A legal framework for access to data – A competition policy perspective

Heike Schweitzer and Robert Welker[*]

A. Data access in the digital economy

The transition of the economy to the new conditions of the digital economy is underway. The new role of data is at its core. There is a broad consensus that data have become a key input for and element of competing in vast areas of the economy and for the development of the European economy at large: Data are at the heart of new and increasingly sophisticated forecasting techniques – often based on machine learning or other artificial intelligence (AI) technologies – that can lead to better decisions in a multitude of economic and societal areas.[1] A key driver of these technologies is the ever-increasing ability to automatically analyse vast amounts of unstructured data that often are generated as a 'by-product' of the use of machines or services or of other business activities without incurring much additional cost.[2] The new, data-driven prediction machinery[3] can help to realise efficiency gains and improve productivity throughout the value chain. Furthermore, it allows for the development of new and more personalised products and services in many areas of the economy, both in business-to-consumers (B2C) and in business-to-business dealings (B2B). By combining usage data generated in the course of the use of different products and services on a multitude of markets concerning different areas of life, digital conglomerates can create increasingly detailed, complex and comprehensive user profiles, rendering the personalisation of products and

* We are grateful to Frederik Gutmann for his valuable research support. Also, we thank Axel Metzger for a greatly stimulating discussion.

1 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, 2–3.

2 Heike Schweitzer and Martin Peitz, 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?' (2018) Neue Juristische Wochenschrift 275, 275.

3 See Ajay K. Agrawal, Avi Goldfarb and Joshua Gans, *Prediction Machines: The Simple Economics of Artificial Intelligence* (Ingram Publisher Services 2018).

the targeting of marketing activities ever more sophisticated.[4] With the rise of the Internet of Things ('IoT'), business strategies are about to change fundamentally, shifting from the provision of products to the provision of data- and software-based internet services.[5] Data and the ability to draw value from it will drive innovation and growth for decades to come.

Against this background, a debate started some time ago on how to adapt the legal framework to the new reality of the data economy. This endeavour has many facets, ranging from data protection[6] to cybersecurity[7]. One of the main problems identified is a lack of data available for innovative re-use, including for innovating in the area of AI.[8] The European Commission has announced a 'comprehensive approach' that aims to increase the availability, use of and demand for data and data-enabled products and services.[9] Apart from the opening up of public sector information for business use (government-to-business (G2B) data sharing),[10] data sharing between companies (B2B data sharing) shall be promoted.[11] The goal is to create an environment where businesses 'have easy access to an almost infinite amount of high-quality industrial data'[12] as well as the necessary tools, infrastructures and competences for handling data. The new data innovators shall be able to build on the scale of the Single Market, thereby boosting growth and European competitiveness.[13]

To allow companies to take off at sufficient scale within the European Single Market, the Commission has set out to overcome the persisting

4 Heike Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welker, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen* (Nomos 2018) 26.

5 Alexander Ziegler, *Der Aufstieg des Internet der Dinge: Wie sich Industrieunternehmen zu Tech-Unternehmen entwickeln* (Campus Verlag 2020).

6 With the GDPR as the main legal pillar.

7 See Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No. 526/2013 (Cybersecurity Act) [2019] OJ L151/15.

8 European Commission, 'A European strategy for data' (n. 1) 6.

9 Ibid 1.

10 Ibid 7, 13. See also Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L172/56.

11 European Commission, 'A European strategy for data' (n. 1) 7.

12 Ibid. 4–5.

13 Ibid. 3, 5.

market fragmentation and establish a 'European data space' where data can flow within the EU and across sectors.[14]

The principles and rules that can help overcome the persistence of 'data monopolies' and 'data silos' in the market are currently under debate.[15] Markets for specific types of data exist.[16] But in many contexts, relevant data resources will be under the exclusive control of a firm that is not willing to grant access. This is particularly true for the rich data troves controlled by the big online platforms. But it is also true when it comes to the data produced within the evolving IoT.

From a bird's-eye view, the possible approaches to data access can be placed on a scale between two fundamentally different philosophies. On the one end of this scale, data remain under private control. Access is granted, if at all, on the basis of freely negotiated contracts (private control framework). On the other end of this scale, data are regarded as a common good, and access is guaranteed based on broad legal access obligations (open access framework).

In its recent communication on a European data strategy, the Commission has argued for a differentiated, but generally cautious approach. In the G2B sphere, the Commission generally supports an open access approach.[17] In the business-to-government (B2G) sphere, it means to encourage voluntary data sharing, but to complement it with an EU regulatory framework – potentially including data access obligations – to govern the

14 Communication of the Commission, 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. See also Regulation (EU) Nr. 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59; and Directive (EU) 2019/1024 (n. 10).

15 See, for example, Bertin Martens, Alexandre de Streel, Inge Graef and others, 'Business-to-Business Data Sharing: An Economic and Legal Analysis' (2020) JRC Working Papers on Digital Economy 2020–05 <https://ssrn.com/abstract=3658100> accessed 15 September 2020.

16 Cf. Christian Santesteban and Shayne Longpre, 'How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science' (2020) 65 The Antitrust Bulletin 459, 481–483.

17 See Section B., below, for a description of the fundamental policy approaches. The Commission expressly bases its strategy on the non-rivalrous nature of data and the possibility to replicate it without cost, concluding that there is a need for a broad data access regime: European Commission, 'A European strategy for data' (n. 1) 4.

public sector's re-use of privately-held data for public policy goals.[18] In the B2B sphere, on the other hand, *voluntary* data sharing is to remain the rule. Public interventions should generally be of a facilitative, enabling nature: Since a lack of data interoperability has been identified as one of the hurdles for an increased flow of data in the B2B and G2B context,[19] a 'rolling plan for ICT standardisation'[20] is to encourage the application of shared compatible formats and protocols for gathering and processing data from different sources, such that data become interoperable across sectors and vertically within the supply chain.[21] The development of clear and trustworthy data governance mechanisms is to be supported;[22] and the legal framework for data markets is to be clarified in a future 'Data Act'.[23] Competition law will address power imbalances.[24] Particularly entrenched types of power may justify ex-ante regulation in specific sectors.

This paper broadly supports this approach but strives to further explore and develop its conceptual basis. To this end, the second part of the paper sets out general policy approaches in determining the 'right' amount of data openness and argues for a market-driven system of data allocation (B.). The third part will explore the market failures that call for corrective measures to complement a 'freedom of contract' regime. It is structured around three scenarios: access to individual-level usage data by data co-generators, access to bundled individual-level data or aggregated data by third parties in an aftermarket setting and data access based on general innovation policy aims. Existing sectoral regimes[25] will be scanned for their underlying policy rationale (C.). The paper concludes with some general recommendations (D.).

---

18 European Commission, 'A European strategy for data' (n. 1) 7: The Commission refers to the recommendations of its Expert Group, consisting of 'the creation of national structures for B2G data sharing, the development of appropriate incentives to create a data-sharing culture, and the suggestion to explore an EU regulatory framework to govern the public sector's re-use for the public interest of privately-held data'.

19 Ibid 8.

20 European Commission, 'Rolling Plan for ICT Standardisation 2020' (2020) <https://ec.europa.eu/docsroom/documents/41541> accessed 15 September 2020.

21 European Commission, 'A European strategy for data' (n. 1) 8, 12.

22 Ibid. 5.

23 Ibid. 13.

24 Ibid. 8.

25 See Sections C.I.3. and C.II.3. below. Not all relevant sectoral regimes can be covered, however. In particular, access rules in the transport and mobility sector are outside of the scope of this paper.

Before diving into the debate on data access, one note of caution is in order: data come in many forms and varieties. They can be personal or non-personal,[26] they can be individual-level, bundled-individual-level or aggregated data,[27] structured or unstructured;[28] annotated[29] or non-annotated; content data or metadata; they can refer to environmental information, or to usage patterns; and they can be primary data or processed data at different stages of the value chain.[30] Whenever access to data is agreed on or mandated, the specificities of the relevant type of dataset must be taken into account. The focus of this paper is on usage data – whether individual-level, bundled-individual-level or aggregated, and whether personal or non-personal.

B. *Private data control versus open access – fundamental choices for the data economy*

The public debate on data access frequently circles around two poles: Should data be regarded as just another type of privately controlled resource? The legal recognition of private rights of control and exclusion might – but need not necessarily – result in the creation of a new type of

26 For the definition of personal data see Art. 4(1) GDPR.

27 Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era', Special Advisers' Report (2019) 25–26 <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 15 September 2020.

28 Structured data are highly organised and formatted in a way that makes them easily searchable.

29 Annotated data are made usable for the training of machine-learning algorithms through labelling.

30 For a brief description of the data value chain see Schweitzer and Peitz (n. 2) 275–76; Inge Graef, Thomas Tombas and Alexandre de Streel, 'Limits and Enablers of Data Sharing. An Analytical Framework for EU Competition, Data Protection and Consumer Law' (2019) TILEC Discussion Paper No. DP 2019–024, 4–5 <https://ssrn.com/abstract=3494212> accessed 15 September 2020: First, raw personal and non-personal data are collected directly or bought on a secondary data market; second, data are structured and turned into information; third, those structured data are analysed by algorithms and information is turned into knowledge, such as a prediction; and finally the analysis of the structured data leads to an action such as improving products or offerings.

intellectual property right in data.[31] Or should data be a new type of commons in the evolving data economy? Along this line, some propose that data should be considered a new type of infrastructure for the data economy, which could argue for an open access approach. The OECD's 2015 report on data-driven innovation is representative: 'The economic properties of data suggest that data may be considered as an infrastructure or infrastructural resource […] from a functional perspective'[32] – they are non-rivalrous in consumption, meaning they can be used infinite times without depreciation;[33] the demand for data is, as with physical infrastructure, driven 'primarily by downstream productive activities that require the resource as an input';[34] and they are a general-purpose input, i.e. they can be used and reused to develop different products and services.[35] Given these features, a general open access regime could seemingly maximise efficiency and innovation.

I. Private control vs. open access: The basic trade-off

The discussion partly repeats debates that are well-known from the area of intellectual property law: there is a trade-off between a free flow of information and exclusive control.[36] Where data are an important input for many promising economic activities, an open access regime would lower barriers to entry and promote competition and innovation in adjacent and novel markets. On the other hand, exclusive control over data facilitates

31 For this debate see: Alain Schmid, Kirsten Johanna Schmidt and Herbert Zech, 'Rechte an Daten – zum Stand der Diskussion' (2018) 11 sic! Zeitschrift für Immaterialgüter-, Informations- und Wettbewerbsrecht 627; Josef Drexl, 'Designing Competitive Markets for Industrial Data Between Propertisation and Access' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 257; Wolfgang Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (2016) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 639 – all with further references.

32 OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* (OECD 2015) 179.

33 Ibid 179–80.

34 Ibid 179–81.

35 Ibid 179, 181–83.

36 Axel Metzger, 'Innovation in der Open Source Community – Herausforderungen für Theorie und Praxis des Immaterialgüterrechts' in Martin Eifert and Wolfgang Hoffmann-Riem (eds), *Geistiges Eigentum und Innovation* (Duncker & Humboldt 2008) 188.

their monetisation and thereby incentivises the collection and processing of the data in the first place. While a consistently proprietary approach would bear the risk of an inefficient under-use of data, a radical open access approach could lead to a 'tragedy of the commons',[37] resulting in under-investment in the creation of data.[38]

II. The benefits of open access to public sector data

In some areas – in particular with regard to large portions of public sector information – negative incentive effects appear to be less relevant, and an open access approach is broadly pursued.[39]

Ensuring better access to public sector data is widely believed to be a key factor to enhance the possibilities to innovate in the emerging European data economy – also because it will open new ways to combine public sector data with private sector data.[40] However, public sector data and the Open Data Directive will not be dealt with in this paper.

III. Private control as the basic paradigm for private sector data

When it comes to private sector data, the debate on data access is not limited to solving the puzzle of how to optimise innovation. The data – in particular usage data – that have become so valuable in the data economy carry a type of information that differs from the information that intellectual property rights have protected so far. For good reason, a relevant part of this information is protected by other legal regimes, e.g. the protection of

37 Jane Yakowitz, 'Tragedy of the Data Commons' (2011) 25 Harvard Journal of Law and Technology 1.

38 Heike Schweitzer and Martin Peitz, 'Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?' (2017) ZEW Discussion Paper No. 17–043, 60 <http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf> accessed 15 September 2020.

39 Directive (EU) 2019/1024 (n. 10); see also Heiko Richter, 'Open Science and Public Sector Information – Reconsidering the exemption for educational and research establishments under the Directive on re-use of public sector information' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 51.

40 Recital 16 Directive (EU) 2019/1024 (n. 10).

trade secrets[41] when it comes to confidential business information or the GDPR when it comes to personal data. Furthermore, an open exchange of competitively sensitive information is prohibited by competition law.[42]

1. The status quo: Private control through de-facto possession

The current legal regime for private sector data allocation is built on a private control approach. This is irrespective of the fact that data as such are so far not protected by intellectual property rights: private data control is based on a de-facto possession of data and on the ability of data controllers to regulate other parties' access by technological measures.[43] If in the interest of the data controller, data access is granted selectively based on contractual agreements.

In principle, a regime of private control can lead to the emergence of more or less open and transparent data markets, where companies sell access to their data if the price exceeds the potential gains of an exclusive 'in-house' monetisation. A system of decentral coordination can ensue that ideally leads to an efficient allocation of data. Where usage data is generated in a co-operative bilateral relationship – e.g. between a service provider and the user of a service, or a producer of industrial machinery and its user – effective competition in the services or machinery market can lead to a coexistence of competing models, where the service or machine user could either get access to 'his' or 'her' data in exchange for a higher product price or forgo data access in exchange for a lower price.[44]

41 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1; implemented in Germany through the *Gesetz zum Schutz von Geschäftsgeheimnissen* (GeschGehG).

42 See European Commission, Guidelines on the applicability of Art. 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements [2011] OJ C11/1, paras 55 et seq.

43 Schweitzer and Peitz, 'Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf?' (n. 38) 66.

44 See Section C.I.2. below.

2. *Limits of the private control approach*

In reality, while markets for some types of data indeed exist and have existed for some time,[45] markets for usage data in respect of services and machinery are rare and, where they exist, typically non-transparent.

This may be due to various reasons: For one, private data controllers have to consider the legal constraints to data sharing (following from the GDPR, trade secrets protection, competition law etc.) as described above. As of now, firms have to grapple with a high degree of legal uncertainty, which raises the cost of sharing data.[46] Secondly, the uncertainty extends to the value of data. Methods for assessing the value of data are currently much debated.[47] The value will crucially depend on how the data are used, and it may depend on who has access to the relevant data and which other datasets the data are combined with. Given the dynamic development of the digital economy, it is easily conceivable that a private data controller or a potential data user will under- or overvalue the relevant data,[48] or that the private data controller will fear undervaluing them or missing out on important competitive opportunities, and will therefore be reluctant to cede control. Thirdly, where the exclusive use of data allows the data controller to monopolise adjacent data-driven markets, the expected monopoly rent may exceed the expected value from marketing that data. This may be true with regard to markets like online advertising markets, which currently offer the most obvious opportunities to monetise data on a large scale. It may also be true where exclusive access to usage data leads to a lock-in of users – both with regard to the primary product or service, which becomes more valuable as the product or service is personalised, and with regard to complementary markets.

---

45 Cf. Santesteban and Longpre (n. 16) 481–83.

46 Cf. German Federal Ministry of Economic Affairs and Energy, 'A new competition framework for the digital economy – Report by the Commission "Competition Law 4.0"' (2019) 56–59 <https://www.bmwi.de/Redaktion/EN/Publikationen/Wirtschaft/a-new-competition-framework-for-the-digital-economy.html> accessed 15 September 2020.

47 Jordi Casanova Tormo, 'Estimating Reasonable Prices for Access to Digital Platforms' Data: What Are the Challenges?' (2020) 4 European Competition and Regulatory Law Review 172; David Nguyen and Marta Paczos, 'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective' (2020) OECD Digital Economy Papers No. 297, 31–38 <https://www.oecd-ilibrary.org/docserver/6345995e-en.pdf> accessed 15 September 2020.

48 On market failures due to imperfect information in data markets see Martens and others (n. 15) 27.

Fourthly, in some settings, monopolisation tendencies, and sometimes strategies, may extend to the primary services or product market. This is true, in particular, for some online platform markets characterised by strong network effects and efficiencies of scale and scope.[49] The concentration of the primary market will then be accompanied by private control over particularly large and valuable usage data, which in turn further increases the barriers to entering the primary market and thus entrenches the incumbent's pre-existing position of market power.

3. The gaps of a private control approach do not justify its renunciation

The first question to be answered is whether these shortcomings of data markets or outright market failures argue against a private data control approach and in favour of an open access approach in a principled way. Broad and general compulsory data access obligations would, however, not make the problems disappear. The legal constraints on data sharing – whether resulting from the GDPR, from competition law or trade secret protection – would remain under an open access approach and would need to be framed as legal exceptions. Their specification case by case would leave much room for legal disputes and require a sophisticated dispute resolution mechanism or regulatory oversight. The same would be true with regard to pricing. Difficult issues would need to be resolved with regard to access conditions and whether access would be limited to primary data or extend to other stages of the data value chain. The regulatory regime required would need to be agile enough to address the many different settings in which data access requests can come up and develop solutions that are sufficiently sensitive to the potentially negative incentive effects that data access obligations would imply. It would need to do so in a setting where the evolution of the data economy – and data markets in particular – are still in flux. It would miss out on the many fine-grained insights that a decentralised search process for context-sensitive data access regimes will arguably produce.

In line with the European Commission's 'agile' approach, there is therefore a strong case for letting markets evolve based on a regime of private control. Firms are currently in the process of experimenting with the po-

49 Stigler Committee on Digital Platforms, 'Final Report' (2019) 8 <https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf> accessed 15 September 2020.

tential uses of their data and exploring their value. Novel strategies of and governance regimes for data sharing and data pooling are likely to evolve in different areas of the IoT. While its outcome is unpredictable, this process can be expected to produce a greater variety of more differentiated solutions than any attempt of a centralised rights allocation could.

4. *Addressing the market failures in a private control context: The role of competition law*

Given the societal and economic importance of data access, a private data control regime must, however, be embedded in a legal framework that stands ready to address significant market failures in a forceful and consistent manner. Information asymmetries and monopoly power must be tackled, and positive as well as negative externalities of data access or data exclusivity must be considered. The legal framework to take up these tasks ranges from, *inter alia*, contract law, including, where applicable, consumer protection law, to competition law and, as a measure of last resort, sector-specific regulation. Importantly, the legislator should consider the introduction of access and usage rights to usage data for all co-generators of such data so as to improve the preconditions for competition.[50]

Within the overall legal framework, competition law functions as a background regime and as a benchmark for developing best principles for data access. To live up to this role, competition law must clarify when data sharing and data pooling will constitute an infringement of Article 101 TFEU.[51] As to Article 102 TFEU, the aftermarket doctrine needs to be clarified with regard to data-driven lock-in,[52] so as to provide guidance on when a customer lock-in can lead to data access requirements. Moreover, the concept of data-related abuses must be further explored – where recent case law, such as the German *Facebook* case,[53] has demonstrated that it is not always and not necessarily a refusal to grant access that constitutes an

50 See Section C.I.5.b) below.

51 See Crémer, Montjoye and Schweitzer (n. 27) 94–98, 109. The Commission has already announced an update of the Guidelines on horizontal cooperation agreements with respect to data-sharing and pooling arrangements: see European Commission, 'A European strategy for data' (n. 1) 14. A public consultation process has already begun; see <https://ec.europa.eu/competition/consultations/2019_hbers/index_en.html> accessed 15 September 2020.

52 See Crémer, Montjoye and Schweitzer (n. 27) 87–91, 101–06, 125.

53 See German Federal Supreme Court (BGH), Case KVR 69/19 – *Facebook*.

abuse, but an abuse may also lie in the combination of different sets of usage data by a dominant firm. Finally, Article 102 TFEU should guide the discussion on when data access is an adequate remedy for a data-related abuse.

Where data access is indeed the appropriate remedy, competition law as such will frequently need to give way to sector-specific legislation to ensure that data access is granted on fair, reasonable and non-discriminatory (FRAND) conditions. While the relevant case law on rights to a licence to a standard-essential patent (SEP)[54] may appear to provide a rough role model for the process by which contractual negotiations on data access should take place, data access regimes may turn out to be even more complex and diverse in practice: the proposed use cases for data may differ widely and affect the conditions under which data access should be granted as well as the access pricing. Different datasets may be needed; data access may be requested at different levels of the value chain, and in each case, an inquiry into the indispensability of the access may be required. The requisite timing of data access may differ: in some settings, the provision of historical data will suffice, in other settings, near-time or real-time access may prove necessary for firms to compete effectively. Similar issues may arise regarding the necessary degree of interoperability,[55] the formats in which data access must be granted and the design of the access interfaces. Conflicts will likely be frequent and – in a competition law framework – highly case-specific. Fast-track procedures for resolving such disputes will be needed if data access is to be effective.

In some areas, these challenges will be overcome by setting up a highly standardised data access regime. In particular, access to individual-level usage data with the consent of the relevant individual can be – and has been – organised at reasonable cost.[56] In other areas, the complexity of the challenge may caution against the attempt to set up a compulsory data access regime, and may guide a search for structural solutions that incentivise the

54 See in particular Case C-170/13 *Huawei* ECLI:EU:C:2015:477.

55 For the different forms of interoperability see Crémer, Montjoye and Schweitzer (n. 27) 83 et seq. A lack of data interoperability has been identified as one of the hurdles for an increased flow of data B2B and G2B – see European Commission, 'A European strategy for data' (n. 1) 8. On data interoperability see also: Michal S. Gal and Daniel L. Rubinfeld, 'Data Standardization' (2019) 94 New Your University Law Rev. 737.

56 See Section C.I.3. below.

entity mandated with organising access to establish a well-functioning market.[57]

C. Access to usage data in three different baseline settings – Variations in the legal framework and in the role of competition policy

Where the private data control approach is the starting point, the need for market interventions in general and for a competition law intervention in particular turns into a discussion about the existence of a pertinent market failure.

This paper strives to discuss this question against the background of three recurring data access scenarios:[58] Firstly, access to individual level data by a co-generator of usage data in a bilateral scenario (1); secondly, requests for access to bundled individual-level data or aggregated datasets by a third party vis-à-vis a service or product provider who controls broad usage datasets, with the third party claiming that access to the relevant data is needed to effectively compete in complementary markets (2); thirdly, requests by firms to access the large usage data troves of Big Tech companies to compete and innovate in the field of AI (3).

I. Scenario 1: Access to individual level data by data co-generators

1. The data access scenario

A significant part of the debate on data allocation relates to settings where data are co-generated by two or more parties and the exclusive control over this data is in the hand of one party. Examples of co-generated data include the usage data of an IoT device, e.g. a connected car or a piece of connected industrial machinery, or of an online service, including a social network or a search engine.

57 See, in particular, C.II.5. and C.III.4. below.

58 Also see Crémer, Montjoye and Schweitzer (n. 27) 75 et seq.; Heike Schweitzer, 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung' (2019) Gewerblicher Rechtsschutz und Urheberrecht 569, 572–73.

2. Possible market failures

Where usage data are transmitted automatically to the producer of the machine or the service provider and processed to improve or personalise the service, to predict needs for maintenance of a machine, to learn about typical usage patterns or to develop complementary services, the user may find it difficult to switch the product or service after some time: a competing producer or service provider would need to compensate for the loss in personalisation through an additional advantage in quality or price, making the market entry of newcomers significantly more difficult.

Moreover, the user may be locked into data-driven complementary services of the product or service provider, whereby third parties may find it difficult to compete effectively without (possibly real-time) access to the usage data. Examples of complementary services that depend on access to usage data include predictive diagnostic services for machinery, complementary services for drivers of connected cars that rely on in-car data or smartphone apps that need access to the GPS data stored in the device.

With effective competition on the primary product or services market and optimally informed users, competitive pressure would force producers and service providers to offer customer-friendly contract terms and technical data access solutions.[59] Generally, data access and data portability would be valued by customers because it would allow them to avoid a data-induced lock-in, both on the primary market and on complementary markets. On the other hand, a 'closed' model may allow a producer or service provider to engage in long-term planning and investment, and to pass on part of this advantage to the customer in the form of a better price or quality.[60] Consequently, a multitude of competing systems with varying

59 The debate over welfare effects of competition on aftermarkets versus competition between systems with different levels of openness became very extensive following the US Supreme Court's *Kodak* decision: see, *inter alia*, Carl Shapiro, 'Aftermarkets and Consumer Welfare: Making Sense of Kodak' (1995) 63 The Antitrust Bulletin 483. For a discussion of the consequences of the Kodak case in Europe see Robert Bell, Jacob Kramer and Brian Cave, 'Competition/Antitrust Challenges in Technology Aftermarkets' (2015) <http://eu-competitionlaw.com/competitionantitrust-challenges-in-technology-aftermarkets/> accessed 15 September 2020.

60 The possibility to monopolise aftermarkets also enables the producer of the primary product or the provider of the primary service to cross-subsidise the product or service price through the monopoly rents achieved on the secondary market. This pricing model became famous with Gillette razors (free razor, expensive blades; see Joseph Farrell and Paul Klemperer, 'Coordination and Lock-In: Com-

degrees of data openness could coexist, catering to the varying preferences of different groups of customers.[61] This mechanism is well known from markets for operating systems, for example: a more proprietary operating system in which apps have to pass a quality review process in order to gain access to the device's data may have advantages with respect to a more uniform user experience, better app quality standards and better cyber security – while, on the other hand, making apps potentially more expensive and reducing the range of apps to choose from. Based on these trade-offs, different approaches to openness coexist, with Microsoft Windows arguably being more open than Apple's MacOS and Google Android arguably being more open than Apple's iOS.

The competitive mechanism can fail, however. Frequently, the source of such a market failure will be information asymmetries: in B2C markets, consumers will often not be able to calculate the trade-off correctly at the time when they choose the product or service. This is true in particular where long-lasting products or services are chosen. Similarly, it may be very difficult for consumers to evaluate their demand for certain aftermarket services *ex ante* – especially considering that new and innovative aftermarket services may not even have been available at the time of purchase. Consequently, customers will frequently pay less attention to data accessibility than would be appropriate and will not accurately discount the loss of choice on aftermarkets and/or the loss of the possibility to switch. An

petition with Switching Costs and Network Effects' in Mark Armstrong and Robert Porter (eds), *Handbook of Industrial Organization*, Vol. 3 (North Holland 2007) 2037; Randal C. Picker, 'The Razors-and-Blades Myth(s)' (2011) 78 University of Chicago Law Rev. 225) but is, for example, also well-known with printers (cheap devices, expensive branded ink; see Lother Determann and Bruce Perens, 'Open Cars' (2017) 23 Berkeley Technology Law Journal 915, 928–29) or machines for the then-patented Nespresso capsules (cheap coffee machines, expensive coffee capsules). This kind of business model may be individually favourable for consumers with a low level of usage. The efficiency effects should be ambiguous, as such a business model leads to an increase in output on the primary market vs. a decrease in output on the secondary market. For an in-depth analysis of business models and lock-in strategies see Carl Shapiro and Hal Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Review Press 1998) 103–72.

61 A buyer of industrial machinery who plans to seldom make use of it could, for instance, prefer a cheaper purchase price in return for being locked in with the expensive predictive maintenance services of the OEM. A buyer who plans to make frequent use of the same equipment might prefer a higher purchase price in return for free data access that allows her to choose from a broader option of aftermarket services.

adverse selection may follow, and products and services that restrict access to usage data may prevail.

In B2B settings, market actors can be expected to be more sensitive to lock-in-situations. But in dynamic, fast-changing markets, even they may be unable to predict the future potential uses of the data sets and therefore undervalue choice and the option to switch.

In other settings, competition will fail to produce a customer-friendly market outcome because one product or service provider is dominant or because all product or service providers have opted for the same model of denying data access – either due to (tacit) collusion or because a closed model is the best option for each of them individually. Bilateral bargaining power may provide another explanation.

3. Legislative reactions

Most of the data access legislation that currently exists can, in one way or another, be interpreted as a reaction to data access situations of the scenario 1 type. Essentially all of this legislation refers to perceived market failures of the kinds described above. While sectoral regulation (Electricity Directive, PSD2 Directive; see c) below) is, as of yet, usually equally applicable in B2C and B2B settings, a 'horizontal' right to access usage data is only implemented with respect to personal data within the meaning of Article 4(1) GDPR, not with respect to industrial usage data.[62]

a) Article 20 GDPR: A mandatory portability right regarding personal data

The data access rules with the broadest scope of application are enshrined in the GDPR. Wherever personal data within the meaning of Article 4(1) GDPR are at issue, Article 15 GDPR provides any data subject concerned with a non-waivable, general right to access his or her data. Of greater economic importance is the right to data portability as set out in Article 20

62 While usage data in B2B settings will also frequently entail personal data within the meaning of Art. 4(1) GDPR (location data of a person driving a car will, if it can be linked to the driver, be personal data irrespective of whether the journey was undertaken for private or business reasons), a large part of a business's usage data will typically not qualify as personal data (for example: data on its energy use; data on the wear and tear of its equipment etc.).

GDPR.[63] While the data remains under the control of the service provider, each data subject has a right to receive the personal data concerning him or her 'in a structured, commonly used and machine-readable format' and to transmit those data – or have them transmitted – to another controller without hindrance from the current controller.

As has frequently been stated, Article 20 GDPR has been introduced primarily with a view to counteracting data-related lock-in effects:[64] It is intended to facilitate the switching of services whose provision can be significantly informed by historic personal data. Article 20 GDPR thereby enhances each individual's freedom of choice and economic scope of action. From a competition law angle, it thereby lowers barriers to entry to the market for primary services and increases the contestability of the market position of any given service provider.

However, Article 20 GDPR does not qualify as a tailored remedy to the market failure described above: In this perspective, it is both too narrow and overbroad. It is too narrow because it is generally considered that, while Article 20 GDPR grants a right to access and transmit historical data, it does not include a right to full and real-time porting or to data interoperability.[65] With this limitation, Article 20 GDPR is designed 'to enable switching of service providers, rather than enabling data reuse in digital ecosystems'.[66] The lock-in into the primary product or service may be addressed – provided there is sufficient competition in the market for primary products or services. The lock-in into a potentially broad range of aftermarkets is not tackled effectively by Article 20 GDPR where real- or near-time access would be needed. To target the latter lock-in, a right to ensure data interoperability with third party service providers would arguably be required. Under Article 20 GDPR, the decision whether to open data-driven aftermarkets for new entrants or not remains at the discretion of the service provider, however.

---

63 See also Art. 16(2) of the Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 – with reference to the GDPR.

64 European Parliament, 'Resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union' (2011/2025(INI)) [2013] OJ C33E/101, para. 16.

65 Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 Computer Law & Security Review 193, 200–201; Schweitzer (n. 58) 574.

66 European Commission, 'A European strategy for data' (n. 1) 10.

At the same time, if Article 20 GDPR were meant to remedy the market failure problem sketched above, it would be overbroad: The right to data portability is granted to data subjects irrespective of the existence of a relevant information asymmetry, and it cannot be waived even with full information. Furthermore, Article 20 GDPR is blind to whether the service provider possesses any relevant degree of market power or even bilateral bargaining power. Due to the compulsory, non-waivable nature of the right to data portability, a new entrant into the market would be unable to buy off the right to data portability in exchange for a better price and incentives to invest in a long-term relationship. Under Article 20 GDPR, any new entrant must fear that consumers will switch to the incumbent once the latter enters the market and lures the consumer with the greater size of its network, a higher degree of interoperability or, based on the broad scope of his or her data troves, a greater degree of personalisation.

In its current shape, Article 20 GDPR should therefore not be understood as a reaction to a market failure. Rather, it strives to protect the data subject's 'informational autonomy' and continued control over his or her personal data. The fact that the right to data portability is designed as a non-waivable right is proof of the weight that the EU legislator has given to consumers' continued freedom of choice irrespective of the benefits that might result, in the absence of information asymmetries and power, from increased incentives of a service provider to invest in the bilateral relationship on a long-term basis. Paradoxically, the protection of the data subject's informational autonomy thereby comes with a significant limitation of his or her freedom of contract.

b) Electricity Directive: Access to smart meter data

A sector-specific data access regime that clearly reacts to a market failure – namely stable (quasi-)monopolistic positions in the markets for electricity-related infrastructure – has been established in the context of energy consumption and energy input data collected through connected 'smart' meters.[67] Smart meter data can be useful for consumers in various ways.

67 There are also data access obligations with respect to metering data for natural gas; see Art. 3(6)(b) and Annex I(1)(h) of Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC [2009] OJ L211/94. These access obligations, while following a similar logic as the Electricity Directive (facilitating switching between energy suppliers), have not yet been

While there is no specific risk of data-induced lock-in (there is, as of now, no 'personalisation' in electricity markets that would require consumption data to be ported to a new energy supplier), effortless access to energy consumption data facilitates hassle-free switching of energy suppliers, who can offer prices based on precise, historic consumption data. Access to smart meter data is necessary for 'smart' tariffs that change prices depending on the time of consumption, grid load or wholesale prices. Data access is also a requirement for using 'consumer energy management systems'[68] that are integrated, for example, into smart home devices. Energy-intensive processes, like charging an electric car, could be switched on automatically when the price is low, saving electricity costs and simultaneously stabilising the grid. While switching between energy suppliers requires only one-time access to consumption data, smart home devices will usually require real-time or near real-time data access.

Electricity meters have typically been operated and controlled by distribution grid operators, which possess a natural monopoly. Even where markets for meter operation have been liberalised, the market position of former monopolists has often remained extraordinarily strong. In Germany, for instance, energy consumers have had the right to choose an independent electricity meter operator since 2006.[69] The legal relations between independent electricity meter operators, energy suppliers and grid operators are governed by private contracts (subject, however, to regulation). Nonetheless, grid operators still have a market share of over 90 % in the energy metering market.[70] In such a setting, data access cannot be left to privately negotiated contracts and competition.

---

updated with respect to connected 'smart' meters. They will not be dealt with in depth in this paper.

68 An overview of technical details can be found at Rita Pereira and others, 'Consumer energy management system with integration of smart meters' (2015) 1 Energy Reports 22.

69 Now Sec. 5 Federal Law on Metering Point Operation (*Messstellenbetriebsgesetz*), formerly Sec. 21b Energy Industry Act (*Energiewirtschaftsgesetz*). For more (economic) details about the German liberalisation of metering point operations see Stephan Schmitt and Matthias Wissner, 'Die Liberalisierung des Messwesens – Verhindert das Abrechnungsentgelt freien Wettbewerb?' (2015) 39 Zeitschrift für Energiewirtschaft 171.

70 Bundesnetzagentur and Bundeskartellamt, 'Monitoringbericht 2019' (2019) 322–23 <https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2019/Monitoringbericht_Energie2019.pdf?__blob=publicationFile&v=6> accessed 15 September 2020.

Instead, the Electricity Directive 2019/944[71] obliges member states to implement the following mandatory access rights into their national law: customers are to be granted access to data on the electricity they feed into the grid and on their electricity consumption 'through a standardised communication interface or through remote access, or to a third party acting on their behalf, in an easily understandable format allowing them to compare offers on a like-for-like basis' (Article 20(e)). This provision is specifically tailored to facilitate switching between electricity suppliers. Data access for complementary services (smart home devices or other consumer energy management systems) can be obtained through Article 23(2) of Directive 2019/944.[72] While Article 23 does not clearly state that data access is to be provided via real-time or near real-time APIs, Article 19(1) shows that the policy goal of such data access is to promote 'smart metering systems that are interoperable, in particular with consumer energy management systems'. Interoperability requirements can be implemented by the European Commission subject to Article 24(2) of Directive 2019/944. Hence, energy consumers can provide a data access point to the providers of complementary services.[73]

By requiring data interoperability with regard to individual-level data relevant for complementary devices and services, the EU has therefore implemented a mandatory data 'portability' approach that reaches beyond Article 20 GDPR.

c) The Payment Service Directive II (PSD2): Access to accounts and account data

Another sector-specific data access regime that goes beyond Article 20 GDPR but is less clearly tailored to a market failure than the Electricity Di-

71 Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU [2019] OJ L158/125 (Electricity Directive).

72 According to this provision, 'the parties responsible for data management shall provide access to the data of the final customer to any eligible party […]. Eligible parties shall have the requested data at their disposal in a non-discriminatory manner and simultaneously. Access to data shall be easy and the relevant procedures for obtaining access to data shall be made publicly available'.

73 As they are eligible parties within the meaning of Art. 23(2).

rective's access regime is contained in the PSD2.[74] It obliges member states to implement certain access rights to payment accounts ('access to account', or 'XS2A',[75] in FinTech jargon): account servicing payment service providers, such as banks, are required to grant real-time access to the account and transaction data of an account holder via APIs to 'account information service providers', or AISPs (Article 67 PSD2), and to allow the initiation of payments via APIs through 'payment initiation service providers', or PISPs (Article 66 PSD2), on a non-discriminatory basis. Also, the account must be accessible online. Such access must, however, be explicitly requested by the account holder. Furthermore, the Directive establishes certain data protection, data minimisation and cybersecurity obligations.[76] The European Banking Authority (EBA) is called upon to establish 'common and open standards of communication to be implemented by all account servicing payment service providers that allow for the provision of online payment services'.[77]

The PSD2 Directive thus goes significantly beyond the 'simple' data portability right as laid down by Article 20 GDPR: not only does it grant real-time data access via standardised APIs (regarding AISPs), it even allows for service interoperability (regarding PISPs). It thereby enables account holders to make use of innovative aftermarkets services that rely on access to their payment accounts and facilitates competition on these aftermarkets. With these provisions, the EU reacts to the difficulties 'for payment service providers to launch innovative, safe and easy-to-use digital payment services and to provide consumers and retailers with effective, convenient and secure payment methods in the Union.'[78] PISPs are regarded as a 'bridge between the website of the merchant and the online bank-

74 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35 (PSD2 Directive). For the debate see, *inter alia*, Oscar Borgogno and Giuseppe Colangelo, 'Consumer Inertia and Competition-sensitive Data Governance: The Case of Open Banking' (2020) Journal of European Consumer and Market Law 143.

75 See Open Banking Europe, 'Third Party Provider User Management for PSD2 Access to Account (XS2A)' (2017) <https://www.openbankingeurope.eu/media/1176/preta-obe-mg-001-002-psd2-xs2a-tpp-user-management-guide.pdf> accessed 15 September 2020.

76 See Arts 66, 67 PSD2 for details.

77 PSD2, Recital 93.

78 PSD2, Recital 4.

ing platform of the payer's' bank[79] and as a 'low-cost solution' for both merchants and consumers to provide for fast shipments in e-commerce and to reduce transaction costs.[80] AISPs provide for attractive solutions to give the account user 'an overall view of its financial situation immediately at any given moment'.[81] Overall, the PSD2 Directive thereby becomes an important building block of a European internal market in digital times.

In a perfectly competitive market setting with fully informed consumers and a lack of transaction (especially: switching) costs, banks would be incentivised to grant access to a broad range of complementary services on their own initiative to attract potential account holders. Banking markets are, however, frequently characterised by exactly the kinds of informational market failures described above: when deciding where to open a banking account, many potential customers will not pay sufficient attention to which complementary services are compatible with each bank. In particular, consumers would, if at all, focus on compatibility with certain incumbents or important newcomers (like ApplePay). What is more, consumer inertia results in a widespread lack of willingness to switch banks.[82] As a result, banks may be strategically incentivised to vertically integrate and monopolise access for their own complementary payment solutions or restrict access to selected partners.

The PSD2 Directive's data access and interoperability rules are generally well-suited to address these information-based market failures and facilitate competition and innovation in complementary services. Implemented sector-wide they may, however, come with an important downside: they eliminate a possibility for service differentiation – and therefore, a possible competitive advantage – for newcomers in the core market (here: the banking market). In several markets, before the entry into force of the PSD2 Directive, new start-up banks had been emerging whose unique selling point was a bundle of innovative complementary services and/or broad account access for third-party service providers.[83] Certain banking 'dinosaurs' had

79 PSD2, Recital 27.
80 PSD2, Recital 29.
81 PSD2, Recital 28.
82 Borgogno and Colangelo (n. 74); CMA, 'Retail banking market investigation final report' (9 August 2016) paras 64–73 <https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf> accessed 15 September 2020.
83 See, for example, the German upstart bank N26.

already begun to grant access through APIs on a voluntary basis.[84] With the PSD2 Directive, innovative banks may have lost an important competitive 'edge'.

d) Contractual rights to port non-personal data B2C

Finally, the European legislator has recently recognised a contractual right of consumers to port non-personal digital content provided or created by him or her in the course of a contract for the supply of digital content or digital services in case of termination of the contract.[85]

4. Competition law

In the absence of sector-specific data access legislation, data access may be mandated under general competition law.

In B2C relationships, the refusal to allow access to a customer's individual-level usage data upon his or her request in real time may constitute an exploitative abuse. If a third-party undertaking were to request access with the consent of the customer concerned, but were denied such access, this could be part of an exclusionary strategy, undertaken with a view to further entrenching the position of dominance in the primary market or leveraging this position to neighbouring markets. For Article 102 TFEU to apply, a position of dominance of the data controller in the primary market, as well as its abuse, would need to be proven case by case.

In Germany, coinciding principles follow from Section 19 of the German Act Against Restraints of Competition (GWB). Section 20(1) GWB goes further: According to this provision, the prohibition of exclusionary abuses of market power applies not only to dominant firms, but also where a small or medium-sized undertaking depends on another undertaking for the supply or demand of specific products or services such that sufficient and reasonable possibilities to switch to other undertakings do not exist ('relative market power'). In other words: bilateral power suffices to

84 See, for example, Deutsche Bank, 'Unlocking opportunities in the API economy' (2018) <https://cib.db.com/docs_new/Whitepaper_Unlocking_opportunities_in_the_API_economy_Aug_2018.pdf> accessed 15 September 2020.

85 See Art. 16(4) of Directive (EU) 2019/770 (n. 63). Generally for a discussion of contractual data access rights see Axel Metzger, 'Access to and Porting of Data under Contract Law', in this volume.

turn an undertaking into an addressee of the prohibition to unreasonably impair competition or to discriminate between firms competing on a neighbouring market without objective justification. Relative market power can also stem from specific, non-recoverable investments in the business relationship with another undertaking ('company-specific dependency'),[86] even where such dependency is the result of a voluntary contractual relationship.[87] In principle, the refusal to grant access to co-generated usage data can therefore constitute an abuse of relative market power.

Currently, a reform act is pending[88] that proposes to amend Section 20 GWB with a new paragraph (1a) that would recognise that bilateral dependency can arise from the fact alone that an undertaking is dependent on access to data controlled by another undertaking. A dependency on the product or service from which the data derives would not be required.[89] Where complementary products or services are based on the usage data generated in the course of the use of a primary product or service, substitutes for that data will be lacking by definition, such that Section 20 GWB may be broadly applicable to data lock-in scenarios. It would, however, not apply where a firm can gain access to individual-level usage data by turning to the user itself for transmission. If a usage right of data co-generators were to be recognised, this would typically be the case. The main scope of application of Section 20(1a) GWB would then be scenario 2 (see II.4. below).

Finally, the aforementioned reform act would also introduce a new Section 19a GWB, addressed to undertakings on multi-sided markets and network markets that are 'of paramount significance for competition across markets'. Section 19a(2) No. 4 GWB would empower the *Bundeskartellamt* (the German Federal Cartel Office) to prohibit any action that would 'make the interoperability of products or services or the portability of data

86 German Federal Supreme Court (BGH) of 23 February 1988, Case KZR 20/86 – *Opel Blitz;* German Federal Supreme Court (BGH) of 21 February 1995, Case KZR 33/93 – *Kfz-Vertragshändler; both regarding brand-specific investments of authorised car dealers and repairers.*

87 Jörg Nothdurft, in Hermann-Josef Bunte (ed.), *Langen/Bunte, Kartellrecht: Kommentar*, Vol. I (13th edn Luchterhand 2018) § 20 GWB para. 38.

88 Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB Digitalisierungsgesetz) (2020) <https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&v=6> accessed 15 September 2020.

89 Schweitzer and others (n. 4) 192–93.

more difficult and thereby impede competition'. To the extent necessary to make competition on data-driven markets work, it would allow the *Bundeskartellamt* to impose data access requirements on firms of paramount significance for competition across markets *ex ante*.

5. Policy options

a) Access to individual-level data in B2C settings

Stepping back, significant action has already been taken to update the current legal framework as it applies to scenario 1 cases. A broad consensus is emerging that a general transformation of the right to data portability under Article 20 GDPR into a right to data interoperability would be counterproductive: depending on the specific market conditions, it could work in favour of already data-rich firms that, based on a dominant position of a platform of strategic importance,[90] have the potential to expand that position into neighbouring markets. Also, ensuring data interoperability can be a high burden on small and medium-sized firms. A general data interoperability obligation would therefore tend to increase barriers to entry and hamper innovation. Consequently, in B2C markets, a continuation with a more cautious sector-specific legislation appears to be the right approach. Such legislation should be informed by the insights on the complex trade-offs that come with the opening up of narrowly defined primary markets in aftermarket settings.

The implications are currently much debated, in particular with a view to access to in-car data in an emerging 'connected cars' setting. Connected cars collect a multitude of data about the state of the vehicle and its use, as well as environmental data.[91] To a significant degree, these data will be personal data within the meaning of Article 4(1) GDPR. For access to and the processing of in-car data, whether individual level, bundled individual

90 Special conduct requirements for this set of firms (to be precise: undertakings on multi-sided markets and network markets that are 'of paramount significance for competition across markets') are considered by the German legislature in its amendment of Sec. 19a GWB (see above). Sec. 19a(2) No. 3 GWB would allow the Bundeskartellamt to prohibit the bundling of data across markets where it has the potential to impede competition.

91 Cf. Damien Geradin, 'Access to In-Vehicle Data by Third-Party Service Providers: Is there a Market Failure and, if so, How Should it be Addressed?' (2020) 2 <https://ssrn.com/abstract=3545817> accessed 15 September 2020.

level or aggregate, three technological approaches are currently debated: car manufacturers prefer the so-called 'extended vehicle' concept, where all data is transferred to, processed and stored on proprietary servers of the car manufacturers themselves.[92] In defence of this approach, car manufacturers assert cybersecurity and consequently road safety advantages. These advantages are, however, contested by other market actors[93] and independent studies.[94] Alternatives to the 'extended vehicle' approach are, firstly, 'neutral' servers to which access for third parties is granted on the basis of transparent, non-discriminatory terms and, secondly, 'onboard' processing of all in-car data on an open application platform that allows for the installation of third-party applications.[95] Third-party applications that depend on (possibly real-time) access to individual-level or bundled individual-level in-car data may be, for example, predictive maintenance services, complementary on-the-road services like upgraded navigation or 'smart parking' services or insurance tariffs that are usage-dependent or vary with driving style. The 'extended vehicle' would put car manufacturers in a gatekeeper position that would enable them to monopolise aftermarkets and complementary services. The alternatives would not do so, or (in the case of a 'neutral' gatekeeper) to a much lesser extent.[96]

On competitive markets, car manufacturers would be incentivised to choose the technical solution with the level of openness that best suits consumers' preferences. Different solutions and business models with their respective advantages and disadvantages might co-exist (see 2. above). There is, however, reason to assume a significant degree of market failure on this

92 European Automobile Manufacturers Association, 'ACEA Strategy Paper on Connectivity' (2016) 10 et seq. <https://www.acea.be/uploads/publications/ACEA_Strategy_Paper_on_Connectivity.pdf> accessed 15 September 2020.

93 See, *inter alia*, 'Manifesto for fair digitalisation opportunities' <https://www.figiefa.eu/wp-content/uploads/Manifesto-For-equal-Digitalisation-chances.pdf> accessed 15 September 2020, signed by several industry associations.

94 See, for example, M. McCarthy and others, 'Access to In-vehicle Data and Resources – Final Report', TLR Report for the European Commission (2017) 75 et seq. <https://ec.europa.eu/transport/sites/transport/files/2017-05-access-to-in-vehicle-data-and-resources.pdf> accessed 15 September 2020. The authors conclude that, while security is more costly to implement within the alternative technological approaches, it is well possible – and that the demands of safety and security need to be balanced with the goal to achieve fair and undistorted competition (ibid. 8–9).

95 McCarthy and others (n. 94) 32–49.

96 Cf. Wolfgang Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 310, 325.

'systems market'. The problem is not one of market dominance on the car market: markets for consumer cars can be characterised as a reasonably concentrated oligopoly, with a number of established firms and a healthy set of 'challenger' firms. However, information asymmetries are likely to be pervasive: cars are durable investment goods. Customers are therefore locked in to their purchase decision for a significant amount of time.[97] It is difficult for consumers to make a reliable estimate about the full life cycle costs of owning a car of a specific brand – a specific brand's performance on aftermarkets may therefore not be adequately disciplined by the risk of diminishing sales on the primary product market. In such a setting, car manufacturers may be incentivised to monopolise aftermarkets or grant access only to selected partners in exchange for a fee (thereby reaping monopoly rents). While one may argue, on the other hand, that second-hand markets provide a sufficiently convenient way out of the lock-in, the protracted legislative battle to open up markets for automotive repair and maintenance services and spare parts appears to provide proof that a relevant market failure persists nonetheless.[98] Also, the range of possible aftermarkets in the emerging mobility sector is arguably huge, as is the innovative potential that an opening of the relevant data markets can unleash.

To address this case of market failure – and to resolve the persisting legal uncertainty concerning in-car data – there appears to be a case for enacting mandatory real-time data access and portability (or rather: interoperability) rights that enable consumers to choose between independent providers of aftermarkets and complementary services. This would need to be accompanied by a system of certification[99] or technological safeguards

97 Ibid. 317.

98 The type approval regulation of 2007 established non-discriminatory rights to access vehicle repair and maintenance information and on-board maintenance data (vehicle on-board diagnostic information, 'OBD data') – see 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. For further details see Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data' (n. 96) 319; Wolfgang Kerber and Jonas Frank, 'Data Governance Regimes in the Digital Economy: The Example of Connected Cars' (2017) 33 et seq. <https://ssrn.com/abstract=3064794> accessed 15 September 2020. Also see scenario 2 at Sub-section II. below.

99 Cf. Geradin (n. 91) 1–2, with an analogy to the review processes by Apple and Google for their app stores.

(separating basic automotive functions from additional functions, like entertainment) to address relevant security risks.

b) Access to individual-level (industrial) data in B2B settings

The European legislator has been significantly less determined to address data access settings of the scenario 1 type in B2B relationships. In some fields – especially in the area of banking and electricity – access rights of businesses have been recognised alongside those of consumers. Also, depending on the facts of the case, usage data may qualify as personal data even in a business setting,[100] such that Article 20 GDPR applies. But unlike for personal data, there is no generally applicable data access and portability right for industrial data. Consequently, in bilateral settings between a product producer or service provider and its business customer, it is currently mostly left to the parties of the relevant contractual relationship to negotiate a consensual data access solution. Following this logic, the Fairness and Transparency Regulation (EU) 2019/1150,[101] which applies to online intermediation services, such as sales platforms, and online search engines (Article 1(2) Transparency Regulation), refrains from establishing rights of business users of the platform to data access. Instead, it sets out a mere requirement of transparency regarding the 'technical and contractual access, or absence thereof, of business users to any personal data or other data'.[102]

In its communication 'Towards a common European data space', the EU Commission has set out general principles on data sharing B2B, in particular the principles of transparency, shared value creation, respect for each other's commercial interests, protection of undistorted competition and the minimisation of data lock-in.[103] Furthermore, it has sketched different models of data sharing.[104] In its recent communication on a Euro-

100 Case C-398/15 *Manni* ECLI:EU:C:2017:197, para. 37.

101 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.

102 Art. 9 Regulation (EU) 2019/1150.

103 See European Commission, 'Towards a common European data space' (n. 14) 10 and European Commission Staff Working Document, 'Guidance on sharing private sector data in the European data economy' SWD(2018) 125 final, 3.

104 (i) An open data approach; (ii) data monetisation on a data marketplace; (iii) data exchange in a closed platform. See European Commission SWD, 'Guidance on sharing private data' (n. 103) 5.

pean strategy for data, the Commission has announced its intention to get key players from the manufacturing sector to agree on conditions under which they would be willing to share their data generated by smart connected products.[105] A 'Code of Conduct on Agricultural Data Sharing by Contractual Agreement',[106] which was developed in 2018 by a number of agricultural organisations, provides a first impression of what such an agreement could look like. In order to foster trust in agricultural data sharing it emphasises, *inter alia*, the right of the data originator to control the access to and the use of data. Comparatively far-reaching data-sharing obligations exist or are being explored in the transport sector.[107]

Obviously, competition law continues to apply and complements the contractual regime. Data access obligations may, in particular, follow from Article 102 TFEU (see 4. above).

However, a debate has ensued on whether contractual solutions, backed up by competition law, suffice.[108] The data controller and the product or service user will be in a contractual relationship most of the time, but not necessarily so; the product or service user's legitimate interest in accessing and porting the usage data will be the same, regardless of the existence of such a 'direct' contractual relationship. In such a situation, the creation of a – waivable – data access, usage and portability right *in rem* of all those who have actively participated in the generation of the usage data would help. It would recognise that under the conditions of the emerging data economy, where the usage of a product or service constantly generates data, such usage over longer periods of time simultaneously constitutes a valuable investment and contribution of the user to the value of the product or service that should be legally recognised. Also, the legislative acknowledgment of such an access and usage right would provide a baseline for negotiations on the best allocation of rights in a given case.

At the same time, a waivable access, usage and portability right would not protect business users against information asymmetries, market power

105 See European Commission, 'A European strategy for data' (n. 1) 26.

106 EU Code of conduct on agricultural data sharing by contractual agreement, <https://www.copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf> accessed 15 September 2020.

107 European Commission, 'A European strategy for data' (n. 1) 28.

108 Drexl (n. 31) 287–291; 'Datenethikkommission der Datenethikkommission [Opinion of the Data Ethics Commission] (October 2019) 147. See also the draft ALI-ELI Principles for a Data Economy which suggest the legislative creation of a right to access or to port co-generated data. For details and discussion see Axel Metzger, 'Access to and porting of data under contract law', in this volume.

and bilateral power imbalances that may lead to the market failures described above. In such cases, additional instruments of intervention continue to be needed. For such interventions, a waivable access, usage and portability right would, however, serve as a legal reference point. In those national legal orders that – like German civil law – provide for a control of standard contract law terms in B2B relationships, the recognition of an access, usage and portability right of data co-generators would set a legislative benchmark for what is typically considered to be fair.[109] Where a waiver is requested by a dominant firm, the deviation from the legislative benchmark may indicate an abuse.[110]

Interestingly, the recognition of a waivable access, usage and portability right of data co-generators would also provide a novel reference point for the application of Article 101 TFEU. An agreement between the data controller and the product or service user to waive or limit the data access, usage and portability right would arguably qualify as an agreement restrictive of competition, as it would tend to hamper the entry of competitors both into the primary market for the product or service by which the data is generated and into complementary markets. At least where such waivers were agreed on systematically, they could have an anti-competitive object or effect. Without the definition of a legal data usage right, data controllers would not need to implement contract clauses with respect to data access at all; instead, they would simply retain their 'de-facto data possession' and refuse to deal with the data – a unilateral behaviour that is only restricted by competition law where dominance is present (Article 102 TFEU). Article 101 TFEU would allow agreements on the waiver of data access rights to be addressed significantly below the threshold of dominance.

Obviously, such waivers can also come with important efficiency gains and pro-competitive justifications. In particular, they would incentivise long-term investments by the product or service provider. On this basis, a new data-related Block Exemption Regulation could and arguably should be drafted: Contractual waivers of data access rights should be generally exempted under Article 101(3) TFEU where the market share of the beneficiary of the waiver on the primary product or services market remains relatively small (15–20 %). The exemption should, however, be withdrawn

109 According to the German Civil Code, standard contract law terms agreed B2B would only be subjected to a fairness control where they derogate or supplement legal provisions (Sec. 307(3) German Civil Code).

110 Either an exploitative abuse (imposing unfair trading conditions) or an exclusionary abuse of dominance (impeding switching and/or monopolising aftermarkets).

where contractual waivers are requested by a large portion of the market, such that the demand side would essentially be left without a meaningful choice. Furthermore, contractual waivers should not be exempted where they – together with other provisions in the contract – lead to a durable lock-in, both with respect to the primary product and to aftermarket services.

6. *Conclusions on scenario 1*

Overall, sound legal principles appear to be evolving with regard to data access scenario 1. Generally, the private control paradigm applies. In B2C relationships, this paradigm is somewhat disrupted by the non-waivability of the right to data portability under Article 20 GDPR. Nonetheless, the right of consumers to port 'their' data, as recognised by Article 20 GDPR, has the potential to change the competitive landscape. More practical ways to administer one's data, to manage consent and, where desired, to make personal data available for reuse, including with the help of personal data cooperatives or neutral data intermediaries, remain to be explored.[111]

Also, further sector-specific legislation is to be expected – for example in the context of connected cars – that will endow consumers with rights to real- or near-time access to data. The PSD2 Directive and the Electricity Directive provide role models in this regard. Similar regulation appears to be appropriate where power asymmetries or information asymmetries are systemically prevalent on a data-driven market and tend to produce strong and durable consumer lock-in into aftermarkets that is not overcome either by competition on the primary (systems) market or by well-functioning second-hand markets.

For non-personal data, the creation of a data access and usage right *in rem* – although waivable – would make an important difference. With such data access rights, exclusive control of usage data would no longer be the benchmark. Multiple data access points would arise, with the potential to stimulate innovation and competition. Failures in markets for data as well as in markets for data-driven products and services could then be addressed on a flexible basis, combining the strengths of contract law and competition law.

111 See, for example, European Commission, 'A European strategy for data' (n. 1) 10, referring to the MyData movement and similar initiatives and tools.

II. Scenario 2: Third-party access to bundled individual-level data or aggregated data in aftermarket settings

1. The data access scenario

In data access scenario 1, an undertaking may depend on gaining access to the individual-level usage data of its potential customer in order to provide competitive complementary products or services. For such access, the undertaking should however turn to that customer for consent to data access. This is true for both personal data and non-personal data: if a competitor wants to offer products or services that build on individual-level usage patterns of a primary service, it is for that competitor to convince the potential customer to have that usage data transmitted to it. The question of whether that customer will be entitled to have the relevant data transmitted has been dealt with in data access scenario 1.

There are, however, cases in which a firm's ability to offer competitive aftermarket or complementary products or services depends on access to more than just individual-level usage data. In these cases, the potential customer cannot serve as the sole access point for the necessary data. For example, a complementary service provider may need access to large sets of *bundled* individual-level usage data for anonymous use[112] or to *aggregated* usage data[113] to provide complementary products or services that are competitive. Imagine, for example, a predictive maintenance service that requires aggregated data about the 'wear and tear' of a piece of equipment as training data for its prediction algorithm; or a firm that strives to offer road maintenance and needs access to aggregated in-car sensor data on road quality for this purpose. To the extent that bundled individual-level data or aggregated data are not available through, say, a data pool established by a large number of car owners, machine users or an intermediary

112 Cf. Crémer, Montjoye and Schweitzer (n. 27) 25–26: sets of anonymously used individual-level data are typically needed to extract (prediction) patterns out of usage data, but the goal is not to directly provide a service to the individual who generated the data in the first place. For example, with individual-level usage data of a significant amount of subscribers to a video streaming platform, one could train a neural network to make good movie recommendations based on the favourite movies of any given user.

113 Crémer, Montjoye and Schweitzer (n. 27) 26: 'Aggregated data, refers to more standardised data that has been irreversibly aggregated. This is the case for eg sales data, national statistics information, and companies' profit and loss statements. Compared to anonymous use of individual-level data, the aggregation is standard enough that access to the individual-level data is not necessary.'.

(on this, see 5. below), the complementary service provider would need to turn directly to the data controller for data access, i.e. the firm active on the primary market.

Scenario 2 also entails cases where the necessary data are not usage data. One of these cases is currently being investigated by the German *Bundeskartellamt*: Mobility platforms request access to real-time data about train departures and delays from the German railway operator Deutsche Bahn in order to tailor their offer to the needs of the users, e.g. to enable them to book all means of transport to their destination from a single source.[114]

In another subset of cases, competitors on up- or downstream markets face a competitive disadvantage due to the self-preferencing of a vertically integrated competitor. For example, independent retailers on Amazon Marketplace complain that Amazon (allegedly) gains a competitive advantage for its own retail activities on the platform by utilising aggregated data regarding user search and click behaviour on the marketplace.[115] While, in principle, retailers operating on the platform could depend on data access to the Marketplace users' aggregated usage data to remain competitive (hence, a 'clear' data access scenario 2 case), the underlying competition problem is one of a lacking level playing field. It could equally be, and arguably should rather be, addressed by prohibiting Amazon from utilising the Marketplace data for its own merchant activities (see below, 3.).

114 Bundeskartellamt, Press Release of 28 November 2019, 'Proceeding against Deutsche Bahn AG – Bundeskartellamt examines possible anticompetitive impediment of mobility platforms' <https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/28_11_2019_DB_Mobilitaet.html> accessed 15.09.2020.

115 The European Commission is currently investigating this conduct: European Commission Press Release of 17 July 2019, 'Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon' <https://ec.europa.eu/commission/presscorner/detail/en/ip_19_4291> accessed 15 September 2020. On the antitrust hearing before the US Congress, see, *inter alia*, Washington Post Online of 30 July 2020, 'Amazon may have used proprietary data to compete with its merchants, Bezos tells Congress', <https://www.washingtonpost.com/technology/2020/07/29/bezos-testimony-data-antitrust/> accessed 15 September 2020.

2. Possible market failures

In well-functioning markets, access to the necessary bundled and aggregated datasets would arguably be made available by the data controller at an efficient market price. Where the market for the primary product or service is fully competitive, firms active on that market should again be expected to develop different approaches to data openness that cater to the different preferences of their customers. Open systems would try to convince their customers by means of their broad range of diverse complementary services offered on competitive aftermarkets. Closed systems would point to the pros of a more controlled aftermarket environment, possibly with higher quality standards and a higher degree of cybersecurity.[116] Also, a higher commitment to privacy standards may be an argument for not passing on customer usage data, even in the aggregate.

But again, the possibilities for market failures are manifold. In principle, they resemble those identified for scenario 1: information asymmetries may result in customer choice being impaired by bounded rationality. Also, dominant data controllers may find it attractive to extract monopoly rents. Consequently, it may be attractive for firms active on primary product or services markets to foreclose access of potential competitors to aftermarkets to a degree that is not in line with customer preferences.

In some instances, the transaction costs associated with the marketing of data will be prohibitively high.[117] This can result from, *inter alia*, difficulties in estimating the commercial value of the data[118] or uncertainty about the legality of data sharing in the light of the GDPR and Article 101 TFEU.[119] When it comes to personal data, the GDPR may indeed constrain the ability of data controllers to provide access to bundled individual or aggregate data.[120] The same is true with regard to constraints following from

116 On the comparison of the pros and cons of open vs. closed systems see, *inter alia*, Shapiro and Varian (n. 60); Autorité de la concurrence and CMA, 'The economics of open and closed systems' (2014) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387718/The_economics_of_open_and_closed_systems.pdf> accessed 15 September 2020.

117 Martens and others (n. 15) 6; Kerber and Frank (n. 98) 16–17.

118 Tormo (n. 47); Nguyen and Paczos (n. 47) 31–38.

119 Cf. German Federal Ministry of Economic Affairs and Energy, Report by the Commission 'Competition Law 4.0' (n. 46) 56–59.

120 These constraints may be avoided through anonymisation. For an overview of anonymisation techniques and the 'differential privacy' approach towards anonymisation, see Julian Hölzel, 'Differential privacy and the GDPR' (2019) 5 European Data Protection Law Review 184.

Article 101 TFEU with regard to commercially sensitive information. Under these circumstances, the emergence of well-working data markets remains a challenge.

3. Legislative reactions

The EU legislator has been cautious in mandating data access in scenario 2 settings.[121] Article 6(1) Regulation (EU) 715/2007[122] obliges car manufacturers to provide independent repairers with unrestricted, non-discriminatory[123] and standardised access to vehicle repair and maintenance information – but not with access to in-car data more generally.[124]

With regard to the Electricity Directive, some uncertainty remains whether the right to access energy consumption and energy input data collected through connected 'smart' meters extends to scenario 2 settings. While energy consumers can provide a data access point to the providers of complementary services for their individual-level data (see above), it is not entirely clear whether these providers can gain 'direct' data access on the grounds of Article 23(2) Electricity Directive as an 'eligible party' (in a non-discriminatory way, under 'clear and equal terms'; see Article 34). In an earlier draft of the Electricity Directive, the provision entailed a non-exhaustive enumeration of 'eligible parties', including, *inter alia*, 'other parties which provide energy or other services to customers'.[125] It therefore

121 There has been notable regulatory action in the area of road transport with regard to scenario 2. An exhaustive overview of this legislation is provided by Julien Debussche, Jasmien César and Isis De Moortel, 'Big Data & Issues & Opportunities: Data Sharing Obligations' (2019) <https://www.twobirds.com/en/news/articles/2019/global/big-data-and-issues-and-opportunities-data-sharing-obligations> accessed 15 September 2020; European Commission, 'Intelligent transport systems: Action Plan and Directive' <https://ec.europa.eu/transport/themes/its/road/action_plan_en> accessed 15 September 2020. Data access obligations provided in the various Delegated Regulations are, however, of a rather fragmentary nature. This paper will not address them in more detail.

122 Regulation (EC) No. 715/2007 (n. 98).

123 Compared to the access given to authorised dealers and repairers.

124 For the ongoing debate on whether access to in-car data – including access to bundled individual-level data and/or aggregated usage data – should be mandated, see Section C.I.5.a) above (with regard to scenario 1; the debate extends to scenario 2, however).

125 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on common rules for the internal market in electricity' COM(2016) 864 final, 2.

seems that access rights are also granted to providers of products and services seeking access to aggregated smart meter data. Access to bundled individual-level data will, however, only be covered by the Directive as far as that data can be shared in compliance with the GDPR[126] (through, *inter alia*, anonymisation).

The PSD2 Directive does not cover scenario 2; access to accounts and access to account data is only to be granted by request of the account holder.[127]

4. Competition law

In the absence of a sector-specific regime, requests for access to data have to be based on competition rules. The question of whether and when a denial of access constitutes an abuse of dominance under Article 102 TFEU and/or – under German competition law – under Section 19(2) No. 4 GWB continues to be debated.[128]

Firstly, a position of dominance must be established case by case. In some cases, a firm will be dominant on a specific product or services market. This would appear to be the case, for example, for the Deutsche Bahn in the *Bundeskartellamt*'s investigation on access of mobility platforms to real-time schedule data. In other settings, the question arises whether each product or service provider should be considered to hold a dominant position vis-à-vis those customers who are locked into that product or service, i.e. on the relevant 'aftermarkets'. A precise and context-specific analysis will be necessary in this regard, in particular in the typical settings described above: In a data economy, the exclusive control over the usage data of a product or service may automatically lead to significant competitive advantages for all related complementary or aftermarket services, irrespective of a dominant position on a broader market for such products or services. Nonetheless, the efficiencies related to 'closed systems' strategies

126 Any processing of personal data within the framework of the Electricity Directive needs to comply with the GDPR, pursuant to Art. 23(3) Electricity Directive.

127 See Art. 66(2) PSD2 Directive ('When the payer gives its explicit consent') and Art. 67(2)(a) PSD2 Directive ('only where based on the payment service user's explicit consent').

128 See, *inter alia*, Crémer, Montjoye and Schweitzer (n. 27) 98–107; Schweitzer and others (n. 4) 162–71; German Federal Ministry of Economic Affairs and Energy, Report by the Commission 'Competition Law 4.0' (n. 46), 36–37; Graef, Tombal and de Streel (n. 30) 13–17.

should be recognised – also under the novel conditions of the data economy. Not every lock-in should lead to the acknowledgment of a dominant position on a narrowly defined primary market. One of the important tasks for the European Commission will be to re-define the contours of the so-called aftermarket doctrine with regard to the specificities of the data economy.[129]

The German legislator, on the other hand, seems to be committed to expanding the scope of the aftermarket doctrine, albeit not on the basis of Section 19 GWB (concerning dominance),[130] but on the basis of an expansion of the concept of relational power. The new Section 20(1a) GWB proposed in the current draft of a 10th amendment to the GWB would grant an undertaking a right to data access where it is '*dependent on* access to data controlled by another undertaking *for its own activities*' even 'if there is no trade yet in such data', i.e. even if the data controller has not marketed the data before.[131] The provision does not require a showing of dominance; rather, a bilateral power asymmetry that may stem simply from one firm's dependency on the data controlled by the other firm will suffice. Finally, the refusal of access to such data would need to be an abuse of the bilateral power disparity, which is to be established through a comprehensive balancing of interests in the light of the law's objective to provide for freedom of competition.[132] While the proposed Section 20(1a) GWB seems to be tailored to establishing data access rights of the scenario 2 type, this broadening of potential data access obligations is controversial.[133] Its limits – including those resulting from the GDPR, trade secret protection and Article 101 TFEU – will need to be explored by the courts.

---

129 See European Commission Notice of 9 December 1997 on the definition of relevant market for the purposes of Community competition law [1997] OJ C372/3, para. 56. The Commission is currently revising the Market Definition Notice; see Press Release of 26 June2020, 'Competition: Commission consults stakeholders on the Market Definition Notice' <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1187> accessed 15 September 2020. For a discussion of the aftermarkets doctrine with regard to data access rights see also Crémer, Montjoye and Schweitzer (n. 27) 87–91, 101–06, 125.

130 The new Sec. 19(2) No. 4 GWB is rather of a declaratory nature.

131 Emphasis added. See Schweitzer and others (n. 4) 192–93.

132 German Federal Supreme Court (BGH) of 26 October 1972, Case KZR 54/71 (1973) Gewerblicher Rechtsschutz und Urheberrecht 277, 278–79 – *Ersatzteile für Registrierkassen*.

133 Torsten Körber, '"Digitalisierung" der Missbrauchsaufsicht durch die 10. GWB-Novelle' (2020) Multimedia und Recht 290, 292; German Federal Ministry of Economic Affairs and Energy, Report by the Commission 'Competition Law 4.0' (n. 46) 24–25, 36, 52.

When it comes to establishing an abuse under Article 102 TFEU (or Section 19(2) No. 4 GWB), on the other hand, the essential facilities doctrine will typically provide the relevant test. Generally, data – like any other resource – can, in a given situation, be an input, access to which is essential in order to compete.[134] However, the preconditions for applying the essential facilities doctrine are generally strict.[135] The immediate improvement of competition on a downstream market must be balanced against the negative incentive effects on the dominant firm that may result from a requirement to share. Also, where access to an input is granted, competitors are relieved from the need to compete on the primary market, such that more competition downstream may come at the cost of durable entrenchment of market power upstream. Furthermore, access remedies frequently require the precise specifications of access conditions and price as well as intense and constant oversight within a framework that can come to resemble a regulatory scheme (see B. above). Against this background, the question whether an input, including data, qualifies as an essential facility in any given case must be analysed with caution. Some have suggested relaxing the standard due to the non-rivalry of the use of data.[136] Others have pointed to the need to precisely examine the incentive effects case by case.[137]

Finally, and obviously, the limits to data sharing that follow from both the GDPR and Article 101 TFEU will remain in place. For example, both the GDPR and Article 101 TFEU may constrain the access of traders on Amazon to aggregated data regarding user search and click behaviour. In

134 Crémer, Montjoye and Schweitzer (n. 27) 101–05. The German legislature is about to clarify the essential facilities doctrine in this regard. In the course of the pending 10th amendment to the GWB (n. 88). Sec. 19(2) No. 4 GWB is to be amended to specify that data can qualify as an essential facility. This amendment is generally perceived to be purely declaratory in nature: see, *inter alia*, Torsten Körber, 'Die 10. GWB-Novelle als "GWB-Digitalisierungs-Regulierungs-Gesetz"' (2019) Neue Zeitschrift für Kartellrecht 633, 634.

135 See Ernst-Joachim Mestmäcker and Heike Schweitzer, *Europäisches Wettbewerbsrecht* (3rd edn, CH Beck 2014) § 19 paras 66–80.

136 Inge Graef, 'Rethinking the Essential Facilities Doctrine for the EU Digital Economy' (2019) TILEC Discussion Paper No. DP2019–028, 19–23 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3371457> accessed 15 September 2020; Schweitzer and others (n. 4) 171.

137 Alexandre de Streel, 'Essential Facilities Doctrine in the data-driven economy', Presentation for FSR and FCP at the Annual Scientific Seminar in Florence (22 March 2018) <https://www.slideshare.net/FSRCommunicationsand/essential-facilities-doctrine-in-the-datadriven-economy-alexandre-de-streel> accessed 15 September 2020.

such settings, the competition problem may not be one of a denial of access to data, but rather of a self-preferencing of the platform in granting access to its own trading subsidiary.[138] The appropriate remedy would then be the denial of access to all traders, or access to all on a basis compliant with the GDPR and competition law.[139]

Furthermore, a debate has started over whether the essential facilities doctrine should, where it would apply in principle, also benefit data-rich Big Tech platforms. Granting access to an essential facility is intended to allow market entry; while this is generally desirable from a competition policy perspective, the expansion of Big Tech conglomerates into ever more markets raises concerns: it may allow them to expand their position of dominance to ever more neighbouring markets, expanding their ecosystem and further increasing their competitive advantages from network effects and data concentration. Such a development might make it impossible for challenger firms to grow within a niche market until they are in a position to attack an incumbent platform in its core market. Consequently, an argument can be made that data access – in particular access to IoT usage data – should only be granted to the data-rich Big Tech players on the precondition that they reciprocally open their own data troves to competitors, thereby establishing a (more) level playing field.

Overall, the state of debate on how to handle data access in settings belonging to scenario 2 is still in flux. Few cases have been publicised so far (see 1. above). In some settings, contractual data access agreements will likely emerge. In other settings, the GDPR as well as Article 101 TFEU and trade secret protection will significantly constrain the possibility for data access in these settings from the start – apart from access to highly aggregated and possibly historical data. Furthermore, it is, as of now, unclear how strong the foreclosure effects for third parties will tend to be that result from a lack of access to bundled individual and aggregate data and whether third-party service providers will find ways to overcome these hur-

138 Schweitzer and others (n. 4) 124–28.

139 The 10th amendment to the German GWB (n. 88) also envisages the introduction of special conduct requirements with regard to self-preferencing by (vertically integrated) undertakings on multi-sided or network markets with paramount significance for competition across markets. The proposed text of Sec. 19a(2) No. 1 GWB reads: 'The Bundeskartellamt may prohibit such undertakings whose paramount significance for competition across markets it establishes, … to treat the offers of competitors differently from its own offers when providing access to supply and sales markets.'.

dles without access to data controlled by the primary product or service provider.

As of now, broad-brush solutions to scenario 2 do not seem to be available or desirable. A relevant case law will need to evolve to provide a better idea of the relevant settings. Given this, the case-by-case approach and context sensitivity of competition law is a strength rather than a shortcoming.

5. Policy options: The role of data intermediaries

As competition law appears to be an appropriate instrument to address anti-competitive refusals to provide access in scenario 2 cases, updated guidelines on how to deal with aftermarket settings will be useful.

Further-reaching policy options are less clear. However, the number of competitively problematic scenario 2 settings could significantly decrease if data intermediaries were to establish themselves in the marketplace. In principle, data intermediaries could provide effective solutions both with respect to personal data and with respect to non-personal data. They may be able to significantly alleviate the transaction cost problem identified above (C.II.2.).[140]

With regard to personal data, data trustees have already caught the attention of policy makers. Data trustees could not only facilitate the access by third parties to individual-level personal data. Intermediaries of some size could also serve as data aggregators and significantly alleviate data shortages of third parties in this regard.

Similarly, data intermediaries of some size could aggregate usage data of a non-personal kind and make it available to firms with an interest in developing complementary services. Initiatives of this kind already exist.[141] Data intermediaries that aggregate usage data provided by machine and service users could evolve from sectoral data pooling initiatives.

The best available and most agile, pro-competitive and innovation-friendly policy option to improve data access in scenario 2 settings therefore seems to be to facilitate and support the set-up, experimentation with and growth of data intermediaries. Much work remains to be done in this regard. With a view to data trustees that would administrate access to per-

140 Martens and others (n. 15) 6.

141 See, for example, the International Data Space of the Fraunhofer Institute, <https://www.fraunhofer.de/de/forschung/fraunhofer-initiativen/international-data-spaces.html> accessed 15 September 2020.

sonal data, possible conflicts of interests must be investigated and addressed in a governance framework and regulatory scheme that ensures that data access is managed in line with the will and best interests of consumers. At the same time, a viable business model would need to emerge. This is also true with regard to non-personal data. Furthermore, workable governance regimes for data pools would arguably need to be developed. Nonetheless, the establishment of data intermediaries appears to be a promising path to overcome data access bottlenecks that risk becoming a relevant hindrance for the evolution of a competitive data economy.

III. Scenario 3: Access to data for innovation purposes

1. The data access scenario

The third scenario which has attracted much attention and debate starts from the observation that '[c]urrently, a small number of Big Tech firms hold a large part of the world's data', and that this could 'reduce the incentives for data-driven businesses to emerge, grow and innovate in the EU'.[142] The question therefore is whether the vast data troves accumulated by the particularly data-rich digital conglomerates, for instance Google and Facebook, should be made available, in one way or another, as an input for innovation. Prominently, this has been suggested by Mayer-Schönberger and Ramge in their book *Reinventing Capitalism in the Age of Big Data*,[143] in which they propose a general obligation to share a randomly selected percentage of a firm's data that progressively increases with respect to the total size of the firm's data troves (similar to a tax). In Germany, the Social Democratic Party (SPD) has called for 'data for all' legislation.[144]

Obviously, the big online platforms can also be the addressees of access-to-data requests under scenario 1 and/or 2, where data access is needed to compete on a specific complementary market. This is, however, not the logic of scenario 3. In this setting, the question is whether data should be made available to search for new business ideas, or as an input to train AI, which may then be used to compete on completely unrelated markets.

142 European Commission, 'A European strategy for data' (n. 1) 3.

143 Viktor Mayer-Schönberger and Thomas Ramge, *Reinventing Capitalism in the Age of Big Data* (Basic Books 2018).

144 SPD, 'Digitaler Fortschritt durch ein Daten-Für-Alle-Gesetz' (2019) <https://www.spd.de/fileadmin/Dokumente/Sonstiges/Daten_fuer_Alle.pdf> accessed 15 September 2020.

Some conceive of the data troves of Big Tech as quasi-infrastructural resources, similar to public sector data. In this perspective, the data should ideally be available to anybody for experimentation and re-use, with no need to specify the relevant business purpose *ex ante*.

2. *Possible market failures*

Scenario 3 refers back to the fundamental choice between a 'private data control' versus an 'open access' approach (see B. above).

From a private data control perspective, there is a possible market failure to be addressed: extreme economies of scale and network effects have made the big online platform markets tip. The resulting quasi-monopolistic positions are accompanied by a persistent access to a huge stream of rich, high-quality user and usage data. This data not only allows the platforms to constantly improve the quality of service, in particular by providing an ever more targeted service, such that access to data is at the heart of a constant feedback loop safeguarding the existing position of dominance. At the same time, it enables Big Tech firms to monetise their service in the market for targeted online advertising, which is, to a significant extent, a competition for access to the best data troves. Given the general-purpose quality of user data, it can simultaneously provide big B2C platforms with a competitive edge when entering other consumer services markets.

The latter aspect, however, falls under scenarios 1 and 2. Whether a general opening up of the Big Tech data troves would help to make their position on the relevant online platform markets contestable is quite unclear.

The more obvious rationale underlying the call to open up the Big Tech data troves therefore is to enable data-driven innovation on a broad scale. Implied is the proposition to revisit our choice of a private data control approach for scenario 3. The Big Tech data troves are found to flow from the new infrastructural monopolies of the digital times. Purportedly, they are so inextricably intertwined with the structure of our societies that they should be opened up for their broader purposes.

However, whether this line of argument justifies a shift to an open access rationale with respect to the Big Tech data troves is not yet settled. Such a rationale would be in an obvious tension with the GDPR. Much of the behavioural data collected by the big online platforms is personal data in its origin. Their anonymisation may prove to be difficult[145] and may

145 For more details on differential privacy see Hölzel (n. 120).

significantly reduce their value. Nor can clashes with Article 101 TFEU and trade secret protection be ruled out. Moreover, a simple opening of access to the mass of data that Big Tech controls may not be what is really needed and can be used in any meaningful way by innovative firms, including start-ups who may lack the technical infrastructure to handle such volumes of data. Rather, the innovative potential of these data may better be realised by some sort of curated access, an access to a selection of datasets relevant for different purposes, and sometimes access to annotated data.

3. *Competition law*

There is, as of now, no legislative action that attempts to open up the data troves of the Big Tech online platforms for general access.

Obviously, competition law is applicable to the Big Tech online platforms, also with regard to data access requests for innovative purposes. In principle, such requests could, again, be based on the essential facilities doctrine. In this setting, the indispensability of data access would not follow from the principled non-replicability of the data set as in the aftermarket setting, but from the scale and scope of the data pool:[146] specific types of data analysis may only be feasible based on data pools of a size and depth that only the big online platforms control. Whether and which data would qualify as essential and indispensable would then, however, depend on the specific business case of any given petitioner. Yet, a requirement for them to lay open their business plans vis-à-vis the incumbent would give the latter the chance to quickly replicate promising projects, and would therefore raise serious competition concerns. Instead, the essentiality check would either need to be done by a neutral intermediary; or a mechanism would be needed that would ensure data access without an essentiality check. Basically, the latter would translate into an open-access approach. In any case, some sort of curated data access would seem to be required. Also, data access would need to be checked for its GDPR and Article 101 TFEU

146 Crémer, Montjoye and Schweitzer (n. 27) 103. The notion of indispensability within the essential facilities doctrine has been intensely discussed, often with strongly varying results. See Thomas Tombal, 'Economic Dependence and Data Access' (2020) 51 International Review of Intellectual Property and Competition Law 70, 81–86; Martens and others (n. 15) 36; Schweitzer and others (n. 4) 164–68; Giuseppe Colangelo and Mariateresa Maggiolini, 'Big data as misleading facilities' (2017) 13 European Competition Journal 249, 270–73; Drexl (n. 31) 282.

conformity. Regulatory oversight would need to ensure that the access conditions and the access price are fair, reasonable and non-discriminatory. All this would risk resulting in a rather heavy-handed regulatory regime. The 'special obligation' imposed on the big online platforms would surpass what is normal under the essential facilities doctrine.

4. Policy options?

Prospectively, the data power of the big online platforms may present the greatest challenge in the endeavour to ensure a competitive data economy. While competition on markets for complementary services can arguably be ensured based on the solutions proposed above (see scenario 1 and 2), the control of huge amounts of behavioural data can provide for a competitive edge in the development of data processing technologies like AI that will drive innovation in great parts of the economy in the years to come. At the same time, the existing instruments do not seem to provide an appropriate lever to address the problem underlying scenario 3.

So far, the Commission has been reluctant to move in the direction of an open access approach for the big online platforms' data troves. In its 'European strategy for data', it has announced that it will consider 'how best to address more systemic issues related to platforms and data, including by ex-ante regulation if appropriate, to ensure that markets stay open and fair'.[147]

From a market perspective, however, a voluntary and/or structural solution would seem to be preferable to ex-ante regulation. For example, one may envision the establishment of a data controlling entity that would be separate from the entity that operates the online platform and would have incentives to make the data accessible on a commercial basis in a neutral manner.[148] Such a model could promote data-driven innovation and at the same time neutralise the data-based conglomerate power of the big online platforms. Simultaneously, it would tend to intrude less into the platforms' business decisions in a longer-term perspective and be more likely to establish a level playing field.

In Germany, the proposed Section 19a GWB is specifically addressed to the (usually data-rich) undertakings on multi-sided or network markets

147 Commission, 'A European strategy for data' (n. 1) 14.

148 For another proposition to implement intermediaries to reduce market failures on data markets see Martens and others (n. 15) 28–34.

that are 'of paramount significance for competition across markets'. It may allow for some form of structural data unbundling: Section 19a(2) No. 1 GWB enables the *Bundeskartellamt* to prohibit self-preferencing practices, which could either encompass an obligation to share the same data under the same conditions with external business partners as in-house, or a prohibition to use said data for a firm's own commercial activities on up- or downstream markets. Section 19a(2) No. 3 GWB would allow the *Bundeskartellamt* to prohibit measures that create or raise barriers to market entry or impede other undertakings with other means by using data relevant for competition which has been obtained from the opposite market side on a dominated market, also in combination with other data relevant for competition from sources beyond the dominated market, or demand terms and conditions that permit such use.

The prohibition is specifically tailored to address data-related platform envelopment strategies[149] such as the data bundling of Facebook, Instagram and other Facebook services that was prohibited by the *Bundeskartellamt*'s decision in February 2019.[150] It could serve as a basis to enforce 'horizontal' data unbundling, meaning a prohibition to merge data acquired on different markets within a single, large data pool.

Section 19a GWB, however, will not provide for a structural remedy which mandates the 'unbundling' of the operation of a service and the control over the data generated through this service, thereby creating an independent data controller that would be incentivised to market the data to a multitude of firms.

149 See Daniele Condorelli and Jorge Padilla, 'Harnessing Platform Envelopment through Privacy Policy Tying' (2019) <https://ssrn.com/abstract=3504025> accessed 15 September 2020.

150 Bundeskartellamt of 6 February 2019, Case B6–22/16. The Bundeskartellamt prohibited Facebook from requiring their users to consent to a bundling of data collected through Facebook's various digital services and to consent to a bundling of data collected through the Facebook social plugin APIs. For such an integration of different user data within one profile, Facebook would in the future need users' express consent (opt-in), which must not be made a contractual requirement for the use of the social network. The Bundeskartellamt framed the case as an exploitative abuse of dominance, basing the contract conditions' disproportionality on their violation of data protection law. Facebook has appealed the decision before the Higher Regional Court. In a preliminary proceeding, the Federal Supreme Court has indicated that it will ultimately uphold the Bundeskartellamt's decision, albeit based on a different line of reasoning – see German Federal Supreme Court (BGH) of 23 June 2020, Case KVR 69/19.

At the European level, the 'new competition tool'[151] may provide an instrument to require the establishment of a separate data-trading entity – in particular as a remedy to data-driven conglomerate strategies by the big digital platforms by which they try to expand their digital ecosystems and reinforce consumer lock-in.

D. A brief summary

Stepping back, data access remains a convoluted topic. Given the broad variety of data and data access scenarios, there cannot be a 'one size fits all' approach towards data access. Quite in line with the European Commission's agenda, the best way to develop solutions that are tailored to the different settings is to continue with and encourage the ongoing process of decentralised experimentation[152] based, in principle, on a private control approach for data and a system of data allocation through freely negotiated contracts on competitive markets. Already, firms are increasingly trying out various forms of data-sharing arrangements. The Commission strives to facilitate such voluntary data sharing and to put in place an 'enabling legislative framework for the governance of common European data spaces'[153] that will address persisting disincentives to pursue such initiatives[154] in non-interventionist ways.[155] Also, it supports data-driven innovation and strives to stimulate demand for data-driven products and services

151 European Commission, 'Proposal for a Regulation by the Council and the European Parliament introducing a new competition tool', Ares (2020) 2877634.

152 See Commission, 'A European strategy for data' (n. 1) 12–13, generally favouring a market-based approach to data access: 'The general principle shall be to facilitate voluntary data sharing'; 'Only where specific circumstances so dictate … access to data should be made compulsory'.

153 Ibid. 12.

154 See Ibid. 7, where the following reasons for the current reluctance to share data B2B are identified: 'a lack of economic incentives (including the fear of losing a competitive edge), lack of trust between economic operators that the data will be used in line with contractual agreements, imbalances in negotiating power, the fear of misappropriation of the data by third parties, a lack of legal clarity on who can do what with the data'.

155 *Inter alia*, by supporting decisions on what data can be used in which situations, by facilitating cross-border data use, by prioritising interoperability requirements and standards within and across sectors and by codifying usage rights for co-generated data.

by promoting Europe's capabilities and infrastructures for hosting, processing and using data – not by regulating data access.

To support the search for novel and creative forms of cooperation, firms are to be provided with an opportunity to obtain legal certainty regarding the compatibility of such endeavours with competition rules. The Commission has already signalled its readiness to provide informal guidance more frequently.[156] Additionally, the introduction of a voluntary notification procedure for novel forms of cooperation (with a right to receive a decision within a short period of time) has been proposed.[157] The ongoing review of the Commission's Guidelines on Horizontal Cooperation Agreements will provide a welcome opportunity to systematise and clarify the assessment criteria for the new types of B2B data sharing and pooling agreements already observed or to be expected within the novel context of

156 See Commission, 'A European strategy for data' (n. 1) 14: 'The Commission is … prepared to provide additional individual project-related guidance on the compatibility with EU competition rules, if needed'.

157 See the corresponding recommendation of the German Commission Competition Law 4.0: German Federal Ministry of Economic Affairs and Energy, Report by the Commission 'Competition Law 4.0' (n. 46) 59–60, Recommendation 14. The 10th amendment to the GWB includes a provision that would grant undertakings – under certain conditions – a subjective right to a decision of the Bundeskartellamt on whether it sees, on the basis of the information in its possession, no grounds to initiate infringement proceedings. Sec. 32(1), (4) GWB reads:
(1) The competition authority may decide that there are no grounds for it to take any action if, on the basis of the information in its possession, the conditions for a prohibition pursuant to §§ 1, 19 to 21 and 29 [GWB], Article 101 (1) or Article 102 of the Treaty on the Functioning of the European Union are not satisfied. The decision shall state that, subject to new findings, the competition authority will not exercise its powers under §§ 32 and 32a [infringement proceedings and interim measures]. …
(4) Undertakings or associations of undertakings shall be entitled to a decision pursuant to para. 1 from the Bundeskartellamt if they have a substantial legal and economic interest in such a decision with regard to cooperation with competitors. The Bundeskartellamt shall decide on an application pursuant to sentence 1 within six months.

the digital economy.[158] New models of data trusteeship and public support for such business models may help to promote access to consumer data.[159]

However, while competition law will serve as an important – and necessary – background regime, it has its limits. While its case and context sensitivity is among the great strengths of competition law, this strength can become a shortcoming at times: a case-by-case analysis is resource-intensive and slow and comes with a significant degree of legal uncertainty. Where data access requirements are of systemic relevance and no satisfactory structural solution is available that allows for a self-enforcing and incentive-based data access regime, sector-specific data access regulation may be needed.

To ascertain the optimal policy approach in different data access settings, we identified three scenarios that we believe cover a wide area of potential cases:

(1) Access to individual-level data by a co-generator of usage data in a bilateral scenario to facilitate switching and the utilisation of independent aftermarkets products and service providers,
(2) Requests for access to bundled individual-level data or aggregated datasets by a third party vis-à-vis a service or product provider who controls broad usage datasets, with the third party claiming that access to the relevant data is needed to effectively compete in complementary markets;
(3) Requests by firms to access the large usage data troves of Big Tech to compete and innovate in the area of AI.

Taking these scenarios as reference points, we submit the following recommendations:

Scenario 1: With regard to scenario 1, we need to distinguish between access to personal data and access to non-personal industrial data.

When it comes to personal data, Article 20 GDPR already provides for a broadly applicable data portability right, which is however not tailored to

158 See European Commission, 'A European strategy for data' (n. 1) 14. Some insights regarding the current stance of the Commission can be taken from an investigation into the data pooling system of Insurance Ireland opened in May 2019 – see Euoropean Commission Press Release of 14 May 2019, 'Antitrust: Commission opens investigation into Insurance Ireland data pooling system' <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2509> accessed 15 Septemberv2020.

159 German Federal Ministry of Economic Affairs and Energy, Report by the Commission 'Competition Law 4.0' (n. 46) 42–43, Recommendation 5.

relevant market failures and does not encompass a right to data interoperability. Where real-time access is needed to overcome a market failure, sectoral regulation is currently the best approach, following the example of the PSD2 Directive and of the Electricity Directive. Competition law provides an important background regime. Market-based solutions could emerge if personal data cooperatives or neutral data intermediaries were to evolve.

No right to access, portability or interoperability currently exists for data co-generators with regard to co-generated industrial usage data in B2B settings. A legislative acknowledgment of a right to real-time access and portability could significantly promote competition in a data-driven economy: It would establish multiple access points to usage data in settings that are otherwise prone to lock-in effects, both with regard to the primary product and/or service and with regard to aftermarkets. Generally, these access and usage rights should remain waivable, however, to grant the parties involved the necessary flexibility in finding the best data access approach for their bilateral relation. Although a waivable access, usage and portability right would not protect business users against information asymmetries, market power and bilateral power imbalances, the recognition of the right would serve as an important legal reference point. Contractual waivers could – depending on the setting – be restrictive to competition by object or effect and therefore fall under Article 101 TFEU. A block exemption regulation could regulate the conditions under which they will nonetheless be considered pro-competitive.

Scenario 2: Settings where firms need access to individual-level data to offer complementary or aftermarket services will and should be dealt with under scenario 1. The situation is different where access to bundled individual-level data and aggregated data is required to compete effectively. For these settings, competition law is – and will arguably remain in most cases – the relevant regime. Its case-by-case approach and context sensitivity is a strength rather than a shortcoming here. In cases of frequent and repeated market failures, sectoral regulation may need to emerge.

With respect to competition law, the aftermarket doctrine will need clarification through updated guidelines.

A general easing of the requirements of the essential facilities doctrine should be regarded with caution. A relevant case law will need to evolve to provide a better idea of the relevant settings.

The policy approach most in line with a private control approach and a system of decentral coordination would be the promotion of data intermediaries that lead to the emergence of new data markets. Legislative action

should strive to facilitate and support the setting up of, experimentation with and growth of data intermediaries.

Scenario 3 remains the most challenging one. Based on Article 102 TFEU, a convincing and clear legal solution for access to the huge troves of behavioural data currently controlled by the big digital platforms is difficult to find. At the moment, it is not yet clear whether a general opening up of these data resources is appropriate and required to ensure competition – in particular effective competition in the field of AI. The situation will need to be monitored by the Commission.

In principle, data intermediaries (see scenario 2) could also be able to accumulate and offer for sale the vast data troves needed for technological progress in the field of AI.

Additional incentives for marketing the data could come from different forms of data unbundling: if in-house monetisation is limited and/or self-preferencing regarding data access becomes infeasible, firms in control of large data troves could be incentivised to market behavioural data neutrally. Markets for data could receive an important stimulus, and the risk of an ever-increasing data-driven expansion of digital B2C ecosystems may be reduced.

In our paper, we have tried to offer some additional insights regarding the role that the proposed 10th amendment to German competition law may play with regard to data access. For scenario 1, the proposed Section 19a(2) No. 4 GWB[160] will possibly provide an additional instrument to enforce data portability for co-generated individual-level usage data; however, its scope of application will be limited to platform or network operators with paramount significance for competition across markets. However, Section 19a(2) No. 4 GWB is not directly applicable. The existence of such a position will need to be established by the *Bundeskartellamt* first, and the *Bundeskartellamt* will then need to specify the data access obligations.

With regard to scenario 2, the (declaratory) clarification that data can qualify as an essential facility within Section 19(2) No. 4 GWB[161] will arguably not have a large impact, but it improves legal certainty, nonethe-

160 'The *Bundeskartellamt* may prohibit such undertakings whose paramount significance for competition across markets it establishes to make the interoperability of products or services or the portability of data more difficult and thereby impede competition. This shall not apply where the conduct in question is objectively justified. In this respect, the burden of presenting facts and the burden of proof lie with the undertaking in question.'.

161 'An abuse exists in particular if a dominant undertaking as a supplier or purchaser of a certain type of goods or commercial services refuses to supply another un-

less. Section 20(1a) GWB,[162] which expands the prohibition on unreasonably impeding competition to cases of relational power that exclusively stems from one undertaking's dependence on access to data of another undertaking will potentially have far-reaching impact, however. To prevent regulatory overreach, its limits would need to be cautiously explored by the courts.

With regard to scenario 3, the proposed Section 19a(2) No. 1[163] and No. 3[164] GWB could arguably provide for some form of data unbundling (No. 1: vertical unbundling by prohibiting self-preferencing; No. 3: horizontal unbundling by prohibiting the pooling of data across markets). Section 19a GWB will, however, not provide for a structural remedy.

---

dertaking with this product or commercial service against adequate remuneration, *including access to data*, networks or other infrastructure, the supply is objectively necessary in order to operate on an upstream or downstream market and the refusal to supply threatens to eliminate effective competition on that market, unless the refusal to supply is objectively justified.' (emphasis added).

162 'Dependency in the meaning of paragraph 1 may also arise from the fact that an undertaking is dependent on access to data controlled by another undertaking for its own activities. The refusal of access to such data may constitute an unfair impediment even if there is no trade yet in such data.'.

163 'The Bundeskartellamt may prohibit such undertakings whose paramount significance for competition across markets it establishes to treat the offers of competitors differently from its own offers when providing access to supply and sales markets. This shall not apply where the conduct in question is objectively justified. In this respect, the burden of presenting facts and the burden of proof lie with the undertaking in question.'.

164 'The Bundeskartellamt may prohibit such undertakings whose paramount significance for competition across markets it establishes to create or raise barriers to market entry or impede other undertakings with other means by using data relevant for competition which has been obtained from the opposite market side on a dominated market, also in combination with other data relevant for competition from sources beyond the dominated market, or demand terms and conditions that permit such use. This shall not apply where the conduct in question is objectively justified. In this respect, the burden of presenting facts and the burden of proof lie with the undertaking in question.'.