 August 2020; FIA, 'Policy Position on Car Connectivity' (2016) <www.fiaregion1.com/wp-content/uploads/2017/05/20160412fia_policy_brief_on_car_connectivity_fin.pdf> accessed 31 August 2020. After the acknowledgment

It is important to note that in the motor vehicle industry competition policy had to deal for decades with attempts of car manufacturers to foreclose independent repair and maintenance service providers from the lucrative markets for repair and maintenance services.[29] Therefore a long time ago EU competition policy already introduced a regulatory access regime for protecting competition on the automobile aftermarkets. This regime has granted independent service providers access to essential repair and maintenance service information for protecting competition between the authorised dealers of the car manufacturers and the independent providers of repair and maintenance services (including independent spare part producers). Since 2007 this access regime was included in the motor vehicle type approval regulation, which was reformed in 2018.[30] This current access regime to essential repair and maintenance information entails a FRAND-like obligation of the car manufacturers to make this information available in a non-discriminatory way, with 'reasonable and proportionate' fees, and in a standardised format. This regulation also includes standardisation of technical specifications for the access to this information (e.g., via websites and an obligatory on-board diagnostics (OBD) adapter in the car for diagnostic data). Also safety and security concerns are addressed in this regulatory regime, because repair and maintenance service providers need certification and approval for getting access to security-relevant information. However this current type approval regulation (even after its reform in 2018) has not been adapted to the new technological conditions of connected cars, and therefore cannot solve the competition problems caused by the new gatekeeper position of the car manufacturers with their exclusive control over access to the in-vehicle data and the car.[31]

---

of this competition problem in 2018 – see Communication from the Commission of 17 May 2018 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – on the road to automated mobility: An EU strategy for mobility of the future COM(2018) 283 final, 14 – the Commission has announced a further review of the type approval legislation in its European data strategy; see Commission Communication COM(2020) 66 final (n. 1) 28.

29 See for the following in more detail Kerber and Gill (n. 28).

30 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, [2007] OJ L171/1.

31 See for an in-depth critique of the 2018 reform of the type approval regulation Kerber and Gill (n. 28).

What are the most important policy options that have been discussed for solving this problem?[32] The problem of 'access to in-vehicle data and resources' has always been seen as a problem that might be solved best through a sector-specific regulatory approach. One solution is the 'shared server'.[33] Technically it would, like the extended vehicle concept, also imply the transmission of all data to an external server but this server would be under the governance of a neutral institution for making these data available to all stakeholders in the ecosystem of connected cars (with certain principles, such as, e.g., non-discrimination) for enabling competition and innovation in the entire ecosystem of connected cars. This could be seen as a data trustee solution and would eliminate the gatekeeper position of the car manufacturers with respect to the data, but it would not solve the problem of lacking interoperability with the car. Therefore independent service providers would in the medium and long term prefer the transition to open interoperable telematic platforms (on-board application platforms), which would allow the storage of the data in the car and enable the owners of the car to decide whom they give access to the data and access to the car. For such open interoperable telematic platforms standardised technical interfaces would be necessary, as well as a sophisticated safety and security architecture, which would allow independent service providers to directly access the car, e.g. for performing remote services, without compromising the safety and security of the car. The car manufacturers have always argued that only their exclusive control of the technical access can ensure a high level of safety and security, but studies have shown that the safety and security problems can also be solved with open interoperable telematic platforms.[34] One relatively easy regulatory short-term solution, based upon the current technological design of connected cars, would be a comprehensive reform of the type approval regulation by (a) extending the mandatory access regulation to a much broader set of data, namely all data that are necessary for other service providers in the ecosystem of connected cars (and also beyond aftermarket services), (b) requiring standardised technical interfaces (for solving the interoperability problem), and (c) introducing a sophisticated safety and security solution to enable independent service providers to directly access the car in order

32 In Kerber (n. 3) it is analysed to what extent data access claims based upon competition law can be used for solving this problem of access to data in connected cars (as an alternative horizontal solution).

33 See for an overview and comparison of different technological options for access to data TRL (n. 26) 32–49.

34 See TRL (n. 26) 77.

to perform their services.[35] However, a transition to open interoperable telematics platforms, which would require a far-reaching standardisation of technical interfaces, would offer a much better perspective for good solutions.[36]

What are the general advantages and problems of sector-specific data access solutions? The most important advantage might be that with rules that are tailored to the specific economic and technological conditions of a sector, a much better balancing of the many trade-offs with regard to an optimal governance of data is possible. It can allow for better differentiation between different groups of stakeholders within the systems, such as, e.g., the traditional banks, the new innovative financial service providers, and the consumers (as bank account holders). Therefore it can be specifically regulated who should get access to what kinds of data, and under what conditions (e.g. with regard to fees). Additionally, it can be better decided what specific technological, safety/security, and privacy protection requirements have to be fulfilled, and how this should be implemented in this specific sector. This is directly linked to the possibility that such a sector-specific data governance solution often has an explicit regulatory character, which allows for setting ex ante rules (instead of ex-post control as, e.g., in competition law) and the use of a regulatory authority that can monitor and enforce the sector-specific regulation, and might also have some rule-

35 See Kerber and Gill (n. 28) 254–56. This solution would be technically based upon the 'extended vehicle concept' but the extended type approval regulation would give the independent service providers both broad access to the car data and access to the car for remote services. Since the European Commission has announced a review of the current EU type approval legislation to open it up to more car-data-based services, it might use this policy option of extending this already existing regulatory access regime to enable more competition and innovation in the ecosystem of connected cars. See Commission Communication COM(2020) 66 final (n. 1) 28.

36 This is also the recommendation of the TRL study (n. 26) 160. For an analysis that this wrong technological choice by car manufacturers can be the result of a market failure about choosing a too low level of interoperability (and not enough standardisation) see Kerber (n. 26) 322. For the economics of interoperability and standardisation that support the possibility of such a market failure due to wrong incentives to choose too-closed systems see Joseph Farrell and Timothy Simcoe, 'Four Paths to Compatibility', in Martin Peitz and Joel Waldfogel (eds), *The Oxford Handbook of the Digital Economy* (2012) 34, and Wolfgang Kerber and Heike Schweitzer, 'Interoperability in the Digital Economy' (2017) 8(1) Journal of Intellectual Property Information Technology and E-Commerce Law 39, 41–48.

making powers for adapting the rules over time.[37] Recently, it was the Furman report that emphasised the potentially large advantages of setting ex ante rules for a faster clarification of rules, particularly also with respect to opening data sets and open standards.[38]

However, sector-specific regulatory data access solutions also face a number of difficult problems. First and foremost, all the well-known general problems of regulatory solutions have to be taken into account. Do the rule-makers (legislature, regulatory authority) have sufficient knowledge for designing a well-adapted and effective regulatory regime? Can we rely on a regulatory authority to effectively enforce the regulations? Particularly critical regarding sector-specific regulations is the problem of 'regulatory capture', ie that important stakeholders in the sector might use their closeness to policy-makers to influence the regulation in favour of their own interests (rent-seeking behaviour), leading to wrong regulations that do not achieve (sufficiently) the intended policy objectives of more competition and innovation (regulatory failure).[39] Particularly important is also the problem of how a specific regulatory data access regime with ex ante rules can be adapted to the fast-changing economic and technological conditions due to the rapid technological change through innovations. This implies both the problem that an existing regulatory regime should not impede innovations and, vice versa, that innovations can render an old regulatory regime outdated and ineffective. In the fast-changing digital economy this is a huge challenge for sector-specific data access regulations. An additional important problem is that sector-specific regulatory access solutions will only be possible for a limited number of sectors, i.e. it is not possible to develop them for all parts of the economy. This implies that it will always be necessary to have horizontal data access solutions in addition to these sector-specific solutions. The resulting patchwork of different data access solutions can also lead to numerous problems, such as, e.g., problems with the proper delineation of the scope of these specific solutions and problems of asymmetric regulation.

37 Theoretically it is not necessary that sector-specific data access rules must be in the form of a regulatory regime with ex ante rules.

38 See in detail Furman and others (n. 25) 54–83. The Furman report also emphasised that these ex ante rules should primarily be developed in collaboration with the stakeholders.

39 See George J. Stigler, 'The Theory of Economic Regulation' (1971) 2 Bell Journal of Economics and Management 3.

C. From data access solutions to data governance systems

The results of part B have shown that both horizontal and sectoral data access solutions have advantages and problems, and it depends therefore on the type of data access problems and the specific technological and economic conditions, whether using a horizontal or a sectoral data access solution might be more advisable. One option for continuing this analysis would be to analyse more deeply the types of data access problems and the conditions for which (what kind of) horizontal solutions or sectoral solutions should be chosen, and how the specific design of these solutions should look. This would also include a discussion of the proper design of the enforcement system for these data access solutions. However, for this article a different path of inquiry has been chosen. The main thesis is that for a proper understanding of data access problems and finding effective solutions we have to use a broader approach that goes beyond the direct solution of the data access problem itself. Instead we have to think in terms of data governance systems. Before discussing in a more general way the basic architecture and building blocks of such data governance systems in part D, three important lessons can be learnt about the need for such a broader approach from our analysis of sector-specific data access solutions in part B.

(1) We cannot understand data access problems and their solutions if we only look at the bilateral relation between a data holder and a data claimant, and are trying to balance the benefits and costs of data access. This is a serious problem for all horizontal solutions, especially in combination with private litigation, in which the data claimant has to sue the data holder for access to data. Instead, the discussion of sector-specific solutions (PSD2 and connected cars) shows clearly that it might be necessary to analyse the working of an entire sector (or ecosystem) in order to understand the effects of the exclusive control of data by a data holder on a number of different (and often interrelated) markets, and the benefits and costs of different governance solutions for data for achieving the objectives of more competition and innovation. From an economic perspective this requires a careful analysis of the market failures in these sectors, which in addition to competition and innovation problems can also encompass informational and behavioural problems of consumers or wrong technological

decisions of firms with respect to standardisation and interoperability.[40] For example, in the case of the governance of data in connected cars, it is very important to understand the far-reaching effects of the monopolistic gatekeeper position of the car manufacturers on all secondary markets for aftermarket and complementary markets, and its implications for foreclosing independent service providers and leveraging market power. This does not mean that such a deep analysis into the markets should (always) be done in the application of horizontal solutions (which would not be feasible), but in choosing the specific criteria that are applied in horizontal solutions for data access (or data portability) one should consider this problem of the broader effects of granting or denying data access in the wider market context on competition and innovation.

(2) Data access discussions nearly always implicitly assume that the de facto control of a certain set of data by a firm is legitimate (in a similar way as we assume the legitimacy of the ownership of a physical 'essential facility'), and the relevant question is only whether other firms should also gain access to these data of this firm. However the discussion in our two examples shows that it might also be necessary to ask who should be in control of these data in the first place, ie we might also have to ask about the proper initial allocation of the de facto control of (or the rights in) these data. The data governance regime established by the PSD2 can also be interpreted as the definition and assignment of a new right to the owner of an online bank account to make the data of her bank account available to independent financial service providers as well as allowing payment service providers to initiate payments directly from this bank account without the permission of the bank. Therefore this regulatory regime not only defines and assigns an access right to independent service providers (with the consent of the bank account owners), but also reassigns the rights in the bank account data from a de facto exclusive control of the bank to the owner of the bank account (in the form of an additional right to data portability and interoperability).[41] Also, the policy discussion in the case of the data of the connected car is directly linked to this aspect of the initial allocation of the

40 Regarding the problem of the governance of data in connected cars, it could be possible to identify all of these market failure problems, see Kerber (n. 26) 316–25.

41 Very important in this respect is that the regulation does not allow the waiving of this additional right in the contractual relationship between the bank and the consumers as bank account owners. Otherwise the entire regulation might not work in the intended way. Emphasising the importance of the nonwaivability of data access rights see Josef Drexl and others (n. 14).

de facto control of (or rights in) the car data and the technical access to the car. The car manufacturers with their technological decision in favour of the 'extended vehicle' concept have allocated the exclusive de facto control of the data and access to the car to themselves (leading to a de facto 'appropriation' of the data). The alternative policy option of introducing the different technological solution of an open interoperable telematics platform would allow an initial allocation of the de facto control of the data and access to the car to the car owners. This also shows clearly that different technological solutions can lead to very different data governance solutions.[42]

(3) The third lesson to be learnt from sector-specific data access solutions refers to the problem that in many cases additional regulatory solutions are needed for making data access solutions effective, i.e. to achieve the intended effects of protecting or enabling competition and innovation. Therefore data access rules might have to be complemented by additional regulatory solutions. For example, the PSD2 data access regime addresses not only access to the bank account data but also stipulates that independent payment service providers can directly initiate payments from the bank account of the consumers, which requires that the banks offer a standardised technical interface (e.g. APIs) for enabling the interoperability of this complementary service with the bank account. A regulatory solution for interoperability might also be necessary in the example of connected cars, because certain complementary services of independent providers (e.g. remote repair and maintenance services) are only possible if the car manufacturers offer a standardised technical interface to enable the performing of such services. Also, safety and security concerns play an important role in both examples. Giving independent service providers access to data and enabling them to directly perform services can lead to additional risks for safety and security that require sophisticated solutions, such as mandatory certification of the independent service providers. Other regulations to help make these access regimes effective include the regulation of access fees and other access conditions such as non-discriminatory access.

The important insight from these three different lessons from sector-specific data access regulations is that it is often not enough to focus only on the direct data access problem itself, but it is necessary to use a broader analytical framework that allows for a more systematic analysis of data governance problems and a potentially broad set of legal and regulatory solu-

42 See Kerber (n. 26) 317 and also generally Datenethikkommission (n. 3) 15, emphasising that technology and its design can be used as a governance instrument.

tions for dealing in an effective way with data access problems. In the following part D, such a broader approach to analyse and design data governance systems for solving data access/sharing problems will be presented.

D. Data governance systems: Basic approach and instruments

I. General and specific data governance systems

One of the important results of the discussions about data rights in recent years is that the initial approaches of either introducing exclusive property-like rights on data or focussing primarily on simple access to data does not reflect enough the complex and context-dependent effects of the role and impact of data in the digital economy. There are no simple general 'one size fits all' solutions as to what data rights should look like. Rather, depending on the type of data and specific conditions, very different data governance solutions might be optimal. This can range from open data (public domain), through a multitude of different intermediate solutions, which might assign different rights in a set of data to different groups of stakeholders, to the other extreme solution of strict exclusive rights. From an economic perspective a 'bundle of rights' approach might be best suited for describing and analysing the vast scope of possible solutions concerning who should have what rights for what purposes in certain sets of data (or data streams). In the PSD2 example we have seen how the bundle of rights in online bank account data are defined and assigned to the different stakeholders, banks, bank account owners, and financial service providers. The 'bundle of rights' approach is a very flexible instrument that has the additional advantage of not being biased in favour of either the property (exclusionary) aspect or the access (sharing) aspect of data.[43] The same is true for using the broad and open concept of 'governance' of data.

43 The 'bundle of rights' approach goes back to the economic theory of property rights, which deconstructed 'property' as consisting of a bundle of rights with regard to an object, and asked for the economically efficient definition of such a bundle of rights. See for the property rights theory Armen A. Alchian and Harold Demsetz, 'The Property Right Paradigm' (1973) 33(1) The Journal of Economic History 16. For a focus on the analysis of 'rights in data' instead of an exclusive property-like right in data with the idea that in a multi-stakeholder situation as in the case of data of connected cars different stakeholders can have (different) rights in the same data see Kerber (2017) (n. 1) 127–31.

A data governance system refers to the entire set of rights and legal rules (and regulations) that are relevant for collecting, processing, analysing, using, sharing, and selling data in a certain system.[44] One can distinguish between the general data governance system of an entire economy and specific data governance systems for particular sectors, ecosystems, or other clearly delineated domains within an economy. The general data governance system of an entire economy encompasses all general rules that are relevant for data. In the EU this entails, in particular, the GDPR with the entire set of rights that are granted to persons with regard to their personal data, but also the many different rights and legal rules that are relevant for other data as well, such as civil law, IP law, competition law, consumer law, etc. All legally defined general rights in data and general legal rules and regulations that influence and shape the bundles of rights on collecting, processing, analysing, sharing, using and selling data can therefore be seen as part of the general data governance system of an economy. Therefore the horizontal data access solutions (using competition law, the data portability right of Article 20 GDPR, unfair trading law etc., as discussed in section B.I.) are part of this general data governance system. The current policy discussions about facilitating horizontal data access solutions (e.g. through an amendment of German competition law or enhancing the data portability right of Article 20 GDPR) intend to improve the general data governance system.[45]

Specific data governance systems refer to the specific sets of rights and legal rules that are relevant for data in a specific part of the economy. This can be a traditional industry or sector (or part of a sector), a digital ecosystem or platform, or an otherwise clearly delineable part of the economy, for which specific legal rights or rules for data exist that differ from the general rules about data. Sector-specific data access solutions, as have been discussed in part B, can therefore be seen as specific data governance sys-

44 The set of rights and legal rules of a data governance system can also be called a data governance regime. See Wolfgang Kerber and Severin Frank, 'Data Governance Regimes in the Digital Economy: The Example of Connected Cars' (2017) <https://ssrn.com/abstract=3064794> accessed 31 August 2020.

45 The set of rights and rules of the general data governance system can therefore also be seen as part of the general legal framework of the market economy, or, in the German ordoliberal approach, the so-called *Ordnungsrahmen* (economic order). Therefore the general data governance system can also be called *Datenordnung* and policies for improving this general set of rights and rules on data can be interpreted as *Ordnungspolitik*. See for this ordoliberal approach Viktor J. Vanberg, 'Freiburg School of Law and Economics', in Peter Newman (ed.), *The New Palgrave Dictionary of Economics and the Law*, Vol. 2 (MacMillan 1998) 172.

tems. The discussion about horizontal vs. sectoral data access solutions can then be reframed as a discussion about the question whether data governance problems should be solved through the rules of the general data governance system or by introducing a specific data governance system that leads to a different bundle of rights on data in this delineated part of the economy. The data-relevant rights and legal rules in a specific data governance system are usually a combination of (a) a set of system-specific rights and rules and (b) the rules of the general data governance system. For example, in the PSD2 regulation the additional rights on access to bank accounts and bank account data for bank account owners and financial service providers only apply to online bank accounts, and only with regard to a limited number of financial services, such as payment services and account information services. For all other data of bank customers, other bank accounts, or other services the general rules and not this specific set of rights and rules apply. One of the difficult questions in introducing specific data governance systems is therefore not only whether such a specific data governance system should be implemented and how to design the respective specific rights and rules. It is also necessary to delineate the scope of the specific data governance system, i.e. one must carve out for what part of the banking sector such a specific data governance system should be implemented, and which parts should remain under the rules of the general data governance system.

II. Market failures and policy objectives

What methodological approach should be used for analysing and designing data governance systems? In the discussion about granting access to data or sharing data, a number of criteria have emerged that are seen as relevant for deciding whether a claim for data access or data-sharing should be granted or not. As already mentioned in the introduction, these are: the benefits through more competition and innovation, incentives for the production of data, whether data claimants have participated in the production of these data, protection of business secrets and privacy (GDPR), bargaining power asymmetries between firms, and also public interests.[46] However, for the application of such a list of criteria it is necessary to analyse the effects of data access problems and data governance solutions with regard to these criteria. The problem is that all the relevant effects of differ-

46 See again the references (n. 3).

ent data governance solutions, ie whether we accept the exclusive control of data by data holders or grant access to other firms (via competition law or regulation), or introduce (or improve the effectiveness of) data portability rights can have many different effects on different markets, especially if opening data also leads to new innovations and the creation of new markets. Particularly the new economic and technological characteristics of the digital economy, in which markets can be interrelated in complex ways, such as in digital ecosystems with primary and secondary markets, and potentially large economies of scope between products and services within the ecosystems, might make deep economic analyses of the effects of different data governance solutions necessary.[47] Since in the digital economy the markets are much more linked with each other than before the digital transformation, the analysis of such effects as well as the delineation of separate sectors for introducing specific data governance systems has become much more difficult.

From an economic perspective the analyses should focus primarily on market failures and how to remedy them by using data governance solutions and other policies such as competition law, consumer law, data protection (privacy) law, standardisation policy, or direct regulatory solutions.[48] The most important market failure problems that are relevant with regard to data issues are competition problems (foreclosing competitors and leveraging market power through gatekeeper positions through exclusive control of data, lock-in problems, or quasi-monopolistic platform markets), information and behavioural problems of consumers (through intransparency about the collection and use of data by data-collecting firms, high transaction costs of self-managing privacy, etc.), externalities (eg with regard to the provision of data but also to harms caused by data breaches

47 See e.g. Crémer and others (n. 2) 19–38, Marc Bourreau and Alexandre de Streel, 'Digital Conglomerates and EU Competition Policy' (Center on Regulation in Europe 2019) 5–24 <https://cerre.eu/news/digital-conglomerates-and-eu-competition-policy/> accessed 31 August 2020. In our example of access to data in connected cars it is, e.g., a necessary precondition for proving the above-described competition problem with regard to the secondary markets that system competition between car manufacturers does not work sufficiently. This requires a deeper economic analysis, e.g. of lock-in effects and the behaviour of car buyers. See Kerber (n. 26) 387.

48 For an analysis of market failure with regard to data see, in particular, also Bertin Martens 'Data access, consumer interests and social welfare: An economic perspective of data', in this volume. Without the existence of market failures we could rely on the contractual relationships regarding data between firms or firms and consumers.

and cybersecurity risks), too low levels of interoperability and standardisation (due to biased incentives of firms with regard to interoperability and standardisation), and innovation problems (due to not enough use and sharing of data for data-driven innovation, data analytics, AI, and training of algorithms). Also of particular importance is that several market failures can exist simultaneously, which can make it necessary to analyse the interplay between these different market failures as well. This might lead to the need of a combination of different regulatory solutions in a specific data governance system. Our examples PSD2 and data in connected cars have shown both the existence of more than one market failure and the need for such a coordinated policy approach for solving competition, interoperability, and safety and security problems.

Since the economic market failure theory is based upon the concept of economic welfare, it cannot take into account additional policy objectives such as the protection of privacy as a fundamental value or distributional objectives, eg, the protection of vulnerable consumers or fairness considerations about the extent to which consumers can get a fair share of the value of their personal (or consumer) data. These and other additional policy objectives, which might be seen as relevant from a normative perspective, e.g. in specific contexts and sectors, have to be included in the analysis of the effects of different data governance solutions.[49] Based upon such analyses conclusions can be drawn about policy recommendations on the proper set of rights and rules with regard to data and additional necessary regulations for solving the problems.

III. Some instruments for data governance systems

This chapter has the task of providing a brief overview about specific instruments that can be used as basic elements of such data governance systems. All of these instruments can be found in the current discussion, and many of them can be used in combination with both general (horizontal) data access and (sector-)specific data governance solutions. Some of these instruments refer directly to the data themselves, and help to shape the definition and assignment of the 'bundle of rights' on data, whereas others

49 Such a broad economic policy approach that allows for including values and policy objectives beyond economic welfare can also lead to the need to deal with trade off-problems between economic welfare and these other values and policy objectives. One important example is the trade-off between privacy as a fundamental value and the effects of access to more personal data on economic welfare.

focus more on the additional regulatory solutions that might be necessary for making the data governance solutions effective.

1. Consumer data rights and data portability

A very interesting new instrument for defining and assigning rights on data is the already mentioned 'consumer data rights'.[50] Since data about consumers can be very valuable and consumers produce an increasing amount of data by using smart connected devices (IoT), the question has emerged whether consumers should have more control over these data and also participate more in the value of these data. This is also part of the discussion about data in connected cars, which according to a wide-spread opinion should be 'owned' by the car owners, and not by the car manufacturers (or by the manufacturers of smart devices in other IoT applications).[51] The consumer data rights approach asks what rights consumers should have with regard to the access, control and portability of their consumer data. An important objective of the consumer data rights approach is the empowerment of consumers to better control their consumer data, decide themselves whom they give access to these data, as well as participate in their value. Since most consumer data are also personal data as defined by privacy laws, such a control might also be exerted through the rights on personal data that are granted by privacy laws (such as, in particular, the GDPR in the EU). However, the advantage of the consumer data rights approach is that consumer data rights can be applied much more flexibly and in a more targeted form than rights in personal data provided for by privacy laws. For example, the scope of consumer data that are subject to these consumer data rights can be broader than what is defined as personal data in privacy laws, and might also encompass, e.g., observed or derived data.[52] It might therefore be an advantage to define and assign consumer data rights outside of privacy laws, because this allows for a much more sophis-

50 See as an overview OECD (n. 14).

51 That the owner of a smart device should be also the 'owner' of the data that are produced with this device was also the basic idea of the 'data producer right' proposed in Commission Communication COM(2017) 9 final (n. 1) 13.

52 See for this discussion, e.g., OECD (n. 14) 7–21; see also the concept of data mobility in Furman and others (n. 25) 65–71 that goes beyond the data portability right of the GDPR.

ticated and targeted fine-tuning of these rights to the specific problems of different sectors and ecosystems.[53]

This is also directly linked to the current critical discussion about the ineffectiveness of the data portability right of the Article 20 GDPR.[54] Here the solution of the PSD2, which defines data portability rights of the consumers outside of the GDPR and complements it with additional regulations, is superior to the application of Article 20 GDPR, which would have not been sufficient for opening bank accounts. In the same way the data portability right is also not capable of solving the data access problems in the data of the connected car example.[55] In its data strategy the European Commission wants to 'explore enhancing the data portability for individuals under Article 20 of the GDPR giving them more control over who can access and use machine-generated data'.[56] It might be important for this reform discussion to focus also on more data portability solutions outside of the GDPR, and the consumer data rights approach might be helpful in that respect.

2. *Data trustee solutions*

Data trustee solutions are another group of very promising data governance instruments that can be used in manifold ways for solving a wide range of problems in different contexts. Here only two main types of data trustee solutions will be distinguished. One discussion refers to the problems of consumers to manage their personal data and protect their privacy, the insight that they are often overwhelmed with the task of reading, understanding and managing long, intransparent privacy policies, and that therefore the currently applied 'notice and consent' solutions suffer from

53 Therefore the approach of the Australian government of introducing a general data consumer right, which is then implemented in sector-specific variants, reflects this flexibility. See Louisa Specht-Riemenschneider, 'Data access rights – A comparative perspective', in this volume.

54 See, e.g., Graef and others (n. 13), Krämer, Senellart and de Streel (n. 13).

55 See Daniel Gill and Wolfgang Kerber, 'Data Portability Rights: Limits, Opportunities, and the Need for Going Beyond the Portability of Personal Data' (2020), 2(2) CPI Antitrust Chronicle, 54.

56 Commission Communication COM(2020) 66 final (n. 1) 21; see also European Union, 'Consumer Data Rights and Competition – Note by the European Union' (2020) OECD Doc. DAF/COMP/WD(2020)40. See for other proposals Krämer, Senellart and de Streel (n. 14) 75–84.

serious market failure problems.[57] One possible solution might be new intermediaries acting in the interests of these consumers, and helping them to protect their privacy, especially through managing the rights in their personal data, ie whether and to whom they give consent for processing them and for what purposes according to their specific privacy preferences. These new intermediaries can also play an important role for making more data available for the data economy for innovation, research, and improving public policies, e.g. through donating or selling (or, more precisely, licensing) them. Such data trustee solutions as personal information management systems (PIMS) have been discussed for a long time,[58] but so far the attempts to develop profitable market solutions, e.g. by specialised start-ups, have not been successful. Recently a new discussion has started about the need to develop new data trustee solutions as one promising instrument for solving the privacy management problems of consumers, and what such solutions might look like.[59] Since experience has shown that pure market solutions do not seem to be successful, the future discussion might have to focus on the question of how the development of such intermediaries with a data trustee role for consumers can be supported by addi-

57 Despite a contentious discussion about the 'privacy paradox' there is an increasing consensus that here a serious market failure exists due to information asymmetries and behavioural problems of consumers that is aggravated by misleading strategies of data-collecting firms. See Patricia. A. Norberg, Daniel R. Horne and David A. Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors' (2007) 41(1) Journal of Consumer Affairs 100; Daniel J. Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880; Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Privacy and Human Behavior in the Age of Information' (2015) 347(6221) Science 509; Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2019) University of New South Wales Research Series 19–53 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432769> accessed 31 August 2020.

58 Article 29 Data Protection Working Party (n. 13).

59 See Kommission Wettbewerbsrecht 4.0 (n. 13) 43, Datenethikkommission (n. 3) 133–136; Commission Communication COM(2020) 66 final (n. 1) 10; for a broad recent overview see Aline Blankertz, 'Designing Data Trusts. Why We Need to Test Consumer Data Trusts Now' (Stiftung Neue Verantwortung e.V. 2020) <www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf> accessed 31 August 2020; Aline Blankertz and others 'Datentreuhandmodelle' (2020) 66–73 <www.stiftung-nv.de/sites/default/files/20200428-datentreuhandmodelle.pdf> accessed 31 August 2020; and Krämer, Sennellart and de Streel (n. 14).

tional regulatory solutions.[60] For our discussion here is important that such data trustee solutions for helping to protect the privacy and manage the rights in personal data of consumers can be seen as an important building-block of the general data governance system (with regard to all personal data of the consumers). However, also specific data trustee solutions for a limited set of personal data, eg mobility data or energy consumption data, might be possible, which then can be integrated into a comprehensive specific data governance system.

The second type of data trustee solutions focusses mainly on the manifold problems that can emerge regarding data in B2B contexts. Data trustees can fulfil the function of providing a trustworthy neutral entity for managing problems between firms that can reduce transaction costs (through increasing trust), ensure compliance with data protection rules or IP protection, help to solve competition problems by making data available in a non-discriminatory way, or help to open data by providing access to large data sets according to certain principles.[61] One of the proposed policy solutions in the data in connected car example, the 'shared server', can be interpreted as a data trustee solution. It implies that all car data would be transmitted to an external server (outside of the car), which however is governed by a neutral entity that makes the data available to the stakeholders of the ecosystem of connected cars in a non-discriminatory way under certain general principles. In the same way other data sets (or data streams) which should be made available to (a certain group of) firms for enabling competition and innovation can also be administered by an entity which fulfils the role as a data trustee. In that respect data trustees might also play a role in the EU strategy of developing common European data spaces, in which for different sectors large data sets of, e.g. anonymised, data are made available for AI applications or the training of algorithms.[62] Data trustees might also play a role in all these cases where firms have to grant access to data due to competition law provisions (e.g.,

60 This need for additional regulatory support can refer to solving conflicts of interest between consumers and these data trustees but might also refer to the question whether there should be an obligation of data-collecting firms to negotiate with these intermediaries. One of the problems of such data trustee intermediaries is their lack of bargaining power vis-à-vis powerful data-collecting firms and platforms. See Blankertz (n. 59) 18–22, who despite preferring market solutions also discusses regulatory solutions which, e.g., can also mandate the use of such data trustees.

61 See for these and other objectives, e.g., Blankertz and others (n. 59) 2.

62 See Commission Communication COM(2020) 66 final (n. 1) 11–23.

the EFD according to Article 102 TFEU), but also where serious concerns emerge that a direct transmission of data to data claimants might lead to the danger of losing any control over the use of these data. In such cases neutral and trustworthy data trustees might offer solutions enabling other firms to access and use these data (for the purposes intended with this data access), but ensuring that the monitoring of this use by the data trustee helps to prevent any misuse (and therefore protects the interests of the data holders).[63] These different ways data trustee solutions can be used in B2B contexts show that they can play manifold roles both in the general data governance system and in specific data governance systems.

3. *Interoperability and standardisation*

Solving problems of interoperability and standardisation is an important issue with regard to many data governance problems, as we also have seen in our examples of PSD2 and connected cars. However, it is important to distinguish three different problems: (1) One problem concerns the well-known issue of 'common data formats' as a precondition for data access, data-sharing and data portability, which can be supplemented by the often additional need for data standardisation (clear definition of data sets and their quality). (2) Beyond these conditions for the data sets themselves, it is additionally necessary to have clear standardised technical interfaces for the access to or transmission of data. This might require regulation on a technological level, e.g. by requiring standardised APIs. It might be more challenging if independent service providers also need real-time access to data for providing their services. (3) It is necessary to distinguish an additional separate problem of providing technical interfaces that allow independent service providers to interoperate with a system, as, e.g., when initiating payments in bank accounts or remotely uploading software updates on the IT system of the connected car (for providing remote maintenance services). Here the problem is not primarily about transmission of (or access to) data but about performing complementary services, which can necessitate much higher requirements for interoperability and therefore the technical interface.[64] Depending on the technological and economic con-

63 This is also linked to the discussion about data sandboxes, in which innovators can experiment with consumer data, e.g. under the supervision of an agency, see Furman and others (n. 25) 71.

64 The last two distinctions correspond to the concepts 'data interoperability' and 'full protocol interoperability' in Crémer and others (n. 2) 83–86.

ditions of the data governance problems, only one, two, or all three of these problems have to be solved so as to enable competition and innovation in these data governance solutions. All three problems can be very relevant in both general and specific data governance systems. What is important from an economic perspective is that, on the one hand, there might be serious market failure problems due to biased incentives that lead to not enough interoperability and standardisation; on the other hand, however, it also has to be taken into account that more interoperability and standardisation does not always have positive effects on competition and innovation. This has to be considered with regard to general standardisation policy as well as with regard to interoperability and technological standardisation in specific data governance systems.[65]

4. Minimum standards for safety, security, and privacy

Another key issue for data governance systems in the digital economy with its new and huge problems of cybersecurity is the problem of how to deal with safety and security risks. These risks can encompass identity theft, data breaches, misuse of data, fraud, and the damaging of entire technical systems with potentially huge risks regarding accidents and loss of lives. So far the policy solutions for dealing with these risks, e.g. through liability and/or minimum standards for safety and security (especially regarding the many new IoT applications), are still very insufficient.[66] As far as data governance systems entail solutions for data access/portability and/or interoperability, it is necessary to also develop solutions for the safety and security problems that might be linked to these data governance solutions. Therefore (high) minimum standards for safety and security (as well as 'security by design' and sophisticated liability solutions) might be necessary. This refers also to the already discussed issue of more interoperability and stan-

65 For the economics of interoperability and standardisation (with the ensuing market failure problems) see John Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books 2012); Farrell and Simcoe (n. 36), and as a brief overview Kerber and Schweitzer (n. 36).

66 See, e.g., for cybersecurity risks of smart home applications Sara E. Kettner and Christian Thorun, 'Big Data im Bereich Heim und Freizeit' (2018) <www.abida.de/sites/default/files/Gutachten_HeimUndFreizeit.pdf> accessed 31 August 2020. See generally for the economics of cybersecurity Tyler Moore, 'The Economics of Cybersecurity: Principles and Policy Options' (2010) 3(3–4) International Journal of Critical Infrastructure Protection 103.

dardisation, which might also have to itself include safety and security standards. But other solutions, such as the licensing or certification of independent service providers, might also be very helpful policy solutions that can be part of integrated specific data governance systems (as we have seen in the PSD2 and the current motor vehicle type approval regulation).

The policy measures for dealing with cybersecurity risks can also contribute to the protection of privacy for making the storage and processing of personal data more secure. However, as we have seen in our discussion of intermediaries that might help consumers to manage their data (PIMS), privacy risks also exist with respect to the collection of data due to intransparency (and misleading practices of data-collecting firms) regarding the extent of the collection and use of personal data and behavioural problems of consumers. Since so far the market solution of privacy-protecting data trustee solutions does not exist (and might also work only to a limited extent in future), it might be necessary to use more regulatory solutions for implementing additional minimum standards for the privacy policies of data-collecting firms. This might be done by either using more the current provisions in the GDPR (e.g. on consent or privacy-by-design/default) and in consumer law, or by introducing new additional regulations, e.g. also in certain sectors as part of specific data governance systems. These specific regulatory solutions can refer to the requirements for consent (opt-in, opt-out, etc.) or minimum rules for transparency regarding the collection and use of personal data, but might also encompass substantive minimum standards on limits for the collection and use of personal data.[67] Another important field of quasi-regulatory solutions that can constitute important elements of general and specific data governance systems is that of labelling and certification of firms regarding their compliance with the GDPR, or, additionally, on their level of data protection.[68] It can also be particularly

67 See, e.g., European Data Protection Supervisor 'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy, Preliminary Opinion 2014' (EDPS 2014) 24–25 <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf> accessed 31 August 2020.

68 For a critical analysis of the provisions on data protection certification in the GDPR see Eric Lachaud, 'Why the Certification Process Defined in the General Data Protection Regulation Cannot Be Successful' (2016) 32 Computer Law & Security Review 814; Irene Kamara and others, 'Data Protection Certification Mechanisms: Study on Articles 42 and 43 of the Regulation (EU) 2016/679 – Final Report' (2019) <https://ec.europa.eu/info/sites/info/files/data_protection_certification_mechanisms_study_final.pdf> accessed 31 August 2020. Also, industry-specific codes of conduct on compliance with the GDPR are possible.

important for the data economy to have clear rules on the standards for anonymisation of personal data, because anonymised data sets are not subject to EU data protection law. Sector-specific standards for anonymisation of personal data that take into account the sector-specific risks of reidentification can therefore be a very valuable element of specific data governance systems that can help to increase legal certainty in the context of both the privacy of consumers and the data economy.[69]

E. Perspectives

The most important results of this article are the following:

(1) Both horizontal and sectoral solutions for access to (or sharing of) data have advantages and problems, and it can be expected that depending on the specific technological and economic conditions in different parts of the economy either general data access rules or sector-specific data access rules are more suitable for solving the problems.

(2) Focussing only on the problem of whether one firm should get access to data that another firm holds will often be too narrow an approach for solving problems of insufficient access to data for competition and innovation. It is often necessary to use a broader analytical approach that, on the one hand, analyses a broader set of data governance solutions, including for example the use of data trustees or technological solutions that change the initial allocation of de facto control of data, and, on the other hand, might also allow for a broader set of remedies, including additional regulatory solutions like requiring interoperability and standardisation or minimum standards for safety, security, and privacy, for ensuring the effectiveness of the data governance solutions. This is the broader approach of analysing entire data governance systems, especially with respect to the effects of existing market failures on welfare and other policy objectives.

(3) In the last part we have briefly analysed a number of instruments that can be used as building-blocks in such data governance systems, both for the general and for specific data governance systems. Particularly interesting new instruments might be based upon the new approach of consumer data rights (especially with regard to data portability), the

69 See for the problem of data anonymisation and the difficulties in defining the precise requirements for a data set that qualifies as anonymous according to the GDPR Crémer and others (n. 2) 85–87.

manifold types of data trustee solutions (both for privacy management and in B2B contexts), interoperability and standardisation policies, as well as necessary regulatory policies with respect to safety and (cyber)security, as well as privacy. Whereas in the general data governance system these different policies will have to be applied independently of each other, they can be directly aligned through an integrated regulatory regime in specific data governance systems that try to address all market failure problems in a coordinated way.

In this article we have not addressed one key question about data governance solutions, namely the institutional question who should decide on data governance solutions. Although the ultimate decision-maker is always the legislature, the question emerges who should decide whether a specific data governance system should be implemented and how the specific rights and rules in both general and specific data governance systems should be designed. Should the courts be the de facto rule-makers and/or enforcement agencies (like competition authorities) who can publish guidelines and pursue enforcement priorities? Or should we have regulatory authorities with broader regulatory powers that also have the authority to decide on specific data governance systems with their specific rights and rules with respect to data? The 'digital market unit' proposal in the Furman Report suggests such an institutional solution, because it would confer on this new regulatory authority broad powers, (1) for designating which platform firms have a 'strategic market status' and should be subject to ex ante regulation, eg concerning 'codes of conduct', but (2) also for making decisions about enabling more data mobility, open standards and interoperability as well as opening data. Therefore the Furman proposal is primarily also an institutional proposal that a new regulatory authority should have the powers to introduce, change and shape important parts of data governance systems with regard to data access, data sharing and interoperability.[70] It is not possible here to discuss the merits and problems of such an institutional solution. However, the Furman proposal emphasises

70 What is important is that the regulatory powers with regard to data governance solutions in the Furman proposal are not limited to data access or interoperability problems caused by platform firms with a 'strategic market status.' They can also be applied to other firms, see Furman and others (n. 25) 70, 73. See also the proposal of a 'digital authority' with similar powers in the Stigler Report: Committee for the Study of Digital Platforms, 'Market Structure and Antitrust Subcommittee – Report' (1 July 2019), 9, 83–87 <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure-report.pdf?la=en&hash=E08C7C9AA7367F2D612DE24F814074BA43CAED8C> accessed 31 August 2020.

the need for also finding proper institutional solutions for how the data governance solutions (including their necessary complementary regulations) can evolve and be adapted in a timely way to the ever-changing economic and technological conditions of the digital economy.[71] This is particularly important, because there is an urgent need for a more forward-looking perspective on data governance policy, eg to identify early new data governance problems that might threaten competition, innovation, and privacy, and to develop solutions that prevent the problems. This refers, among other things, to the emergence of new bottleneck and gatekeeper positions based upon the exclusive control of data. So far data governance policies tend only to react to already existing gatekeeper positions instead of more actively trying to prevent them.[72]

71 Another institutional proposal has been made by the German Kommission Wettbewerbsrecht 4.0 (n. 13) 6. It recommends the introduction of a new EU Framework Directive that would give the European Commission the powers to enact sector-specific regulations granting users the right to make their internet accounts accessible to third-party providers.

72 See also for an emphasis on a forward-looking approach Datenethikkommission (n. 3) 84.