GRUR International, 72(4), 2023, 337–356

https://doi.org/10.1093/grurint/ikad012
Advance Access Publication Date: 8 March 2023
Article

HEIKE SCHWEITZER* / AXEL METZGER**

Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Cowmpetition and Innovation?

In the ongoing transformation from 'industrial capitalism' towards an 'informational capitalism', one of the core challenges is for the law to design and enforce an appropriate legal framework for access to and use of data. Focusing on access to data generated by the use of products or online services (product and online services usage data), the aim of this paper is to describe and systematize the core elements of this legal framework in the making and to provide some guidance on how it could be further developed. Access by the users of products or online services to the individual-level data that their usage generates must be distinguished from access to bundled individual-level and aggregated data by third parties. With regard to data co-generators' access to individual-level product usage data, the Draft Data Act proposes to create new rights to access that will become part of a new private law infrastructure of data rights. These access rights are granted independently of whether the data holder is dominant. With regard to data co-generators' access to individual-level services usage data, the Digital Markets Act (DMA) establishes rights of access only vis-à-vis gatekeepers within the meaning of the DMA. Third-party undertakings who request access to bundled individual-level or aggregated data can, as of now, only base their claim on Art. 102 of the Treaty on the Functioning of the European Union (TFEU) and – in the case of search data – on Art. 6(11) DMA. A regulatory approach has been proposed as an alternative. This paper strives to systematize this hodgepodge of approaches and discern the broader principles that can guide the legislature in creating and fleshing out the legal framework for data. Ideally, markets for bundled individual level or aggregated data will emerge based on the rights of data co-generators to access individual-level data. For this to happen, data intermediaries will have to play a larger role and succeed in bundling and marketing such data.

I. Introduction

In the ongoing transformation from industrial capitalism towards what has been termed 'informational capitalism',[1] one of the core challenges is for the law to design and enforce an appropriate legal framework for access to and use of data. Data have become an important input for production, distribution, marketing and innovation processes in almost all sectors of the economy. Their competitive relevance is constantly increasing. What is more, certain categories of data can be relevant across market boundaries and can be essential for interconnecting products and services in the Internet of Things (IoT).

Among the particularly important categories of data are behavioral data as generated by the use of online services, and usage data as generated by the use of products or machines. These data – frequently combined with other data – may be the basis for developing ever more individualized products or services and personalized marketing. Targeted advertising has driven the spectacular growth of some of the largest platforms – Google (Alphabet) and Facebook (Meta) in particular. In the context of the emerging IoT, machine usage data are the basis for predictive maintenance and for the development of other tailored aftermarket services or complementary services.

Yet, it is precisely for this core resource of the data economy that fundamental legal categories are still missing. This legal gap has driven past debates on whether property rights to data are needed.[2] The underlying idea

* Prof. Dr., LL.M. (Yale), Chair of Private Law and Competition Law, Humboldt-Universität zu Berlin, Germany.

** Prof. Dr., LL.M. (Harvard), Chair of Private Law and Intellectual Property Law, Humboldt-Universität zu Berlin, Germany.

1 See Manuel Castells, *The Rise of the Network Society* (2nd edn, Wiley Blackwell 2010); Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019).

2 In early statements, the Commission considered the introduction of a 'data producer's right', see European Commission, 'Building a European Data Economy' COM(2017) 9 final, 13. For a critical analysis see Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' [2016] GRUR Int 989; Daria Kim, 'No one's ownership as the status quo and a possible way forward: A note on the public consultation on Building a European Data Economy' (2018) 13 JIPLP 154; Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 on the European Commission's 'Public consultation on Building the European Data Economy'' <https://ssrn.com/abstract=2959924> accessed 23 January 2023. For parallel discussions in Germany see Koalitionsvertrag zwischen CDU, CSU und SPD 19. Legislaturperiode [2018] 129; Marc Amstutz, 'Dateneigentum' [2018] AcP 438; Karl-Heinz Fezer, 'Repräsentatives Dateneigentum' (2018) Studie im Auftrag der Konrad-Adenauer-Stiftung.

was that the novel challenges would be easier to solve if we were to transfer established legal categories to data.

Simultaneously, many have highlighted the tension between the urgent need to facilitate a wide and competitive use of data for innovative purposes and the proposed creation of property rights to data: In line with the goal of promoting and expanding the use of data – a resource that is non-rival by its very nature – the legislature should not strive to create rights to exclude, but rather focus on the creation of rights of access to data.[3]

As of now, rights of access to data are limited: According to Art. 15 of the General Data Protection Regulation Regulation (GDPR), every data subject has a right to access the personal data concerning him or her, and Art. 20 GDPR grants data subjects a right to port these data. In addition, some regimes of sector-specific regulation have established rights to access individual-level data – e.g. in the field of banking and energy (see below, III.2.). Given the inherent constraints of these rights of access, commentators have turned to competition law as an already existing body of rules that applies horizontally and comes with a potentially powerful regime of public enforcement. A focus on competition law – and more particularly on Art. 102 TFEU and its national counterparts – seemed appropriate in particular to restore competition in and for data-driven ecosystems or to access the large troves of behavioral data as controlled and used across markets by a relatively small number of very large digital platforms.

However, to this day, competition law-based cases on access to data have remained scarce. Access to data has played a role in a handful of merger control decisions.[4] But few Art. 102 TFEU decisions deal with data – and no decisions have been passed so far that would mandate access of competitors to behavioral or product or machine usage data controlled by a dominant firm. Instead, the European Commission has published, in February 2022, a 'Proposal for a Regulation on harmonized rules on fair access to and use of data (Data Act)'[5] that proposes to introduce a new set of rights of access for product users and, derivatively, for third parties authorized by them, to the data generated by their use of the product – access rights which are independent of a position of market power of the data holder or a position of dependence of the requesting party. As regards data generated by the use of online *services*, the Digital Markets Act (DMA)[6] obliges designated gatekeepers – but only them – to provide effective data portability both for end users (Art. 6(9) DMA) and for business users (Art. 6(10) DMA).

This paper strives to systematize the debate on access to behavioral and/or product/machine usage data, to examine where we currently stand in the mastery of the new challenges and, based on this stock-taking exercise, to make some suggestions as to where we should go.

The attempt to systematize will build upon a well-known distinction between two different data access scenarios of practical importance: In the first scenario (scenario 1), market participants who have played a part in the generation of relevant data – e.g. as users of a service or machine – request access to the individual-level data generated by their use or the possibility to authorize third parties to have access on their behalf. In the second scenario (scenario 2), third parties who have had no part in the generation of the data request access to large sets of bundled individual-level or aggregate data to develop and improve complementary services within the framework of a data-driven value creation network.[7] One may envisage different legal rules to deal with each of these categories of data access requests. As regards scenario 1, the de facto allocation of control of the data may be accepted as given, and data access may be mandated only where, given the specific circumstances of a case, a refusal to grant access would amount to an abuse of dominance (Art. 102 TFEU). In addition, some sort of competition law-inspired regulation – like the DMA – might mandate particularly powerful data holders (e.g. gatekeepers) to grant data access to data co-generators irrespective of an abuse. Alternatively, rights to data access and use may be created irrespective of whether the original data holder holds a position of market power – as proposed by the Draft Data Act. Such rights may be established horizontally (as proposed, for some settings, by the Draft Data Act), or by way of sector-specific regulation. Legislation of this kind no longer limits itself to addressing well-defined market failures (like market power). Rather, it follows a market-shaping approach: it creates a new sort of parallel rights of access and use of data and thereby redefines the legal infrastructure based on which markets evolve. While the Draft Data Act's market-shaping agenda[8] seems plausible in principle, one may wonder why the users' right to access data generated by their activity is limited to data generated by the use of products and does not extend to the individual-level data generated by the use of services. Clearly, the right to data portability under Art. 20 GDPR does not fill this gap, as it is generally considered to be ineffective.

When it comes to data access scenario 2, endowing all potentially interested third parties with a right to data access and use is not an option: such a rule could significantly compromise the privacy interests of end users, result in a mandatory sharing of competitively sensitive information between competitors and could significantly compromise the incentives to generate data in the first place.[9]

3 See, for example Maximilian Becker, 'Rights in Data – Industry 4.0. and the IP Rights of the Future' [2017] ZGE 253; Josef Drexl and others, 'Ausschließlichkeits- und Zugangsrechte an Daten' [2016] GRUR Int 914; Louisa Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen' [2016] CR 288 with further references. For an economic analysis see Kerber (n 2).

4 For a review of the merger case law on data access see Heike Schweitzer and others, 'Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy' (2022) Report for the German Federal Ministry for Economic Affairs and Climate Action (BMWK) 175 ff <https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/20221026-data-access-and-sharing-in-germany-and-in-the-eu.pdf?__blob=publicationFile&v=4> accessed 23 January 2023.

5 COM(2022) 68 final.

6 Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1.

7 For a distinction between these two scenarios see already: Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition policy for the digital era' (2019) Final Report 75-76. See also Heike Schweitzer and Robert Welker, 'A legal framework for access to data – A competition policy perspective' in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Nomos 2021) 103, 115 ff.

8 On this see Axel Metzger and Heike Schweitzer, 'Shaping Markets: A Critical Evaluation of the Draft Data Act' [2023] ZEuP 42.

9 See also Schweitzer and Welker (n 7) 108-09 (with further references) who discuss potential 'tragedy of the commons' problems.

In this setting, a market failure framework – or more particularly the application of competition rules – appears to be the most plausible framework for justifying rights of access. So far, no relevant precedents exist, however. Nor do we observe a regulatory regime emerging. Notably, the DMA contains only one provision that falls into the scenario 2 category, namely Art. 6(11) DMA, relating to ranking, query, click and view data generated by online search engines offered by gatekeepers. No data access mandates would be necessary if markets for bundled individual level or aggregated data were to evolve, in particular if data intermediaries were successful in developing and marketing such products. With the passage of the Data Governance Act (DGA),[10] the European legislature strives to increase trust in data intermediaries and to encourage their proliferation. But with its highly regulatory approach, it may ultimately discourage rather than promote their establishment.[11] So far, data intermediaries have not yet gained broad traction.

In sum, as of now, the emerging European legal framework for data access still presents itself as a patchwork. With many promising bits and pieces, it does not yet form a coherent whole. This paper is the attempt to develop a conceptual grid that brings these pieces together and that helps to identify the missing parts. In doing so, it builds on a recent report for the German Economic Ministry on data access[12] and on a recent paper on the Draft Data Act.[13]

II. Access to data in the EU: From a market failure to a market-shaping approach

Data-driven markets are markets in the making: In the transformation towards an 'informational capitalism', undertakings experiment with novel data-driven business models and strategies. Unsurprisingly, different jurisdictions react differently to the friction that these experiments create.

In the US, there does not seem to be a widely perceived need to intervene in the 'natural' distribution of data access opportunities.[14] In the EU, by contrast, the debate on rights of access to data has picked up speed. Interestingly, the debate is not primarily driven by market actors: A number of surveys show that there are relatively few companies that consider access to external data to be a major impediment to the deployment of their business model. When asked about the largest barriers to data sharing, compliance with the GDPR[15] is frequently pointed out as the most prominent one. Mandatory data access is seen as a business opportunity by some, typically smaller, companies. Simultaneously, significant concerns are voiced by others, with regard to trade secrets in particular.[16]

Primarily, the push for more data access seems to come from policymakers. In line with Mariana Mazzucato's plea for an industrial and innovation policy that tackles the 'grand challenges' of the modern world,[17] European policymakers appear to be determined to establish a legal framework for data access that does not content itself with identifying and fixing market failures. Rather, they want to provide a legal framework for markets in the making, with a view to pro-actively opening up novel opportunities for data-driven competition and innovation, thereby pointing businesses to new growth opportunities. The Draft Data Act, with its focus on competitive and innovative data-driven aftermarkets in the IoT sector is exemplary in this regard.

This approach is combined with a focus on 'gatekeeper power' when it comes to the control of large troves of behavioral data by the largest digital platforms. The difference in approach – the creation of new horizontal private law rights to data access and use for data co-generators, independently of the existence of private power, in the IoT sector; a special category of regulatory data portability obligations imposed on digital gatekeeper platforms when it comes to online services – is notable and will be discussed below (see III.3.). Both the Draft Data Act and the DMA focus on access to individual-level data by data co-generators – i.e. on data access scenario 1.

The next section shall therefore review the state of the law as regards access to individual-level data (III.) and examine it critically (IV.). The state of the law as regards access to bundled individual-level or aggregate data will then be reviewed (V.) and discussed (VI.). The last section of this paper will pull together the various threads and conclude (VII.).

III. Access to individual-level data by the users of IoT products and of digital services

In our data access scenario 1, a firm has exclusive control of individual-level data – whether personal or non-personal – that were generated as a byproduct of a specific person's or undertaking's use of a particular product or service. A third party may need access to these data, typically to provide complementary or aftermarket services to the person or undertaking to which the data relate.[18] Where the data are controlled exclusively by the firm providing the primary product or service, the product or service user may be unable to provide the third party with such access, however.

Frequently, requests for access and use of individual-level data by the relevant 'data subject'[19] that has, through its activity, contributed to the generation of the data are referred to as requests for 'data portability'. There is, however, no established definition of this term. Originally – namely in the context of Art. 20 GDPR – data portability seemed to

10 Regulation (EU) 2022/868 of 30 May 2022 on European data governance (Data Governance Act) [2022] OJ L152/1.

11 Moritz Hennemann and Lukas von Ditfurth, 'Datenintermediäre und Data Governance Act' [2022] NJW 1905, at 1910.

12 Schweitzer and others (n 4).

13 Metzger and Schweitzer (n 8).

14 For an overview of the policy debate on data access in the U.S. see Schweitzer and others (n 4) 52 ff.

15 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

16 Schweitzer and others (n 4) 91 ff.

17 See, for example, Mariana Mazzucato, Rainer Kattel and Josh Tyan-Collins, 'Challenge-Driven Innovation Policy: Towards a New Policy Toolkit' (2020) 20 Journal of Industry, Competition and Trade 421 ff.

18 Other uses of the data are feasible as well. For example, a third party may want to create bundles of individual-level data and sell them or use them for the training of algorithms.

19 While the term is taken from the GDPR (see art 4(1) GDPR), its use in this paper is not limited to personal data, but extends to non-personal data.

refer to a one-off transfer of a specified dataset. Data portability can also be continuous and real-time, however (see, e.g. Art. 6(9) and 6(10) DMA). Furthermore, the term 'data portability' leaves open whether an effective *transfer* of data is required, or whether a mere *in situ* access may also suffice. Despite the fuzziness of the term, we will use it to describe the totality of access scenarios that fall under scenario 1. This implies that the concept of data portability as we use it here can also encompass an obligation to grant continuous and real-time access.

A right to data portability may follow from a legislature's decision to grant a defined group of natural or legal persons a right to access and use the relevant data – a right that is independent of a data holder's position of power or the requesting party's position of dependency. For personal data within the meaning of Art. 4(1) GDPR, Art. 20 GDPR endows data subjects with such a right. While Art. 20 GDPR was meant to facilitate the data subjects' possibility to switch providers, it does not include a right to full and real-time porting or to data-interoperability.[20] In sum, Art. 20 GDPR has not been effective in meeting its goal.[21]

Outside the realm of the GDPR, firms or persons who have, by their activity, participated in the generation of the relevant data could, in principle, be granted some sort of access or portability right. However, so far, the existing legal order has not generally recognized such a legal entitlement. As it stands, the law rather respects the *de facto* allocation of control of such data as well as the contractual agreement struck between the parties that contribute to the generation of data as the legal starting point.

Sometimes, competition law will require a correction of this allocation and mandate data access (1.). For some sectors, sector-specific legislation reaches beyond competition law and mandates data portability irrespective of whether the data holder holds a position of market power (2.). Alongside these regimes, the DMA now imposes specific obligations on designated gatekeepers to enable the portability of the data generated by the use of online services, both to the benefit of end users and of business users (see Art. 6(9) and (10) DMA) (3.). The Draft Data Act proposes a break with this pointillistic approach by establishing a 'horizontal' right to portability of product usage data for the product users and, derivatively, third parties. While this approach deserves support in principle, the legal nature of this right remains dubious (4.).

1. Data portability under Art. 102 TFEU

a) Starting points

In the absence of transaction costs, bargaining will lead to an efficient allocation of property irrespective of its initial allocation ('Coase theorem'[22]). As regards data as a non-rival resource, shared rights of access and use may frequently be expected to be an efficient outcome. Transaction costs and other market imperfections are ubiquitous, however. Uncertainty regarding the business opportunities associated with data and the risks related to data sharing, as well as legal uncertainty regarding the interpretation of the GDPR, can contribute to a reluctance to share.[23] In the face of such reluctance, the original allocation of rights of access and control – or, in the absence of rights, the allocation of de facto control – may come to determine the direction of data-driven innovation and the structure and evolution of data-driven markets and ecosystems.

Where – as has frequently[24] been the case in the past – the de facto control of services of machine usage data lies with the service provider or the manufacturer or seller of a product or machine, and where these data are relevant for the personalization of the product or service or for the possibility to provide complementary or aftermarket services, the data holder will be able to decide whether to design an 'open' or a 'closed' system: it can enable product and service users to have access to 'their' usage data, or it can deny such access. Where the primary market is competitive, and in the absence of a durable lock-in, both systems may come with advantages and disadvantages, and potential customers can choose according to their preferences. Where the law would provide service or product users with a right to data access, manufacturers, sellers or service providers could still try to bargain for a right to an exclusive use of the data – e.g. in order to be able to engage in long-term investments that may benefit both sides. In the absence of transaction costs, information asymmetries and asymmetries of bargaining power, the contracting parties should be expected to agree on the same, most efficient allocation of data access rights under both models (see above). In the presence of transaction costs and information asymmetries, the degree of 'openness' of data-driven systems is likely to be affected by the legislature's decision to grant or to deny product and service users a right to data portability, however.

Competition law will protect the process of competition as it develops based on any given allocation of rights. In data-driven markets, the exclusive control of usage data may hamper the ability of consumers to switch, and a denial of access may be a powerful instrument to foreclose competition. Where such usage data are competitively relevant across markets, an exclusive control may enable the data holder to leverage a dominant position to novel markets. In other words: the exclusive control of usage data may contribute to the finding of dominance, and the insistence on exclusivity may amount to an abuse under Art. 102 TFEU. While abuses of dominance may occur irrespective of the initial allocation of access rights, the risk of dominance-induced dysfunctionalities in the market is more pronounced where the legal regime initially respects the position of de facto control of the original

20 Paul De Hert and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 CLSR 193, 200 ff; Heike Schweitzer, 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung' [2019] GRUR 569, 574.

21 See Oscar Borgogno and Guiseppe Colangelo, 'Data Sharing and Interoperability Through APIs: Insights from European Regulatory Strategy' (2018) European Union Law Working Papers No 38, 14 ff <https://ssrn.com/abstract=3288460> accessed 4 November 2022; Moritz Hennemann, 'Datenportabilität' [2017] PinG 5.

22 Ronald H Coase, 'The Problem of Social Cost' (1960) 3 Journal of Law and Economics 1.

23 Schweitzer and others (n 4) 93.

24 While the de facto control of data by the service provider or product manufacturer is a frequent outcome – in particular where the service or product user is an end user or a small or medium enterprise – such an allocation is by no means a given. Where the product user is aware of the business opportunities associated with the data and business savvy, and where the market for the primary product is competitive, the parties may contractually agree to grant exclusive control of the usage data to the product user.

data holder and refrains from creating independent additional access rights in favor of the service or product user. In such a case, the threshold for finding a denial of access to constitute an abuse will generally be high, as evidenced by the 'essential facilities doctrine' (EFD) (see below, V.1.). By contrast, where the legislature endows the service or product user with general rights of data access, the request by a dominant undertaking to waive such a right alone may qualify as an abuse. In other words: The initial allocation of data access rights matters for the application of Art. 102 TFEU: The threshold for competition law to alter the initial allocation is high.

b) Relevant market and market dominance

Article 102 TFEU is applicable only to undertakings that are dominant on a relevant market. Where data markets exist,[25] a position of dominance may exist on a relevant market for data. However, many types of data which have become competitively relevant, in particular individual-level service and product usage data, have never been openly traded. Consequently, competition authorities have not yet found separate input markets for 'raw' machine sensor data in the IoT sector, for example, or for click-data of platform users on the internet.[26] Where a relevant input is not openly traded, demand for this input by third parties may sometimes suffice to presume the existence of a 'hypothetical' relevant upstream market for the purposes of Art. 102 TFEU. This is what parts of the case law on the EFD suggest.[27] However, according to this case law, this is only appropriate where access to the relevant input is absolutely indispensable to compete downstream. Settings in which access to specific types of data is indispensable to compete on a neighboring market may well exist, and the number of such settings may grow as the data economy continues to evolve. The evolution of the data economy is still at a relatively early stage, however. In many settings, the indispensability criterion, strictly interpreted, will not be met.

In such cases, the (possibly exclusive) control of certain types of data – typically data generated in the use of the product or service – may nonetheless be relevant when assessing a data holder's market power on the relevant product or services market, as it may amount to a barrier to entry.[28] The potential relevance of data for assessing the position of undertakings on a given market is broadly recognized in EU competition law.[29] Nonetheless, whether and how access to or control of data matters must be determined case by case. Exclusive control of data that constitute a competitively relevant and non-substitutable input into data-driven products or services will be particularly important: such control can immunize the data holder from competitive discipline on the relevant product or services market and may, therefore, allow him/her to behave monopolistically. But sometimes, certain types of data can be substituted by other types of data, e.g. access to inferred data may substitute for access to raw data. While none of the largest digital platforms and data holders – like Google, Facebook or Amazon – actively trade data, they all offer data analytics services.

A specificity of some types of data is their cross-market relevance: Control of these data may come with a possibility to influence competitive dynamics beyond the market(s) in which the undertaking is (already) dominant. The Art. 102 TFEU case law recognizes that – where markets are linked in specific ways – even conduct of an undertaking on a market that is distinct from the dominated market and which produces effects on that distinct market may fall under Art. 102 TFEU.[30] Control over data that are competitively relevant across market boundaries may be such a relevant link. For the largest digital platforms, this has now been implicitly recognized with the DMA (see below, III.3.).

Overall, EU competition law is flexible enough to capture the competitive relevance of data and consider various ways in which they may contribute to the creation or maintenance of a position of market dominance and/or its expansion to separate markets.[31] Nonetheless, the determination may come with difficulties in practice. For example, potential competitors and competition authorities may not know what data exactly an undertaking controls. Also, developing innovative uses of the data may presuppose a process of experimentation that potential competitors cannot engage in without prior access. In such a case, data-driven entrenchment may manifest itself in the fact that there are no (potential) competitors who request data access in the first place. Also, where data-driven markets are only emerging, the determination of potential substitutes for a given dataset may be an uncertain exercise. It follows what has already been observed above (1.a)): The original position of exclusive *de facto* control of data may of itself be the seed of a position of market power which competition law may not be able to capture effectively.

c) Refusals to allow for the porting of data that was generated by the use of a product or service – abuse of dominance?

It may also be difficult to establish that refusals by a data holder with exclusive *de facto* control of relevant service or product usage data to grant access to individual-level usage data to the service or product user or to a third party commissioned by the user constitute an abuse of dominance.

25 For markets for data see Cristian Santesteban and Shayne Longpre, 'How Big Data Confers Market Power to Big Tech: Leveraging the Perspective of Data Science' (2020) 65(3) Antitrust Bull. 459, 481-83. See also Inge Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 World Competition 473; European Commission, 'Support study accompanying the evaluation of the Commission Notice on the definition of relevant market for the purposes of Community competition law' (2021) Final Report 90 ff.

26 For a review of relevant cases and discussion see ibid 90 ff.

27 See, in particular Case T-184/01 *IMS Health II* ECLI:EU:T:2001:259 and Case C-418/01 *IMS Health* ECLI:EU:C:2004:257; see also Josef Drexl, 'Intellectual Property and Antitrust Law: IMS Health and Trinko – Antitrust Placebo for Consumers Instead of Sound Economics in Refusal-to-Deal Cases' (2004) 35 IIC 788; Inge Graef, 'Data as Essential Facility: Competition and Innovation on Online Platforms' (PhD thesis, University of Leuven 2016); Stefan A Schmidt, *Zugang zu Daten nach europäischem Kartellrecht* (Mohr Siebeck 2020) 211 ff.

28 See Bundeskartellamt and Autorité de la Concurrence, 'Competition Law and Data' (2016) Joint Report 11 ff.

29 See Case T-612/17 *Google Shopping* ECLI:EU:T:2021:763; *Google Android* (Case AT.40099) Commission Decision C(2018) 4761 final.

30 See Case C-333/94 P *Tetra Pak* ECLI:EU:C:1996:436, paras 27 ff.

31 See Bundeskartellamt and Autorité de la Concurrence (n 28) 11.

In the current market environment, 'closed' data models are frequently the dominant strategy for service providers or product manufacturers or sellers. The reasons for not sharing data are many and range from uncertainties about data protection requirements to concerns about trade secrets, difficulties in assessing the value of the data and an inclination to reserve future data-driven aftermarkets or complementary markets for oneself. Where all relevant market players opt for the same line of action, competitive pressure that would tend to force undertakings to offer a data portability option is absent. Furthermore, information asymmetries may become a source of market failure: Customers as well as potential competitors in evolving aftermarkets or complementary markets will frequently not know precisely what data are collected and available. Also, given the dynamics of the emerging data economy, consumers, but also businesses may not be able to adequately assess the risks that go along with a 'closed data' model at the time when they choose the product or service. This is true, in particular, where long-lasting products or services are chosen. An exclusive allocation of access rights to the provider of a service or machine which may have seemed innocuous at the time when the choice was made may result in a data-related lock-in over time.

Presuming a position of dominance of the data holder, it seems likely that the unilateral termination of a customer's previous possibility to port data, with the effect that third parties would be cut off from already existing possibilities to compete, would qualify as an abuse, in the absence of an objective justification.[32] A finding of an abuse will be more difficult where a user requests the introduction of a data portability option for the first time.[33] Within a relevant contractual relationship, a denial of data portability might be considered exploitative, but the conceptual benchmark for an exploitation may be difficult to establish where the absence of portability is the market standard.

An abuse may be found based on a 'hybrid' exploitative/exclusionary theory of harm along the lines of the Federal Supreme Court's *Facebook* doctrine:[34] A customer-unfriendly – and therefore potentially exploitative – product or service design that impedes access to individual-level data may be liable to foreclose competitors who need data access to challenge the dominant undertaking in its primary market or to offer complementary services. Such a theory of harm, while viable in principle and accepted under German competition law, would however reach beyond the established boundaries of abuse of dominance doctrine within EU competition law.

The difficulties in designing an effective data access remedy may give competition authorities and courts even more ground for caution in applying Art. 102 TFEU: The dominant enterprise may be required to introduce a completely novel interface, to change the way the relevant data are stored and organized and to create a possibility to port data. Decisions would need to be taken on whether data portability must be granted once only, at regular intervals or continuously and in real-time; on the data format; on the design of the interface for the data transfer; and on the precise (fair, reasonable and non-discriminatory, FRAND) conditions of the transfer, including on the question of a possible remuneration, etc. In order to work effectively, such a remedy may need tight regulation and oversight. Generally, competition law is reluctant to impose remedies that intervene so severely in the design of a product or service.

Overall, Art. 102 TFEU seems to be a difficult and relatively weak basis for introducing an effective data portability regime.

2. Regulatory solutions for data portability settings

It does not come as a surprise, therefore, that data portability regimes have rather emerged – or are being debated – outside the realm of competition law.

The most prominent example of a full-fledged sector-specific data portability regime is the revised Payment Services (PSD2) Directive,[35] which promotes the sharing of some types of payment transactional and account information: Articles 64 et seq. of the PSD2 Directive provide for a special access regime for 'payment initiation service providers' (Art. 66) and 'account information service providers' (Art. 67) to payment accounts of account servicing providers such as banks via APIs, provided that the account holder explicitly requests such access.[36] The goal is, *inter alia*, to open up the financial sector for more competition and innovation in complementary services provided by Fintechs (cf. Recitals 3 et seq.).[37] The European Banking Authority will define common and open standards to be implemented by all account servicing payment service providers (Recital 93).[38] In the energy sector, customers are to be granted access to data on the electricity they feed into the grid and on their electricity consumption 'through a standardized communication interface or through remote access, or through a third party acting on their behalf, in an easily understandable format allowing them to compare offers on a like-for-like basis' (see Art. 20(e) of the EU Electricity Directive 2019/944,[39] which is tailored to facilitate switching of electricity suppliers). Data access for complementary services (smart home devices or other consumer energy management systems) can be obtained through Art. 23(2) of Directive 2019/944.[40] While Art. 23

32 See Case 27/76 *United Brands v. Commission* ECLI:EU:C:1978:22, paras 184 and 194.

33 Schweitzer and Welker (n 7) 103 ff.

34 Federal Supreme Court, 23 June2020, KVR 69/19 –*Facebook*. On this case see Heike Schweitzer, 'Missbrauch von Marktmacht durch Datenzugriff: Kartellrechtliche Vorgaben für den Umgang digitaler Plattformen mit Nutzerdaten' [2022] JZ 16.

35 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 L337/35.

36 For an attempt to conceptualize this right to data access see Schweitzer and Welker (n 7) 122-25.

37 ibid.

38 For a fuller discussion see Sebastian Omlor, 'Der Zugang zum Zahlungskonto nach deutschem und europäischem Zahlungsdienste- und Wettbewerbsrecht' [2021] ZEuP 821.

39 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.

40 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'.

does not clearly state that data access is to be provided via real-time or near real-time APIs, Art. 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'. The European Commission shall specify interoperability requirements and procedures to ensure an effective implementation of this right to data access (see Art. 24(2) of Directive 2019/944).

With regard to access to, and the portability of in-car data, a broad discussion on the most appropriate data access and governance regime has emerged. The European Commission is currently consulting whether – in addition to the Draft Data Act – a special legal regime for access to vehicle data, functions and resources is needed.[41] In the agricultural sector, agricultural data are predominantly collected by the farms, but it is private third-party software that is used to process these data. The data are typically stored in locked datasets controlled by the producer of the land machine or technical component. Farmers have called for more control of the data that they generate as well as avenues to tackle information asymmetries and power imbalances that exist with the digital service providers.[42] There are also concerns regarding problematic clauses for farmers in contracts with their service providers that stipulate that they cannot share their agricultural data across a variety of suppliers. This has led farmers to request a right to data portability to avoid lock-in. In addition, farmers call for a right to access the data and software needed to repair their own machinery ('right to repair') – rather than being contractually obliged to use licensed service stations (who may charge high prices and not be readily available in remote areas), as is currently often the case.[43] On the other hand, there are concerns that if the agricultural data are not correctly shared, it could result, *inter alia*, in commodity speculation and market manipulations.[44] The EU's Code of conduct on agricultural data sharing by contractual agreement[45] proposes to tackle several of these issues in a non-binding manner, e.g. by clarifying roles and who should normally have control of which data or in providing a framework for data portability.

It is a shared characteristic of these (potential) regulatory regimes that rights of users to port individual-level data they have (co-)generated by their activity are granted irrespective of whether the data holder is dominant or not. Data-driven lock-ins and barriers to entry may occur even in product or services markets that are, in principle, competitive. Also, these regimes tend to come with their own portability infrastructure.

3. Portability obligations for gatekeepers – Arts. 6(9) and (10) DMA

The largest amounts of behavioral usage data are currently produced in the interaction with online service providers, and the largest troves of such data are accumulated by the biggest digital platforms. Generally, no regulatory data portability rights have emerged so far for the data generated by the end users' use of online services beyond Art. 20 GDPR and some sector-specific regimes. The DMA is the notable exception: In the future, designated gatekeepers within the meaning of Art. 3 DMA will have to grant end users a right to port the data provided or generated through their activity in the context of the relevant core platform service (Art. 6(9) DMA),[46] and business users will enjoy a comparable right to access and use data provided or generated by them or their end users (Art. 6(10) DMA).[47] These data portability obligations reach beyond Art. 102 TFEU in that they are imposed upon designated gatekeepers irrespective of a prior finding of an abuse of dominance. But contrary to what the Draft Data Act proposes with a view to data generated by the use of products – namely the creation of data portability rights irrespective of market power (see Art. 4(1) and Art. 5(1) Draft Data Act) – the DMA only applies to data generated in the use of 'core platform services' (Art. 2(2) DMA) by gatekeepers, i.e. to undertakings with a particular market position.

4. Transparency obligations for online intermediation services – Art. 9 P2B Regulation

The DMA is not the first legislative instrument to address the specific role of online platforms in the digital economy. Already in 2019, the Juncker Commission and the European Parliament proposed and finally adopted Regulation 2019/1150 on 'promoting fairness and transparency for business users of online intermediation services' (P2B Regulation).[48] Article 9 P2B Regulation

41 See the European Commission's Call for Evidence for an Impact Assessment regarding Access to Vehicle Data, Functions, and Resources, 29 March 2022, Ref. Ares(2022)2302201. For the debate on access to in-car data see: Bertin Martens and Frank Müller-Langer, 'Access to Digital Car Data and competition in Aftermarket maintenance Service' (2020) 16 J. Compet. Law Econ. 116. See also Wolfgang Kerber, 'Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data' (2018) 9 JIPITEC 310; Wolfgang Kerber and Daniel Gill, 'Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations' (2022) <https://ssrn.com/abstract=4174028> accessed 4 November 2022.

42 Marie-Agnes Jouanjean and others, 'Issues around data governance in the digital transformation of agriculture: the Farmers' Perspective' (2020) OECD Food, Agriculture and Fisheries Papers No 146, 7.

43 ibid 7 ff.

44 ibid.

45 <https://cema-agri.org/images/publications/brochures/EU_Code_of_conduct_on_agricultural_data_sharing_by_contractual_agreement_2020_ENGLISH.pdf> accessed 4 July 2022.

46 According to art 6(9) DMA, designated gatekeepers will be obliged to offer effective data portability – continuous, real-time and free of charge – to end users and third parties authorized by them. This obligation shall make sure that gatekeepers do not restrict the switching or multi-homing of end users and thereby undermine the contestability of core platform services and restrict the innovation potential of digital services (Recital 59).

47 According to art 6(10) DMA, designated gatekeepers will be obliged to grant business users, as well as third parties authorized by them, access to the data provided by them or generated in the context of their business services on the platform – again continuous, real-time and free of charge. Access and use must be granted to aggregated and non-aggregated data. Where the data includes personal data, in particular of end users who engage with the products and services offered by the business user, access and use of the data presuppose the consent of the end user. But the gatekeeper must enable business users to obtain such consent (Recital 60).

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

– the Regulation's central rule on data access – applies to 'online intermediation services', a category of platforms which overlaps to a certain extent with the definition of 'gatekeepers' under the DMA. According to Art. 2(2) P2B Regulation, 'online intermediation services' are characterized by their role as a trading platform for business users which offer goods or services to consumers on the platform. These services may qualify as 'gatekeepers' under the DMA if they reach the threshold of impact and size as set out in Art. 3 DMA. In this case, the rules of the DMA and the P2B Regulation apply cumulatively.[49] Smaller services are subject to the rules of the P2B Regulation only.

Article 9 P2B Regulation does not oblige online intermediation services to grant access to individual-level data which business users or consumers provide for the use of the platform or which are generated by the use of the platform services. Instead, it merely sets out transparency requirements. However, these transparency requirements are far-reaching. Under Art. 9(1), platforms must provide in 'their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both,' which business users or consumers provide for the use of the online intermediation services or which are generated through the provision of those services. Article 9(2) further specifies that the platform must inform the business user about the data collected (a), the access to such data by (other) business users (b), the access to aggregated data by (other) business users (c), and the transfer of data to third parties (d). It is obvious that such information may be highly relevant to business users. It may include ratings, reviews and other data related to the customers and transactions of the business users and may provide valuable insights for the further development of their services.[50]

When the P2B Regulation was passed, academics criticized it for establishing a transparency requirement only instead of a right of access to individual-level data.[51] Since then, the DMA has partly closed that gap: gatekeepers are now bound by an obligation to ensure the portability of individual-level data (see above, III.3.). For smaller online intermediation services, the P2B Regulation – contrary to the Draft Data Act (see below, III.5.) – seems to follow a 'market failure' approach: It addresses the information asymmetry that may exist between a platform provider and a business user irrespective of market power. Without Art. 9 P2B Regulation, only the platform provider would know which data regarding business users and their customers are being collected and who is being granted access to such data. And without Art. 7(3)(a), it would be impossible for the users of online intermediation services to identify any discrimination between business users regarding access to those data. Articles 9 and 7 do not foresee a right of access to data, or to equal treatment in this regard. But the transparency requirement should enable business users to take informed decisions when choosing between different online intermediation services. De facto, an informed choice will, however, be restricted to market settings where different platform providers offer different data access regimes.[52] The P2B Regulation refrains from adopting a further-reaching 'market-shaping approach'.

5. Data portability under the Draft Data Act[53]

Compared to the DMA, the Draft Data Act proposes to regulate data access of the scenario 1-type on a much broader scale: According to this legislative proposal, data 'co-generators' shall be endowed with rights of access to the data generated by their use of a product irrespective of whether the data holder holds a 'gatekeeper' position. Simultaneously, this new legislative model is limited to data generated by the use of products – whereas the DMA applies to data generated by the use of a gatekeeper's online services.

The Draft Data Act's new data access rights are set out in Arts. 4 and 5. According to Art. 4(1), data holders shall be obliged to grant product users – whether consumers or businesses – access to the 'data generated by the use of the product or related service'. According to Art. 5(1), the data holder must, upon request by the product user, also share with third parties acting on behalf of the user. However, the right of access of these third parties is a 'derived' right only: They may process the data 'only for the purposes and under the conditions agreed with the user' (Art. 6(1)). Nonetheless, much of the Draft Data Act is concerned with framing the relationship between the data holder and third-party data recipients: In practice, they will frequently deal with the data holders directly.

The access rights are complemented by additional obligations that shall ensure their practical effectiveness, including an obligation of the IoT product manufacturers to design and produce these products with a view to ensuring the easy and secure accessibility of data (see Art. 3(1))[54] and an obligation to provide information before the conclusion of a contract for the purchase, rent or lease of a product or a related service (including virtual assistant services – see Art. 7(2)), on the nature and volume of the data likely to be generated from the use of the product or related service, how the user may access these data etc., Art. 3(2). Indeed, the duty to provide information is of major importance for the effectiveness of the envisaged right to access, port and use co-generated

49 Recital 12 DMA.

50 Recital 33 P2B Regulation.

51 See Christoph Busch, 'Mehr Fairness und Transparenz in der Plattformökonomie? Die neue P2B-Verordnung im Überblick' [2019] GRUR 788, 794-95; Silvia Martinelli, 'The vulnerable business user: the asymmetric relationship between the business user and the platform' [2020] EJPLT 82, 90-91.

52 This is not necessarily so, however: In tightly oligopolistic markets in particular, the non-sharing of data may be a dominant strategy adopted by all platforms alike.

53 For a more elaborate discussion of the Draft Data Act see Metzger and Schweitzer (n 8). The following section is largely based on that analysis.

54 See Metzger and Schweitzer (n 8). See also Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Research Paper No 22-05, 73-74 <https://ssrn.com/abstract=4136484> accessed 4 July 2022.

data. The fact that product users will typically not know what data are collected by the manufacturer or other data holder may be one of the reasons why data access requests have remained relatively rare so far (see further below, V.1.d)).

Articles 8-10 set out a special legal regime that specifies the conditions under which the data are to be made available (FRAND), limits the compensation the data holder may request, mandates the availability of a dispute settlement regime and provides for rights of the data holder to apply appropriate technical protection measures when sharing the data.

The aim of the Draft Data Act is to ensure that users of a product or related service have access to the data they 'co-generate' by the use of the product or service. The creation of such an access right shall help avoid data-based 'lock-ins' and promote aftermarket innovation; it shall prevent 'the exploitation of contractual imbalances that hinder fair data access and use for micro, small or medium-sized enterprises' and thereby 'ensure a fairer allocation of value in the data economy'.[55] Furthermore, it shall enhance the 'interoperability of data and data sharing mechanisms and services', and 'facilitate switching between data processing services'.[56] Overall, it shall promote data access with a view to 'unlocking the value of data in Europe' and enhance opportunities of innovation.[57]

The rights of data access to be created by a future Data Act are rights to individual-level data portability and use only; situations where a company requests access to bundled individual-level data or aggregate data are not covered. Moreover, they are completely independent of a data holder's position of dominance, or of a dependency of the product user on the data holder. Rather, the aim is to redesign the basic private law structure of rights allocations and to establish a general legal infrastructure of individual non-exclusive rights of data access and use in order to avoid the emergence of data access blockades from the start and thereby to facilitate the transformation towards a data economy.

The structure of this right of data access and use is novel, which is why its precise legal nature remains fuzzy. Clearly, the product user's right of access is not merely contractual: Under Art. 4, the data holder is obliged to grant access irrespective of the existence of a contract with the product user. At first glance, one might consider that the Draft Data Act implicitly recognizes some sort of primary exclusive (intellectual property) right of the data holder with regard to the data;[58] a right which is then curtailed by limitations – in particular rights of access in favor of the product user (and, derivatively, third parties) in order to prevent an inefficient underuse of the protected subject matter.[59] However, such an understanding would miss the fact that the Draft Data Act does not strive to endow the data holder with a *right* to exclusivity; rather, it simply recognizes the data holder's position of de facto control and then specifies that both the data holder and the product user have a right to use the data. In this perspective, it seems that the fact that both the 'original' data holder and the product user contribute to the generation of the data and that data are non-rival in their use has inspired the creation of some sort of a 'co-ownership' regime. The multiplication of rights to make independent use of the data and the prohibition on hindering or excluding each other prevents the emergence of monopoly positions regarding what may be an important input in innovation and a key factor for competition. The idea of a parallel endowment of the data holder and the product user with independent rights of use is then complemented by the general principle of 'fair dealing' that shall govern the relationship between data holder and product user: Both parties may use these data independently, but with respect for the legitimate interests of the other.

In principle, the idea of establishing a novel legal infrastructure of access rights is promising. It may even be a necessary precondition for the evolution of competitive data-driven markets in the EU. However, in some important respects this concept is then fleshed out in a manner that risks jeopardizing the benefits for competition and innovation that the regime is meant to bring about (see below, IV.).

IV. Access to individual-level data – where should we go?

Of the two data access scenarios dealt with in this article, access to and the porting of individual-level data (scenario 1) is currently by far the most important. Article 102 TFEU has been – and will arguably continue to be – a relatively weak basis for enabling data access in such settings. In recognition of the relevance of this data access scenario and the need to intervene, the European legislature has, within the last couple of years, come a long way towards regulating access in sector-specific settings. For data generated by the use of a product, the Draft Data Act now proposes a horizontal approach to data access. It rightly presumes that, for the IoT, characterized by the establishment of digital ecosystems with converging market boundaries, a sector-specific approach would become impracticable (while recognizing that the Draft Data Act's regime may be complemented by sector-specific regimes that specify the precise conditions of access and use for particular industries).

However, if the goal is to establish competitive and innovative data-driven markets, the Draft Data Act still falls short in some important respects, namely with regard to ensuring a right of independent use for both the data holder and the product user (1.), including freedom to compete on all relevant markets (2.), with regard to ensuring freedom of contract with a view to data access rights (3.), and with regard to finding a way to integrate gatekeepers within the meaning of Art. 3 DMA into the competitive landscape (4.). Finally, one may ask whether the basic idea underlying the Draft Data Act should not be expanded to service-related usage data (5.).

55 Draft Data Act, Explanatory Memorandum, 15.

56 Recital 5.

57 Draft Data Act, Explanatory Memorandum, 1.

58 See Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022) 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436> accessed 4 June 2022.

59 See Wolfgang Kerber, 'Specifying and Assigning "Bundles of Rights" on Data An Economic Perspective' in Franz Hofmann, Benjamin Raue and Herbert Zech (eds), *Eigentum in der digitalen Gesellschaft* (Mohr Siebeck 2022) 151, 162.

1. Rights of independent use of data

Commentators have observed that the way the Draft Data Act has construed the product user's access right amounts to an implicit recognition of a de facto position of 'ownership' by the data holder, at least from an economic perspective.[60] Where the requirements of the access rights of Arts. 4 and 5 are not met, the data holder remains free to technically exclude others from accessing machine-generated data. Article 11 Draft Data Act even recognizes explicitly that the data holder may use technical protection measures. All in all, while the data holder has not been granted a full-fledged legal property right, s/he does remain in a privileged position for all practical purposes.[61]

However, the Draft Data Act does strive to constrain the data holder's position of control, *inter alia* by imposing limitations on his or her use of the data: according to Art. 4(6), the data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the product user. If this were to be taken literally, every use of the covered data would depend on the product user's contractual consent. This would not only result in a hold-up position for product users regarding a data holder's data use. More broadly, the aim of the Draft Data Act – namely to enable independent innovation and competition in aftermarkets and complementary markets – would be severely compromised.

A competition-friendly approach would suggest otherwise: both co-generators, the data holder and the product user, should be granted an independent right to use the data without the approval of the other party.[62] The rights of use and their limits should be symmetrical: he data holder should not depend on the consent of the user to use co-generated data as long as the legitimate interests of the user are not concerned. Inversely, the product user, having requested access to data, does not need to ask the data holder for consent with regard to the intended use of the data, as recognized by Art. 4(2). In the light of the competition rules on information exchange, this is essential: Given that usage data is a competitively relevant input, the product user as well as third parties must be able to compete and innovate without the data holder being informed of their business plans. Vice versa, the data holder should be able to do the same. The only constraint to be imposed on all parties concerned is a 'fair dealing' commitment: As 'co-owners' of the data, the data holder and the product user (as well as third parties) must respect the other parties' legitimate interests, including, for example, the protection of the data holder's trade secrets (Art. 4(3) Draft Data Act).

2. Independent use of data by product users and third parties: the inappropriateness of non-compete clauses

The ambiguity of the product users' right to access co-generated data, as currently provided for in the Draft Data Act, comes to the fore, in particular, in the 'non-compete' clauses set out in Arts. 4(4) and 6(2)(e) Draft Data Act. According to these provisions, neither the product user nor a third party acting on behalf of the user shall use the data 'to develop a product or related service that competes with the product or related service from which the data originate'. According to Recital 28, this limitation 'aims to avoid undermining the investment incentives for the type of product from which the data are obtained'. The Data Act shall stimulate innovation in aftermarkets and foster the development of entirely novel, innovative products and services. But it shall not promote the contestability of the data holder's position on the primary market.

The merits of this approach are controversial. Many commentators have argued that Arts. 4(4) and 6(2)(e) of the Draft Data Act are necessary to protect the legitimate interests of the data holder.[63] Competitors may compete on the primary product market, but they may not use the insights to be gained from a competitor's product usage data stream in doing so. If the primary product market were fully competitive, irrespective of access to the usage data stream, this would indeed be a plausible approach.

However, in an economy that is increasingly characterized by individualized products, competitors may need access to the usage data stream in order to compete in the primary market, namely to tailor their product to the needs of product users. However, such a use of the product usage data would seem to be prohibited under Arts. 4(4) and 6(2)(e) Draft Data Act. If this were the case, a product user would be prevented from using the data portability right to switch to a competing product provider. In contrast to data portability under Art. 20 GDPR, the Data Act would not protect product users from a data-driven lock-in. Also, the Draft Data Act's 'non-compete' clauses are in clear tension with the idea of a 'co-ownership' of machine usage data, combined with independent rights of use for both the data holder and the product user.

If the underlying assumption is that protecting the incentives of the data holder to equip its product with data collection technology requires a reservation of the primary market to the data holder, this should not be accepted as a given. Ideally, such investment will be driven by competition on the primary market and compensated for in the primary market. Where a period of exclusivity is needed to recover a given investment, an exclusivity of use can be bargained for (see below, IV.3.).

The 'non-compete' clause is all the more dangerous because its limits are difficult to discern: What will be required of a vertically integrated third party offering aftermarket services to show that it does not also benefit from the access to data for its competition on the

60 See Kerber (n 58) 1.

61 ibid.

62 But see Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022) Study for the European Parliament Committee on Legal Affairs (JURI) 93-94.

63 See, *inter alia*, Drexl and others (n 54) 87. See also Peter Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation and Competition Research Paper No 22-05, 20-21 <https://ssrn.com/abstract=4076842> accessed 4 November 2022. David Bomhard and Marieke Merkle, 'Der Entwurf eines EU Data Acts: Neue Spielregeln für die Data Economy' [2022] RDI 168, 172 point to some open questions but do not criticize the non-compete clause fundamentally.

primary product market? What will a product user need to show when it plans to enter the primary market? The rationality of the 'non-compete' clause is also questionable because it is not at all obvious that access to the stream of usage data would allow a product user or third party to 'reverse engineer' and thereby imitate the primary product.

3. The product user's right of data access: mandatory or default?

One of the challenges that a horizontal creation of a right to data portability has to grapple with is the multitude of settings which will be covered. The effects of a requirement of a 'co-use' of data may, however, be very different in different settings: Where the data holder is not active in the relevant aftermarkets or complementary markets, the value of such independent use may be high and the value of blocking such use will be low. In other settings, an investment in the primary market may only be attractive based on an exclusive use of data in special aftermarkets or complementary markets. If there is effective competition in the primary market and if, in addition, product users retain the possibility to switch from time to time, it is difficult to find a plausible reason why the data holder and the product user should be prevented from agreeing on an exclusive use of the product usage data by the data holder.[64] The position of the Draft Data Act on this point is not very clear. Recital 40 and Art. 12(2) seem to be based on the premise that the statutory allocation of the product user's access right is of a mandatory nature. However, this premise is not made explicit, and Art. 12(2), which declares any deviating contractual terms to be non-binding, formally only applies to Arts. 8-11 of the Act.

Also, despite the benefits of conceptualizing the Draft Data Act's access rights as default rules, the recognition of an unconstrained possibility for product users to waive their access rights may come with significant risks. In particular, if the product user is a consumer, issues of bounded rationality are certain to arise. But even in dealings with business users – and even in the absence of market power – the efficiency of such agreements may be tainted by problems of asymmetric information. Typically, the data holder will know more about the nature of the collected data and their possible uses. While this asymmetry is meant to be addressed by the information duty in Art. 3(2), the asymmetries are more profound and not fully offset by this provision. Frequently, neither party will be able to fully oversee the possible future uses of the collected data. Many companies with large collections of usage data continuously expand their 'data lakes' without full knowledge of what the exact use of these data will be like in the future. The product user will often be in an inferior position when accepting a waiver *pro futuro*.

Arguably, the Draft Data Act should therefore consider the product user's access right as a default rule in principle, but provide for safeguards in two respects: First, in the case of some sort of dependency of the product user on the data holder, and even more so if the data holder is dominant on the relevant product market, the product user's right to data access must become mandatory. Secondly, even where the primary market is competitive and the product user retains the possibility to switch, the Draft Data Act should establish a maximum duration for a waiver – e.g. two to three years. At the end of this period the product user should have a possibility to revoke the waiver.[65] The revocation would come with the possibility to access past usage data so as to be able to switch to a competing product without losing the benefit of data-driven personalization. Compared to a regime with mandatory rules of data access, this model would provide for more flexibility to develop business models based on an exclusive exploitation of the collected data.

4. Data access and gatekeepers

According to its Art. 5, the Draft Data Act requires the data holder to make available the co-generated usage data to a third party upon a user's request. However, designated gatekeepers under Art. 3 DMA shall be excluded as eligible third parties. What is more, such gatekeepers shall not solicit or commercially incentivize a product user to supply to one of its services data that the user has obtained under the Data Act's access right, or to agree to receive such data (Art. 5(2) Draft Data Act). For explanation, Recital 36 refers to the 'unrivalled ability' of gatekeepers to acquire data, such that access to product usage data would not be necessary to achieve the objectives of the Data Act – i.e. the goal of promoting competition and innovation in aftermarkets or complementary markets. An obligation to grant access to gatekeepers at the request of a user would 'thus be disproportionate in relation to data holders'. According to this logic, derived data access by gatekeepers would be an unjustified intrusion upon the legitimate interests of the data holder.

This construction is unconvincing, however: If the data holder and the product user have independent rights of use, and if the Data Act is to promote innovative uses of data on complementary or aftermarkets where the data holder may not even be present, a general presumption that a gatekeeper's access to data will intrude upon the legitimate interests of the data holder is implausible. Rather, the exclusion of gatekeepers from the access regime is a reaction to a concern that their access to data could enable them to engage in even more far-reaching envelopment strategies[66] by which they would leverage their positions of power from core platform service markets to complementary data-driven product or services markets. If this is the concern, their exclusion from the 'derived' data access regime appears to be underinclusive, however, considering that the data holder, for its part, remains free to grant gatekeepers access to data.[67]

64 See also: Leistner and Antoine (n 62) 79-80.

65 For a more detailed description of this idea see Metzger and Schweitzer (n 8).

66 Daniele Condorelli and Jorge Padilla, 'Harnessing Platform Envelopment in the Digital World' (2020) 16 J. Compet. Law Econ. 143.

67 This appears to be a deliberate choice – see Recital 36 of the Draft Data Act: The 'exclusion of designated gatekeepers from the scope of the access right under this regulation does not prevent these companies from obtaining data through other lawful means'.

Simultaneously, Art. 5(2) would not only amount to a far-reaching intrusion upon the gatekeeper's freedom to compete, but it would also severely restrict the rights of product users to freely choose how to make use of 'their' data. It may be significantly more pro-competitive and proportionate not to exclude gatekeepers from data access under Art. 5 Draft Data Act, but to grant access only based on the gatekeeper's commitment to open up its own data troves for sharing.

5. A horizontal and general data portability right also for service-related usage data?

Finally, given that – with some adaptations – the Draft Data Act's model promises to significantly promote data-driven innovation and competition in the field of the IoT, there is a question why this model should not also cover online service-related usage data. In this regard, users will only have a right to data portability vis-à-vis gatekeepers for the time being (see Art. 6(9) and (10) DMA and above, III.3.).

The European legislature's caution may be driven by the specificities of the data generated by the use of online services: First, these data will often qualify as 'personal data' within the meaning of Art. 4(1) GDPR – at least in their raw version. Article 20 GDPR endows data subjects with a right to data portability, i.e. a 'right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format', and the 'right to transmit those data to another controller without hindrance'. However, Art. 20 GDPR is generally considered to be ineffective in its current form (see above, I.).

Second, with regard to many types of behavioral data produced in the interaction with online service providers – e.g. with regard to location data – there will be substitutes. Widespread tracking practices have led to a multiplication of many types of behavioral data. So, sometimes, access to the individual-level data controlled by one specific data holder may be less important compared to access to product usage data.

Third, unlike the IoT sector, where consumers typically pay for the product and usage data come as a by-product, online service providers have frequently turned to business models that rely on the monetization of data, primarily in advertising markets. With its more restrictive approach to access to service usage data, the legislature may, for better or worse, want to protect this business model.

Whether these differences justify the difference in approach regarding access to the data generated by the use of products and services will need to be further discussed. One may argue that business models that focus on the monetization of data should not prevent the legislature creating a new private law infrastructure of data access rights. Such rights may function as a preventive mechanism that may prevent the development of data-related positions of market power. On the other hand, the creation of such access rights may come with significant problems for many SMEs in the online services sector. This may particularly be the case for access to real-time data as long as the technical processes and standards are not sufficiently developed to implement access protocols at low costs.

For the moment, it will be interesting to observe how the Data Act will affect the relevant markets once it has entered into force. Meanwhile, an immediate first step could be to establish transparency requirements along the line of Art. 9 P2B Regulation so that users of services could at least identify what data are collected or generated and to whom access to data is granted. An expansion of the access rules of the Data Act to services-related data should only be envisaged, as a second step, if those access rules have proven to achieve their purpose for the IoT markets. In addition, the legislature should, if the suggestions for broader access rules for ecosystem orchestrators and for data-driven markets (see below VI.1. and 2.) were taken up, consider applying such access rules to individual-level data.

V. Access to bundled individual-level and aggregated data – state of the law

With regard to access to *individual-level data*, a sound approach appears to be slowly emerging. Interestingly, it is an approach that does not grow from competition law principles but that has been developed outside its realm. When it comes to access to *bundled individual-level* and *aggregated data*, the situation is different. So far, there is almost no relevant legislation to cover this scenario. Competition law would generally seem to be appropriate to address data access problems of this kind – but a relevant body of case law has not yet emerged.

As a reminder: In this second data access scenario, an undertaking requests access to bundled individual-level data or to aggregated data from a data controller, firstly either because the sort of data analytics that are needed to provide a competitive complementary service to the service provided by the data holder – for example, predictions on the need for machine maintenance – depend on access to broader datasets. In this sub-scenario of scenario 2, data access is meant to enable effective competition on a complementary or aftermarket on which the data holder is, or is not, active. Or secondly, data access is requested because it is needed to compete on the primary market where the data holder is active. For example, the data-related advantages of the dominant search engine may be so strong that entry into this market is no longer possible because potential entrants do not have access to the relevant search, click and query data.

Again, we will start by looking at how a refusal to grant access in this scenario may be addressed under Art. 102 TFEU (1.). Secondly, we shall look at the DMA (2.).

1. Refusals to grant access to bundled individual-level or aggregated data under Art. 102 TFEU

a) General considerations

Much of the competition law debate on data access has focused on cases where a dominant undertaking refuses access to aggregated data that is necessary to compete

in an aftermarket or a complementary market. Access to *individual level* usage data pertaining to a particular user will not always suffice for a third-party competitor to enter the market and compete – whether on a complementary market or on the primary product or services market. Sometimes, a (potential) competitor may need access to large sets of *bundled* individual-level usage data for anonymous use[68] or to *aggregated* usage data[69] to provide complementary products or services that are competitive, or to enter the primary market. 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 would need access to aggregated in-car sensor data on the 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 larger number of car owners, machine users or a data intermediary, the complementary service provider would need to turn directly to the data holder for data access, i.e. the undertaking(s) active on the primary market.

In well-functioning markets with effective competition, access to bundled and aggregated datasets may be expected to result from market dynamics: An undertaking active in the primary market may decide to pool its product or service usage data and to offer access to providers of complementary or aftermarket services in order to make its primary product more attractive. Possibly, competitors active in the primary market might decide to pool product or service usage data – in particular where machine learning is of the essence for developing and improving a given service, such that a large pool of data is needed for the training of algorithms. Other competitors may develop a closed ecosystem, refusing to open their aggregated usage data to access by others. In justification, they may point to the benefits of a more controlled aftermarket environment, possibly with a higher degree of privacy and cybersecurity.[70]

However, the possibilities for market failures are manifold. In principle, they resemble those identified for the data portability scenario (scenario 1): Dominant data holders may be reluctant to grant access to 'their' data where that data may contribute to the entrenchment of their monopoly position on the primary market or allow them to enjoy competitive advantages when expanding into neighboring markets. Furthermore, information asymmetries between suppliers and their customers and bounded rationality may lead customers to accept 'data-closed' environments even where this may lead to a durable and costly 'lock-in'.

b) Access to bundled individual-level and/or aggregated data under the 'essential facilities doctrine'

The question of when a dominant undertaking's denial of access to data would – under EU or national competition law – constitute an abuse of dominance under Art. 102 TFEU continues to be debated.[71] A focus of this debate is on the question whether[72] and under which preconditions the EFD will apply, and whether it should be adjusted or refined when applied to data.[73] The applicability and interpretation of the indispensability criterion and the 'new product rule' are particularly controversial. As regards the indispensability criterion, data – like any other resource – can, in a given situation, be an input that is essential for competing effectively.[74] While there may be substitutes for many datasets,[75] some data are unique. The uniqueness can result from the uniqueness of the product or service that the dominant undertaking provides and to which the data pertain. This will typically be the case where the undertaking is a monopolist on the relevant product or services market. But as the IoT gains traction, the uniqueness of bundled individual-level or aggregated usage data may also result from

68 cf Crémer, de Montjoye and Schweitzer (n 7) 25-26: sets of anonymously used individual-level data are typically needed to extract (prediction) patterns from 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 number of subscribers to a video streaming platform, a neural network could be trained to make good movie recommendations based on the favorite movies of any given user.

69 Crémer, de Montjoye and Schweitzer (n 7) 26: '*aggregated data*, refers to more standardised data that has been irreversibly aggregated. This is the case for e.g. 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.'

70 On the comparison of the pros and cons of open vs closed systems see, *inter alia*, Carl Shapiro and Hal R Varian, *Information Rules: A Strategic Guide to the Network Economy* (Harvard Business Review Press 1998) 148; Autorité de la concurrence and CMA, 'The economics of open and closed systems' (16 December 2014) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/387718/The_economics_of_open_and_closed_systems.pdf> accessed 4 July 2022.

71 See, *inter alia*, Crémer, de Montjoye and Schweitzer (n 7) 98 ff; Heike Schweitzer and others, *Modernisierung der Missbrauchsaufsicht für marktbeherrschende Unternehmen* (Nomos 2018) 162 ff; Martin Schallbruch, Heike Schweitzer and Achim Wambach, 'Ein neuer Wettbewerbsrahmen für die Digitalwirtschaft' (2019) Bericht der Kommission Wettbewerbsrecht 4.0, 36-37; Inge Graef, Thomas Tombal 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, 13 ff <https://ssrn.com/abstract=3494212> accessed 4 November 2022.

72 Schmidt (n 27); Graef (n 27).

73 See, for example, Crémer, de Montjoye and Schweitzer (n 7) 98 ff; Graef (n 27); Graef, Tombal and de Streel (n 71) 14 ff; Inge Graef, 'Rethinking the Essential Facilities Doctrine for the EU Digital Economy' (2019) TILEC Discussion Paper No DP2019-028, 19-23 <https://ssrn.com/abstract=3371457> accessed 5 November 2022; Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) 8 JIPITEC 257, 280 ff; Schweitzer and others (n 71) 171; Richard Feasey and Alexandre de Streel, 'Data Sharing for Digital Markets Contestability' (2020) CERRE Report; Bertin Martens and others, 'Business-to-Business data sharing: An economic and legal analysis' (22 July 2020) 35 ff <https://joint-research-centre.ec.europa.eu/publications/business-business-data-sharing-economic-and-legal-analysis_en> accessed 23 January 2023; Schmidt (n 27).

74 Crémer, de Montjoye and Schweitzer (n 7) 101 ff. The German legislator has clarified the essential facilities doctrine in this regard. In the course of the 10th amendment to the Competition Act, s 19(2) No 4 was amended to specify that data can qualify as '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] NZKart 633, 634.

75 According to the Special Advisors' report, the substitutability of data may also depend on the type of data at issue: eg volunteered data will possibly be provided again, personal data could be retrieved under the framework of art 20 GDPR, or IoT data may be accessed in the future with the data access rights set forth in the Data Act. See Crémer, de Montjoye and Schweitzer (n 7) 101 ff. Especially in merger cases, the Commission has often argued that there are comparable datasets available on the market for purposes of eg targeted advertisement or for improving existing or developing new products.

the control of a primary product which generates the usage data. Even where the portability of individual-level data may, in the future, be ensured in such cases, e.g. under a future Data Act for product-related usage data, the producer or provider of the primary product may be the only undertaking with access to the bundled individual-level or aggregated data regarding the usage of that product – which may be needed to provide predictive maintenance services or to develop competitive complementary services.

The lack of substitutes for some types of datasets will not suffice for establishing the indispensability of access under the EFD, however. Generally, the preconditions for applying the EFD are strict.[76] Some unique datasets may be substitutable by others. 'Derived data' as offered by data analytics companies may sometimes be viable substitutes for 'raw data'. Assessing the substitutability of datasets may be a very difficult task.[77]

Given the non-rivalry of the use of data and the fact that many datasets are not protected by full-fledged property rights, but merely by trade secrets, some have proposed generally lowering the indispensability threshold for data access. According to this view, a dominant undertaking's interest in an exclusive data use may be less worthy of protection, and a refusal to grant access to data may, therefore, more easily qualify as an exclusionary abuse. This may be true, in particular, where access can be granted in a way that respects trade secrets.

However, while mandating access to data may improve competition on a downstream market in the short term, this improvement must be balanced against the negative incentive effects on the dominant undertaking that may result from a requirement to share. For example, the dominant undertaking may no longer be willing to invest in data collection in the first place.[78] 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. None of these arguments categorically exclude the applicability of the EFD. But the question whether any given dataset qualifies as an 'essential facility' in a given case must be analyzed with caution.

Another part of the debate relates to the applicability of the so-called 'new product rule' to access to data. In cases that concerned refusals by a dominant undertaking to license intellectual property rights, the CJEU has applied the EFD, but with an additional requirement that access must be granted only where access is indispensable to offer a new product.[79] However, the 'innovation threshold' to be applied has never been particularly clear and has been diluted over time. In *Microsoft*, the General Court merely required evidence that the refusal to grant access was capable of limiting technical development to the prejudice of consumers (Art. 102, second sentence, lit. a TFEU).[80] This should be the standard also in access-to-data cases – all the more since data are not generally protected by property rights.[81]

The intense academic debate on the role and scope of the EFD as applied to data has not been followed up by relevant cases. The access to data cases that have been decided on the basis of the EFD so far are old ones.[82] Cases relating to the new realities of the data economy are hard to find. To our knowledge, no case on Art. 102 TFEU access to data is currently pending before the European Commission.

c) Access to bundled individual level and/or aggregated data in data-driven networks and ecosystems: broader theories of abuse

While the EFD may provide an appropriate framework for dealing with some – but arguably a limited number of – data access requests, exclusionary abuses may also be identified on the basis of other theories of harm.[83]

In *Google Shopping*,[84] the General Court (GC) held that, while the case could be construed as one about equal access to Google's general search results pages, and hence as an EFD case, this did not preclude the possibility of looking at Google's conduct from a different angle and finding that the practice at issue met the preconditions of an independent form of abuse distinct from that of a refusal to supply.[85] Ultimately, the GC found the abuse to consist in an 'active behaviour in the form of positive acts of discrimination in the treatment of the results of Google's comparison shopping service, which are promoted within its general results pages, and the results of

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

77 Drexl (n 73) 281: 'since even the petitioner for access, such as a big data analyst, will often only have a vague understanding about the kind of data contained in the dataset and about which data will produce the most valuable new information based on observable correlations.'

78 For a need to precisely examine the incentive effects case by case, see Alexandre de Streel, 'Essential Facilities Doctrine in the data-driven economy,' presentation for FSR and FCP Annual Scientific Seminar in Florence on 22 March 2018 <https://www.slideshare.net/FSRCommunicationsand/essential-facilities-doctrine-in-the-datadriven-economy-alexandre-de-streel> accessed 4 July 2022.

79 See Joined Cases C-241/91 P and C-242/91 P *RTE and ITV v Commission ('Magill')* ECLI:EU:C:1995:98; Case T-184/01 *IMS Health II* ECLI:EU:T:2001:259; Case C-418/01 *IMS Health* ECLI:EU:C:2004:257 and Case T-201/04 *Microsoft* ECLI:EU:T:2007:289.

80 See Case T-201/04 *Microsoft* ECLI:EU:T:2007:289.

81 Against the application of a 'new product rule' see Crémer, de Montjoye and Schweitzer (n 7) 106 ff; see also Feasey and de Streel (n 73) 37, in favor of a 'consumer harm approach': it should be examined whether, for consumers, the negative consequences of refusing to share data outweigh the negative consequences of mandating data access under competition law. Similarly: Graef, Tombal and de Streel (n 71) 15 ff.

82 See, for example Joined Cases C-241/91 P and C-242/91 P *RTE and ITV v Commission ('Magill')* ECLI:EU:C:1995:98 on a refusal to provide access to lists of television programs that were protected by copyright under national law. See on these cases Josef Drexl, 'Designing Competitive Markets for Industrial Data: Between Propertisation and Access' (2017) 8 JIPITEC 257, at paras 123 ff.

83 For this see already: Crémer, de Montjoye and Schweitzer (n 7) 98 ff: the criteria are only proxies for the fundamental cost-benefit analysis underlying the antitrust case-law on the duty to deal, i.e. whether the positive effects of entry by an access seeker on competition, innovation, diversity and choice in the secondary market outweigh the reduced investment incentives of the data holders and of access seekers to collect data themselves. See also Graef, Tombal and de Streel (n 71) 16. See also Feasey and de Streel (n 73) 37 ff. Others have argued that the structured balancing of interests as developed by the CJEU in *Bronner* must be applied to access-to-data cases; see, for example, Schmidt (n 27) 381 with further references at footnote 138 at the same page.

84 Case T-612/17 *Google Shopping* ECLI:EU:T:2021:763.

85 ibid paras 220 ff.

competing comparison shipping services, which are prone to being demoted' (at para. 240), and which amounted to a 'leveraging from a dominant market characterised by high barriers to entry, namely the market for general search services' (at para. 237). In such a case, the relevant conduct may qualify as an abuse without the EFD's indispensability criterion being met. Furthermore, the GC emphasized that – where a platform has gained a dominant position based on a model of openness to all content providers and the promise to rank results based on their presumed relevance for search engine users, and where this promise is the source of the relevant network effects and economies of scale that now significantly reduce contestability – a change of that model, and the pro-active preferencing of their own content, could also vindicate the finding of an abuse.

While none of these considerations directly related to 'access to data' issues, *Google Shopping* does show that novel categories of abuse may need to be developed to adequately capture unilateral actions of an ecosystem orchestrator who is dominant on a relevant ecosystem market that come with a significant potential of foreclosure. While the precise preconditions of an abusive 'self-preferencing' as found in *Google Shopping* are not yet clear,[86] aspects that arguably mattered were (i) Google's degree of dominance ('super-dominance') on the search engine market;[87] and (ii) the fact that Google Search had obtained its position of dominance based on a model of openness and non-self-preferencing and had abandoned that model without a pro-competitive justification.

Another setting that may call for the development of special criteria for establishing an abuse of dominance relates to data access in digital ecosystems. The fact that the participants in an ecosystem actively contributed to its success, growth and increase in value may be relevant for an abuse analysis where the ecosystem orchestrator, once the ecosystem participants have become 'locked in', pockets an inappropriately large part of the value or uses its access to the ecosystem participants' contributions to restrict competition and further entrench or expand its own market position. Also, in data-driven ecosystems, access to data is one of the factors that may affect the ecosystem participants' ability to compete – a factor that will typically be controlled by the ecosystem orchestrator. In part, the ability to compete will be driven by the ability to access the data generated by the use of an ecosystem participant's own offer (data access scenario 1). But in some settings and respects, the ecosystem participants' competitive position may also be influenced by access to aggregated data, e.g. if an analysis of such data affects the ability to predict the need for aftermarket or complementary services or to innovate. In such settings, the EFD's indispensability requirement may be difficult to apply. At least at this stage of development of the data economy, access to a given dataset alone will frequently not be absolutely indispensable to compete. In a broader and more holistic perspective, it may nonetheless raise the barriers to entry and expansion so significantly that an exclusionary effect is likely to result. The combined effect of the exclusive access of a large and dominant ecosystem orchestrator to data generated in the context of the ecosystem, together with strong positive network effects, economies of scale etc. may be used to entrench established bottleneck positions for a long time and to reinforce the potential for anti-competitive platform envelopment strategies. For example, the exclusive access of a dominant ecosystem orchestrator to the aggregated data generated within the ecosystem will reserve a unique competitive position to that orchestrator for analyzing competitive developments, for predicting aftermarket demand, for offering data analytics on that basis and for engaging in machine learning as one of the most important all-purpose technologies of the future.[88] Along these lines, smart device manufacturers and consumer IoT service providers expressed competition concerns about the strong position of voice assistants at the center of data collection in the consumer IoT in the recent sector inquiry into the consumer IoT sector. They consider, *inter alia*, that the limits on the data they receive from leading voice assistant providers hinder them in their own business development.[89] Furthermore, privileged access to data allows voice assistant providers to more easily improve the quality of their services, thus raising barriers to new entrants on the voice assistant market and hindering the development of smaller competitors.[90]

Despite the increased relevance of access to data – including access to bundled individual-level and aggregated data – there are no relevant competition law cases pending at the EU level. A limited number of cases have been opened by national competition authorities. The German Federal Cartel Office's (Bundeskartellamt) *DB Mobility* case is an interesting example of when and how a refusal to grant access may amount to an abuse of dominance. On 20 April 2022, the Federal Cartel Office issued a statement of objection against the Deutsche Bahn (DB) with a view to a possible hindrance of mobility platforms – *inter alia*, by refusing to provide them with real-time train traffic data. Mobility platforms offer online solutions for integrated route planning across various means of transportation, including rail. For the quality and usefulness of such services, forecast data on passenger rail services – including, in particular, information on delays, cancellations or platform changes – are of the essence. The data are exclusively held by DB. DB refuses to provide such data to mobility platforms, however. Instead, DB – which offers a mobility platform itself, namely bahn.de and the app 'DB

86 For a critique of the concept see Pablo Ibánez Colomo, 'Self-Preferencing: Yet Another Epithet in Need of Limiting Principles' [2020] World Competition 417 ff; Patrice Bougette, Axel Gautier and Frédéric Marty, 'Business Models and Incentives: For an Effects-Based Approach of Self-Preferencing?' [2022] JECLAP 136 ff; Elias Deutscher, '*Google Shopping* and the Quest for A Legal Test For Self-Preferencing Under Article 102 TFEU' [2021] European Papers 1345 ff.

87 Case T-612/17 *Google Shopping* ECLI:EU:T:2021:763, paras 182, 183.

88 See also Wolfgang Kerber and Jonas Frank, 'Data Governance Regimes in the Digital Economy: The Example of Connected Cars' (2017) <https://ssrn.com/abstract=3064794> accessed 4 July 2022.

89 European Commission, 'Final report – sector inquiry into consumer Internet of Things' COM(2022) 19 final, para 42.

90 ibid para 44. See also European Commission, 'Preliminary Report – Sector inquiry into consumer internet of things' SWD(2021) 144 final, paras 418 ff.

Navigator' – reserves these data to itself. In addition, some selected mobility service providers such as Google receive preferential treatment. The proceedings against DB are based both on Art. 102 TFEU and on Secs. 19 and 20 Competition Act. The Federal Cartel Office has not yet specified the precise category of abuse on which the case will be based. The facts which have been made public suggest that this will not be an EFD case, however. Rather, there appears to be an element of discrimination between business partners – with a preferred treatment for Google.[91] Also, Sec 20(1a) Competition Act may play a role. Whether the Federal Cartel Office will try to base its case on an abusive self-preferencing is unclear.

Generally, the ECJ's recent preliminary ruling in *ENEL* may serve as a reminder that discriminatory refusals to grant access to data may fall under Art. 102 TFEU: According to this judgment, a dominant undertaking which uses resources, including data,[92] that are inaccessible to a hypothetical equally efficient but non-dominant competitor for the purpose of extending the position of dominance on another market may constitute an abuse of dominance.[93]

d) Possible reasons for the lack of cases

Overall, the dearth of cases and complaints regarding refusals to grant access to bundled individual level and aggregated data is striking. Arguably, it is not the constraints inherent in the case law on Art. 102 TFEU that are to be blamed. This is corroborated by the fact that significantly more far-reaching competition rules on data access at the national level – such as, in particular, Sec. 20(1a) Competition Act – have not produced any relevant case law, either.[94]

The reasons seem to lie elsewhere. A number of possible explanations come to mind. First, the data economy is still at an early stage. Many firms are struggling with making good use of the data that they themselves control. Experimenting with huge 'external' data troves may be beyond what they can and want to do at this stage. Also, requests for data access would presuppose a relatively well-defined idea of what to do with the data. Such projects may be lacking at this point of time, given that market actors have not yet been able to gather sufficient experience. Frequently, the whole purpose of data access would be to enable them to experiment – which may not be sufficient for requesting access to data under Art. 102 TFEU. Second, developing more specific projects of what could be done with bundled individual level or aggregate data may presuppose more precise information about the types of data that the dominant data holder controls. At this moment, data holders – even dominant ones – are not required to provide such information, with the notable exception of Art. 9(2)(c) P2B Regulation (for all online intermediation services providers).[95] Third, data holders will collect, structure and format data with a view to the business purposes they pursue. It may not be easy to make good use of the data for different purposes. The common comparison of 'raw' data with raw oil may be misleading in this regard. Fourth, at least when it comes to very large and diverse data troves of the kind that the large consumer-facing digital platforms control, potential competitors may lack the data processing capabilities, the skills and the specialized and experienced data science staff to put these resources to good use. Finally, the complexity, length and cost of competition law proceedings in an area where the law on abuse has not yet been clarified may be a disincentive to seek access to data on this basis.

For these and possibly other reasons, the focus on strengthening access to individual-level data (scenario 1) deserves support for the time being. Empowering undertakings to process data in these settings may allow them to learn and acquire the skills that are needed to later expand data-driven business models. If an active scenery of data intermediaries were to emerge, data markets might evolve that would allow for a market-driven access to bundled individual level and aggregated data.[96]

2. Access to bundled individual-level and aggregate data under the DMA

Interestingly, the current focus on scenario 1-type data access also extends to the access to online service usage data controlled by digital gatekeepers within the meaning of the DMA: The DMA almost exclusively addresses access to individual-level data (Art. 6(9) DMA and Art. 6(10) DMA[97]) – see further above, III.3.). Only one of the special obligations of gatekeepers as set out in the DMA extends beyond data portability: Article 6(11) DMA obliges online search engine providers with gatekeeper status to provide access to their ranking, query, click and view data to third-party competitors in the online search engines market. In this one area of activity the European legislator apparently presumes that access to data controlled by the gatekeeper for this 'core platform service' (Art. 2(2) DMA) is indispensable to compete effectively, and that a broad access-to-data mandate is needed to make this area of activity contestable (Recital 61).

91 The transparency requirement of art 9(2)(c) may pave the way for claims against discrimination based on competition law.

92 In *ENEL*, the resource at issue was commercial data on the company's client base acquired as a consequence of its former statutory monopoly.

93 See Case C-377/20 *ENEL* ECLI:EU:C:2022:379, para 91.

94 For a positive reception of this reform see, *inter alia*, Schmidt (n 27) 549 ff; Wolfgang Kerber, 'Datenzugangsansprüche im Referentenentwurf zur 10. GWB-Novelle aus ökonomischer Perspektive' [2020] WuW 249, 256: 'from an economic perspective overall well-designed' and Henri Weber, 'Datenzugang nach dem Referentenentwurf der 10. GWB-Novelle' [2020] WRP 559, 565 (important to foster innovation and competition and preferable to an ex ante regulation).

95 In the future, designated gatekeepers under art 3 DMA will be required to provide business users and third parties authorized by them with effective, high-quality, continuous and real-time access also to aggregated data that is generated in the context of the use of the relevant core platform service (see art 6(10) DMA) – but the right to access will be limited to aggregated data generated by the relevant business user or the end users engaging with its products and services.

96 For a discussion of the role and perspectives of data intermediaries see Schweitzer and others (n 4) 275 ff.

97 art 6(10) DMA also encompasses an obligation to grant access to aggregated data – but only to the aggregated data generated in the context of the use of the relevant core platform service by the business user requesting access or by end users engaging with the products or services offered by the relevant business user; art 6(10) DMA does not entail a broader right for third parties to access aggregated data controlled by the gatekeeper.

Apart from Arts. 6(9)-(11), the DMA focuses not on data access obligations, but rather restricts the gatekeepers' activities related to the processing of data: first, unless the end user has been presented with a specific choice and has provided valid consent in compliance with Arts. 4(11) and 7 of the GDPR, a gatekeeper must not process personal data from end users that result from the use of services of third parties for the purpose of providing advertising services; they must not combine personal data from the relevant core platform service with personal data from any other service – whether offered by themselves or by third parties; they must not cross-use personal data from the relevant core platform service in other services they offer separately – and vice versa; and they must not sign-in end users to other services of the gatekeeper in order to combine personal data (Art. 5(2) DMA). This provision reacts to concerns that all these practices tend to advantage gatekeepers in accumulating more data, thereby raising barriers to entry (Recital 36). Leaving end users a free choice between a 'data intense' version of the service and a less personalized, but otherwise equivalent alternative is thought to promote contestability.[98]

Second, a gatekeeper must refrain from using any data not publicly available that are generated or provided by business users in the context of the use of a relevant core platform service in competition with those business users (Art. 6(2) DMA).[99] Otherwise, gatekeepers with a dual role as platform providers and competitors on the platform could take advantage of the privileged access to data that they enjoy as platform providers when they compete with the businesses to which the data pertain (Recitals 46-48).[100]

In this regard, the DMA does react to concerns that data-based competitive advantages, including advantages that follow from the control of large troves of aggregated data and from the strong network effects and extreme economies of scale that come with this control, tend to lead to very high barriers to entry and undermine the contestability of the entrenched positions of gatekeepers in the provision of the relevant core platform services (Recitals 2 et seq., 32), and enable gatekeepers to leverage their position from one area of activity to another (Recital 3). But the answer is not to enable competitors to access those data on a broad scale, but rather to constrain gatekeepers in their own use of the data.

This approach appears to be rather defensive: Rights to port and use individual-level data, as provided for in Art. 6(9) and (10), may facilitate the switching and multi-homing of customers (Art. 6(9) DMA), and allow business users to compete more effectively on the platform and adjust their offers to consumer preferences more swiftly (Art. 6(10) DMA). But given that the gatekeepers' data advantages essentially result from the access to the whole bundle of data, neither of these provisions will enable undertakings to challenge the gatekeeper's position head-on. The gatekeepers' data-related advantages essentially remain uncontested by the DMA.

VI. Access to bundled individual-level and/or aggregated data – where should we go?

Arguably, there is some reason to consider whether a more aggressive approach in opening up the gatekeepers' data troves for decentralized innovation and competition may be justified. However, given that this data, in their original form, is predominantly personal data within the meaning of Art. 4(1) GDPR, a prerequisite for broader access to data obligations may be a legislative clarification of when such data are to be legally considered as anonymized. For the moment, this issue remains largely unresolved and constitutes one of the major hurdles for a further growth of the data economy. This is also true for a possible broadening of access to bundled individual-level and/or aggregated data outside the scope of the DMA.

Some discussion has emerged whether such a broadening of data access rights is desirable – either based on a more pro-active interpretation and enforcement of Art. 102 TFEU or based on a regulatory approach. Two different settings may be distinguished. The first relates to rights to access bundled individual-level and/or aggregated data within the framework of a digital ecosystem (1.). Academic commentators have mostly focused on special data-sharing obligations in data-driven markets (2.).

1. Special data access obligations for ecosystem orchestrators

With the DMA, recent debates have focused more and more on rules of conduct for digital ecosystems. While different types of ecosystems exist,[101] data will frequently play an important role in all of them: User and usage data may be cross-used in different segments of the ecosystem; they may connect core products with complementary services; and they may drive innovation within the ecosystem. The DMA reacts to these specificities, but its scope of application is limited to 'gatekeepers' within the meaning of Art. 3 DMA, i.e. the largest players only. A refusal of an ecosystem orchestrator to share data with the complementors active in the ecosystem may, however, raise competition concerns below the threshold of the DMA or in ecosystems not covered by Art. 2(2) DMA, e.g. in the case of business management software solutions like enterprise resource planning software (ERP).

98 It remains an open question whether the hopes that consumers, when presented with a free choice, will opt for the more data-sensitive alternatives will materialize.

99 art 6 No 2 DMA specifies that 'data that is not publicly available' shall include 'any aggregated and non-aggregated data generated by business users that can be inferred from, or collected through, the commercial activities of business users or their customers, including click, search, view and voice data …'.

100 Philipp Baschenhof, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?' [2021] Journal of Law, Technology and Policy 28 <https://ssrn.com/abstract=3970101> accessed 4 July 2022 raises the question whether this limitation on the use of data is limited to the use for activities that would place the gatekeeper in actual competition with the business user, or whether it would extend to uses that are in potential competition with a business user.

101 See, for example, Michael G Jacobides, Carmelo Cennamo and Annabelle Gawer, 'Towards a theory of ecosystems' (2018) 39 Strateg. Manag. J. 2255; Michael G Jacobides and Ioannis Lianos, 'Regulating platforms and ecosystems' (2021) 30 Ind. Corp. Change 1131; Michael G Jacobides and Ioannis Lianos, 'Ecosystems and competition law in theory and practice' (2021) 30 Ind. Corp. Change 1199.

In an open ecosystem, complementors contribute significantly to the overall value of the system. However, the more difficult it becomes for complementors to switch to another ecosystem or to multi-home, the more leeway the ecosystem orchestrator gains to only grant access to the large troves of data it controls selectively and on a discriminatory basis, thereby keeping important business opportunities to itself or reserving them for privileged business partners.

Given the fact that, in initially open ecosystems, the value of the system results from a collaborative effort, there may be reason to think about some sort of special allocation of data access rights – including rights of all ecosystem participants to access bundled and aggregated data – in principle similar to the approach chosen by the Draft Data Act, but not limited to individual-level data generated by each participant's individual contribution, but to the 'data commons' of the ecosystem as such. In practice this would amount to an obligation for the ecosystem orchestrator to establish a data pool with shared rights of access. Alternatively, such an approach can be developed on the basis of Art. 102 TFEU (see above, V.1.c)) – and would then be restricted to settings where a dominant position of the ecosystem orchestrator has been established.[102] In both cases, the sharing obligation would be limited to observed data: It should be part of the competition that emerges from the resulting data access to find out which insights can be inferred.[103] The practical effectiveness of Art. 102 TFEU in enforcing data access[104] might increase if guidelines were to clarify that data sharing within ecosystems may constitute a special category of cases, and to develop a more structured test for this setting. Within a competition law framework, relevant criteria would include, *inter alia*, the question whether the access petitioners can still switch ecosystem or multi-home; whether they contribute to the generation of the data, and to the value of the ecosystem; to what extent possibilities to compete and innovate within the ecosystem depend on data access; to what extent the data are an important connecting factor between different segments of the ecosystem; and whether the ecosystem orchestrator has changed course with regard to access to data once it has become dominant.

Data sharing principles within digital ecosystems may also include a rule that an ecosystem orchestrator who simultaneously competes within the ecosystem will only be allowed to combine data generated by its own services with data generated by the offers of other business users of the ecosystem if and to the extent that the ecosystem orchestrator ensures FRAND access to its own data troves for these other users, too.

2. Special rules on data sharing in data-driven markets?

The debate on special data access rules in digital ecosystems is only emerging. Prüfer et al. have presented a more refined proposal to create special data sharing obligations in what they call 'data-driven markets',[105] and to do so outside the realm of competition law,[106] namely by way of special regulation.[107] Markets are considered data-driven 'if a firm's marginal costs of innovation decrease with the amount of user information, that is, if it is subject to specific feedback effects ('data-driven' indirect network effects)'.[108] A three-pronged test is proposed to determine whether these conditions are met: (i) there must be a positive relationship between demand and user information; (ii) user information must be necessary to improve quality; and (iii) quality must create more demand.[109] Such markets may be particularly prone to a data-driven market tipping (monopolization) and thus to lower incentives to innovate for both the dominant firm and (potential) competitors.[110] Also, there is a risk that a dominant company can leverage its dominance to connected markets where the user information is also valuable, thus creating a 'domino effect'.[111] In order to address these risks to competition, a data sharing obligation shall be imposed along the following lines:[112]

- Firms active in a data-driven market should be obliged to share their user data if their market share exceeds 30%.
- These firms shall make 'their' user data available to 'every organization that is active in the respective industry or that can explain how it would serve users with the data'.
- Only user information shall be covered, i.e. 'raw data about users' choices or characteristics, which can be

102 For a proposal that goes into this direction see Feasey and de Streel (n 73) 55 ff.

103 Crémer, de Montjoye and Schweitzer (n 7) 101.

104 For doubts regarding the effectiveness see, *inter alia*, Philipp Marc Steinberg and Markus Wirtz, 'Der Referentenentwurf zur 10. GWB-Novelle (Teil 1)' [2019] WuW 606, 607 et seq.; Tobias Lettl, '10. GWB-Novelle – Problem des Datenzugangs gelöst?' [2020] WRP Editorial issue 2; Torsten Körber, '"Digitalisierung" der Missbrauchsaufsicht durch die 10. GWB-Novelle' [2020] MMR 290, 291 ff; Justus Herrlinger, 'Der geänderte § 20 GWB' [2021] WuW 325, 327 ff; Marc Schweda and Florian von Schreitter, 'Ran an die Datenschätze? Datenzugangsansprüche nach der 10. GWB-Novelle' [2021] WUW 145.

105 See Inge Graef and Jens Prüfer, 'Governance of data sharing: A law & economics proposal' (2021) 50 Research Policy 104330.

106 For a finding that data sharing obligations may follow from competition law where an exclusionary strategy can be established see Crémer, de Montjoye and Schweitzer (n 7) 105 ff; see, on the other hand, Jordi Casanova, 'Online Search Engine Competition with First-Mover Advantages, Potential Competition and a Competitive Fringe: Implications for Data Access Regulation and Antitrust' (2020) <https://ssrn.com/abstract=3647092> accessed 4 July 2022: 'We argue that when dominance is derived from first-mover advantages and innovation feedback loops, rather than high and non- transitory barriers to entry, competition policy and regulation should avoid undermining first-mover advantages through access regulation, as this is likely to result in trade-offs on innovation by all market players. We support instead a focus on prohibiting exclusionary behaviour by first movers to avoid leadership derived from anti-competitive foreclosing abuses rather than from competition on the merits.'

107 Graef and Prüfer (n 105) 4 ff.

108 Graef and Prüfer (n 105) 3. See also Cédric Argenton and Jens Prüfer, 'Search Engine competition with network externalities' (2012) 8 J. Compet. Law Econ. 73; Jens Prüfer and Christoph Schottmüller, 'Competing with Big Data' (2022) 69 J. Ind. Econ. 967.

109 Jens Prüfer, 'Competition Policy and Data Sharing on Data-driven Markets: Steps Towards Legal Implementation' (2020) Friedrich-Ebert-Stiftung 10 ff <http://library.fes.de/pdf-files/fes/15999.pdf> accessed 4 July 2022. See also Tobias Klein and others, 'A Simple Test for Data-Drivenness of Markets' (2021) Tilburg University mimeo. The search engine market has been presented as a paradigmatic example where all three conditions are met and a data sharing obligation should therefore be imposed; see Argenton and Prüfer (n 108).

110 Prüfer and Schottmüller (n 108).

111 Prüfer and Schottmüller (n 108).

112 Graef and Prüfer (n 105) 4 ff.

logged automatically'. In order to avoid interference with investment incentives, the sharing obligation would not extend to 'processed data', where the data holder has invested in data analytics.
- Gatekeepers under the DMA shall be disqualified from data access.
- The appropriate access price to user information should equal the marginal cost of obtaining the user information, which is considered to be '(roughly) zero'.
- For the implementation of the data sharing obligation, Graef and Prüfer have proposed a multi-level governance structure with national authorities and a European Data Sharing Agency (EDSA) yet to be established in charge.

A somewhat similar proposal has been presented by Krämer and Schnurr.[113] Like Graef and Prüfer, they want to address strong data-driven network effects[114] by way of an *ex ante* data sharing obligation[115] with a view to enabling niche entry and growth in data-driven markets.[116]

3. Need for legislative reform?

The question whether there is a need for a more pro-active legislative approach to promote access to bundled individual-level and/or aggregated data is still under debate. There is a broad consensus that more access, including to bundled individual-level/aggregated data, will be needed to foster innovation and competition, e.g. in AI-driven markets. In principle, Art. 102 TFEU is flexible enough to capture conduct that forecloses competition, including refusals to grant access to data or discriminatory data access policies. However, the hurdles to an effective enforcement are substantial. No clear test for establishing an abuse has yet emerged. Consequently, both the anti-competitive effect and a violation of the principles of 'competition on the merits' have to be established case by case. A high degree of legal uncertainty will likely persist for some time to come. Furthermore, the challenges for an effective enforcement extend to the remedial stage: Complex governance structures will be needed to ensure an effective implementation of data access remedies.

Complex governance structures and a potentially costly oversight regime will also be needed to implement a regulatory data access regime, however. Furthermore, data-driven markets are still at an early stage, and the puzzle of the low number of complaints by companies that might desire broader data access remains unresolved.

A significantly more elegant solution for organizing access to bundled individual-level and aggregated data would be a market-driven solution. The evolution of such an approach remains feasible. The further development of the market could be supported by transparency requirements following the model of Art. 9 P2B Regulation. A more effective alternative to individual contract solutions could arguably be based on data intermediaries[117] – who still need to find a viable business model, however. Such data intermediaries would acquire the right to market individual-level data and to transform them into marketable bundles. Companies seeking access to bundled or aggregated data would no longer need to turn to the 'original' data holder in that case, but could acquire relevant data bundles on a competitive market. For such data intermediaries to evolve, the Draft Data Act would arguably need to be more explicit about the possibilities for product users to monetize 'their' usage data, i.e. to empower third parties to use the data for marketing data access for money. So far, the Draft Data Act is silent on this possibility.

VII. Data access under the Draft Data Act, the DMA and competition law – a coherent framework in the making? A summary

In the light of the fundamental transformation towards a data economy, we continue to search for coherent legal principles to guide the recognition of rights of access to data. Slowly, the contours of a novel legal framework are emerging. So far, it focuses – arguably rightly so – on access to *individual-level data*. With a view to such data, the Draft Data Act proposes to create a novel category of non-contractual rights, namely rights of independent data access and use for those who have, by the use of a product, co-generated the data. These data access rights are granted irrespective of whether the data holder is dominant on any relevant market. With the Draft Data Act, data access is provided for within a private law framework, not within a competition law framework. It is not based on the finding of a market failure but strives to promote access to data more generally by redefining the 'original' allocation of rights in data.[118] In principle, this approach deserves support. The recognition of data access rights for data 'co-generators' helps to avoid the emergence of a monopolistic control of individual-level data in the first place and establishes a new benchmark for a 'competition on the merits' in a data-driven economy. However, the Draft Data Act should be refined in some important respects in order to reach a better fit with the goal of promoting competition and innovation (see above, IV.). Whether this approach to access to individual-level data for data co-generators should be extended to online service usage data remains an open question for the moment. As of now, rights to access individual-level online service usage data are explicitly foreseen only in Art. 6(9) and (10) DMA – i.e. vis-à-vis designated gatekeepers.

For third-party competitors who need access to bundled individual-level and aggregated data in order to innovate and compete (data access scenario 2), no generalized private law rights to access are emerging. Data

113 Jan Krämer and Daniel Schnurr, 'Big Data and digital markets contestability: Theory of harm and data access remedies' (2022) 18 J. Compet. Law Econ. 255.

114 For a data-driven theory of harm, three main arguments, comparable to Prüfer and Schottmüller (n 108), were raised: (i) 'in cases where data-driven network effects are strong, markets tend to monopolize (market tipping)'; (ii) 'this tipping effect does not stop in the very market where it started, but may spill over to related, data-intensive markets, which can already exist or may still emerge'; and (iii) 'this also has an effect on innovation, because high entry barriers stifle innovation activity in those areas and markets where entrants may set out to compete with the incumbent', Krämer and Schnurr (n 113) 258 ff.

115 For the shortcoming of competition law and the need to establish some kind of *ex ante* regulation see Krämer and Schnurr (n 113) 268 ff.

116 ibid 270 ff.

117 See, *inter alia*, Katja Seim and others, 'Market Design for Personal Data' (2022) Digital Regulation Project, Policy Discussion Paper No 6.

118 On this see Metzger and Schweitzer (n 8).

access scenario 2 remains the domain of competition law and, possibly, further-reaching power-dependent and context-specific regulation.

Although data-driven advantages are considered to be among the core hurdles for contesting digital gatekeepers and an important driver of platform envelopment strategies, the DMA remains cautious: Apart from a right for any third party undertaking providing online search engines to request access to ranking, query, click and view data generated by free and paid search on search engines subject to the DMA (Art. 6(11) DMA), no rights of access to bundled individual level or aggregated data are granted to third parties. Arguably, more far-reaching obligations to share anonymized data would have been justified. However, a legal specification of when datasets are to be considered anonymized would be a prerequisite for making such data access regimes work in smooth alignment with the GDPR.

Obligations to grant access to bundled individual-level or aggregated data may also be imposed based on Art. 102 TFEU. So far, the provision has not been activated for this purpose. The difficulties for an effective enforcement of data access rights on this basis are manyfold. They start with the need to establish dominance case by case, to determine, within a highly context-specific framework, whether the preconditions of an abuse of dominance are present, and finally to specify the data access conditions, including the data format, interfaces and possibly compensation. Given these hurdles, one may wonder whether Art. 102 TFEU will come to be a viable basis for third party access to bundled individual-level or aggregated data in the medium to long term, or whether it will rather serve to inspire the creation of regulatory regimes where such access is found to be needed to protect data-driven competition. While such regulatory regimes have already been proposed – in particular with a view to so-called 'data-driven markets', the European legislature has not been active in this regard so far. By contrast, the establishment of a coherent set of principles for access by participants in data-driven digital ecosystems to bundled individual level or aggregated data in settings where the ecosystem orchestrator is dominant seems a realistic option. These principles could take some inspiration from the principles established for the access to standards set by standard-setting organizations.

Both with a view to access to individual-level data by data co-generators (scenario 1) and with a view to access to bundled individual-level and aggregated data by third parties (scenario 2), a legal infrastructure will be needed to make such access effective. Article 9 P2B Regulation and Art. 3(2) of the Draft Data Act are indicative of a need to impose information duties on undertakings that are potentially subject to data sharing obligations, such that potential claimants can learn which data exist. The Data Act, once in force, may also promote the evolution of principles that help specify what FRAND access may mean in the context of data sharing – although the Draft Data Act itself is not very clear in this regard at the moment.[119]

Ideally, the evolution of a well-functioning legal framework for access to individual-level data by data co-generators (scenario 1) would promote the development of competitive markets for data – including for access to bundled individual-level and aggregated data. Data intermediaries may emerge and bundle and market the data. Such data monetization on behalf of data co-generators may also provide the latter with a larger share in the commercial value of 'their' data. So far, the European legislature's stance vis-à-vis such a more pro-active monetization of data has remained unclear. The commodification of data is, however, part of the logic of the data economy. It will be essential to make it work to the benefit of those who, by their activity, generate the data. The best way to ensure that consumers benefit will be to avoid monopolization.

119 Metzger and Schweitzer (n 8).