Connected devices – An unfair competition law approach to data access rights of users

Josef Drexl

A. Introduction

The digital economy is no longer limited to the business models of Internet platform operators, the use of personal computers and smartphones. Through embedded sensors, artificial intelligence and advanced mobile telecommunications technology, connected devices collect data, analyse them automatically, communicate with multiple other devices and act autonomously. Through the advent of these devices, digitisation penetrates many sectors of the physical economy. Connected devices significantly contribute to the explosion of data in the digital era and thereby support the European Commission's recent observation that 'data will reshape the way we produce, consume and live'.[1]

The economic and social implications of the advent of connected devices are manifold. They often mark disruptive innovation with the power of completely replacing the previous generations of products. They fundamentally transform existing business models and markets. Connected devices also change the role of users and consumers. We no longer only buy and use a physical product. We also become data providers who actively contribute to the generation of data, including personal data, while it is typically the device manufacturer who remains in control of these data.

Data collected and generated by connected devices may be of great utility for a large group of players. First of all, these data serve the very interest of the users, since they are needed to guarantee the well-functioning of the connected device, especially in terms of utility, safety and convenience. The well-functioning of the device may also require data sharing with other devices, such as in the case of automated and autonomous driving where vehicles have to communicate with traffic lights and signs as well as other vehicles, including those produced and operated by competing manufac-

1 Communication from the Commission of 19 February 2020 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – A European strategy for data, COM(2020) 66 final, 2.

turers. Beyond this, firms active in secondary markets also depend on data access. An example are independent providers of repair services of cars who are in need of access to the on-board data of these vehicles. Even the state may have a huge interest in access to especially aggregated data, such as anonymised health data collected through fitness trackers, mobile health devices and connected drugs, to pursue public interest goals.

In sum, this explains why there is general agreement that data sharing and access is of essence for the development of the digital economy.[2] This insight drives the debate on what kind of regulatory framework the digital economy needs. As regards the measures and approaches that ought to be taken, policymakers not least on the European level have progressed quite considerably in the past years. In 2017, in its Communication on 'Building a European Data Economy', which focused particularly on machine-generated data, the Commission still seemed prepared to consider a potential data producer's right for the owners or long-term users of connected devices for the purpose of enhancing the free flow of data.[3] Meanwhile, however, the perspective has changed. In its more recent Communication on the European Strategy for Data, the Commission announces the proposal of a Data Act, which is supposed to regulate the relationship between the different actors in the data economy.[4] This project seems to mark a final shift to data access legislation.[5] Indeed, the Commission states that the Act is intended to make 'access to data … compulsory, where appropriate under fair, transparent, reasonable, proportionate and/or non-discriminatory conditions'.[6] The focus on data access is also mirrored by the other new project of the Commission, a review of the existing intellectual property framework, including the Database Directive in particular,[7] with the objec-

2 See the early study of OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (OECD 2015), hinting at the importance of data access for promoting multiple public interest goals.

3 Communication from the European Commission of 10 January 2017 – Building a European Data Economy, COM(2017) 2 final, 13.

4 European Commission, 'A European strategy for data' (n. 1) 13.

5 Such policy shift has also been advocated by the author of this chapter. See, in particular, Josef Drexl, 'Data<Access and Control in the Era of Connected Devices – Study on behalf of the European Consumer Organisation BEUC' (BEUC 2018) <www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 31 August 2020. This chapter builds on, and further develops, the analysis of this study.

6 European Commission, 'A European strategy for data' (n. 1) 13.

7 Directive 96/9/EC of the European Parliament and of the Council of 11 March1996 on the legal protection of databases, [1996] OJ L77/20.

tive of enhancing data access and use.[8] This additional initiative shows that legal exclusivity regarding data is now considered a potential impediment to the free flow of data rather than a tool to promote data access.

Data access rights are not a completely new legal tool. They have especially been in use in sector-specific regulation for quite some time. There, data access rights are typically vested in competitors.[9] An obligation to provide data access to competitors may also result from competition law provided that the refusal to grant access constitutes an abuse of market dominance in the sense of Article 102 TFEU.[10] In the competition law context, the terminology of compulsory licensing is often used, especially where the refusal relates to the use of intellectual property rights. Indeed, this terminology would better indicate that data access may also often require an additional (licensing) contract between the data holder and the person entitled to claim data access, whereby this contract fixes the terms and conditions of access, including the question of whether the data holder is entitled to remuneration.[11] Yet the concept of data access rights may still be unusual for experts of intellectual property rights and general private law

---

8 European Commission, 'A European strategy for data' (n. 1) 13. On the potentially negative impact of the protection of databases, not least due to the sui generis database right, see Drexl (n. 5) 67–85; P. Bernt Hugenholtz, 'Data Property in the System of Intellectual Property Law' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2017) 75; Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2017) 27; Matthias Leistner, 'The existing European IP rights system and the data economy – An overview with particular focus on data access and portability', in this volume.

9 See, for instance, on the right of independent providers of repair services to the on-board data of motor vehicles, Recital 8 and Arts 6–9 Regulation 715/2007 of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, [2007] OJ L171/1, as last amended by Regulation (EU) No 459/2012 of 29 May 2012, [2012] OJ L142/16.

10 See Joined Cases C-241/91 and C-242/91 *RTE and ITP v Commission* ('*Magill*') [1995] ECR I-743 = ECLI:EU:C:1995:98 (on the duty of TV broadcasters to license the copyright protecting the programming information to independent TV guide publishers); Case T-201/04 *Microsoft v Commission* [2007] ECR II-3601 = ECLI:EU:T:2007:367 (on the duty of Microsoft to grant access to interoperability information to allow competitors to program competing work-group server operating systems in a way to be compatible with Windows).

11 This is why, in the *Microsoft* case, the General Court (GC) was also requested to decide on principles for calculating 'reasonable and non-discriminatory' royalty

who are more used to thinking in terms of exclusive rights and contractual obligations. However, the Draft Principles for the Data Economy of the American Law Institute (ALI) and the European Law Institute (ELI) now acknowledge a large variety of legal tools and list data access rights as one sub-category of data rights.[12]

Yet introduction of data access rights should only be considered with caution. Obliging private actors to grant access to data constitutes a form of market regulation and intervention. From a constitutional perspective, data access rights, restricting the fundamental right of the data holder to conduct a business,[13] are therefore in need of a justification. Following the principles of sound economic regulation, data access regimes should only be adopted where they respond to a market failure. The Commission acknowledges such restrictions, noting that access to data should only become a legal obligation 'where specific circumstances so dictate'.[14] The Commission further indicates that data access rights should only be adopted in the framework of sector-specific regulation and under the condition that a market failure is identified that competition law cannot solve.[15]

In line with these considerations, this chapter seeks to explore under which conditions an access right to machine-generated data should be granted to the users of connected devices. Thereby, the scope of the following research goes beyond a strict sector-specific approach, as connected devices appear in a great variety of different sectors of the economy. However, it can be assumed that neither the underlying market failure nor the public and private interests involved will largely vary depending on the sector of the economy that now experiences the advent of connected devices. Therefore, the following analysis seeks to develop a common legal framework for data access rights in the context of such devices. This framework could be implemented either in the form of general cross-sectoral legislation or sector-specific legislation building on a set of general princi-

---

rates for access to interoperability data. See T-167/08 *Microsoft v Commission* ECLI:EU:T:2012:323.

12 These Principles are not final and therefore not yet publicly available. See, however, Christiane Wendehorst (Project Reporter representing the ELI), 'The ALI-ELI Principles for a Data Economy' in Alberto De Franceschi and Reiner Schulze (eds), *Digital Revolution – New Challenges for Law* (C.H. Beck and Nomos 2019) 42, paras 37–42.

13 Art. 16 EU Charter of Fundamental Rights. In general, on the constitutional framework for data access, see Thomas Fetzer, 'The constitutional framework of data access rights', in this volume.

14 European Commission, A European strategy for data' (n. 1) 13.

15 Ibid. 13 note 39.

ples. Yet the one does not exclude the other. Sector-specific and cross-sectoral legislation may co-exist, whereby the latter constitutes a form of framework legislation that applies where sector-specific legislation is missing.

In the following, this chapter will first define some general concepts that are used throughout the analysis (at B. below). It will then identify access rights as just one legal element of broader regulatory systems of data governance (at C. below). After describing how connected devices transform markets and business models (at D. below), the chapter will identify data lock-in as the underlying market failure (at E. below). However, data access rights will only be advisable and justified to the extent that existing remedies are not available or insufficient and that access rights are actually needed to remedy a market failure. Therefore, this chapter furthermore explores alternative regimes for data access rights (at F. below). Thereby, it will in particular show that contractual rights and competition law are not sufficient to provide data access. This is why the chapter ultimately proposes an additional unfair competition law approach to data access rights of the user of connected devices (at G. below).

B. General concepts

This research is in need of using uniform terminology. Yet the following definitions do not only serve the purpose of identifying the object of research of this chapter. They are also designed to prepare the design of the ultimately recommended data access right in the light of the underlying market failure.

I. Connected devices

This chapter uses the term 'connected devices' in a broad sense, namely, as all devices that (1) are connected with other things and persons through wired or wireless communication[16] and (2) generate data.

16 Connected devices are often understood as a feature of the Internet of Things, which relies on most modern, even 5G mobile telecommunications technologies. Yet the latter is not necessary condition. For instance, kitchen devices may easily communicate with each other based on Wi-Fi and the kitchen computer may order food through wired communication.

Such devices do not need to be 'intelligent' or 'smart' in the sense that artificial intelligence systems are embedded in the device. Nor does the term presuppose that the device can make autonomous decisions or act as an autonomous agent. The broader definition has the advantage of also capturing larger networks of devices in which specific functions are allocated across a network of units. For instance, as part of a monitoring system of medication, a drug may be equipped with a sensor that sends the information that the patient has taken the drug from the patient's stomach to a connected wearable, from where the information is further communicated to the central server of the pharmaceutical company; there, the information may be analysed, and, ultimately, either a human being or an autonomous digital agent takes further measures.

Hence, the term is to be understood in a technologically neutral sense. Even application of sensor technology, such as in cars, farming machines or smart wearables, is just one form of generating data. The concept also includes devices without sensors, such as smart meters, that collect data and transmit those data through wireless or wired communication. Furthermore, connected devices are not limited to those that communicate autonomously through the Internet of Things. Devices used by humans for the purpose of communication, such as PCs, tablets or smartphones, are equally covered, because it is not relevant to what extent the device stores and processes data without being influenced by the decisions of a natural person. This is because most data collection through connected devices is influenced by human decisions to some extent. For instance, in the abovementioned example of a drug in which a sensor is embedded, the patient has to take the drug first and thereby starts the data collection and communication process. The extent of human influence on such data generation and processing will not matter for answering the question of whether there should be a data access right or not. Furthermore, the relevant data generated through a connected device do not have to be stored in the same device. Connected devices are also those that communicate and share dynamic data in larger networks in real time, even without storing data at all. Connected devices do not only function by using data they autonomously generate; they may also rely on data they receive through wired or non-wireless means from other sources, including other devices.

II. Data

In 2017, when the Commission for the first time was considering the future legal framework for 'Building the European Data Economy', it fo-

cused on machine-generated data as unstructured raw data.[17] This focus can only be explained by the intent to define the subject-matter of the data producer's right that should be allocated to the owner or long-term user of a connected device. Indeed, these raw data constitute the first level of digital data that the use of a connected device generates. In addition, the Commission was probably influenced by earlier legal writing that, at a time when connected devices and machine-generated data were still quite unknown, tried to design an ownership right in data.[18] There, the argument in favour of a data ownership right was predominantly that the act that ultimately leads to the digital encoding is the one that should be considered the act of 'producing data'. Since the focus at that time was on the recognition of a property right in 'digital' data, this approach attempted to restrict protection of data on the syntactic level, hence, without taking the semantic level, as the information that can be taken from the data or the function of the data (as in the case of software or music), into account.[19]

This approach had to face critique. Above all, it failed to explain why the recognition of such data producer's rights was needed from the perspective of an incentive theory. Indeed, it was not argued that such right was needed as an economic incentive to generate the data in the first place.[20] The objective of the scholarly proposal for recognising data ownership was a different one, namely, to enhance the tradability of data. The data producer's right was expected to create transparency as regards property rights in data as a basis for functioning data markets.[21]

Yet, in 2017, the Commission was tempted to pick up this proposal in substance, albeit with a different policy objective. The Commission considered using the economic interests of the owner or long-term user of a connected device to overcome a data lock-in. While the Commission may thereby have identified the underlying market failure correctly, it over-

17 European Commission, 'Building a European data economy' (n. 3) 8–10.

18 See, in particular, Herbert Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers"' (2015) Computer und Recht 137. Yet, already at that time, other authors were opposed to the introduction of data ownership rights; see, for instance, Thomas Heymann, 'Rechte an Daten – Warum Daten keiner eigentumsrechtlichen Logik folgen' (2016) Computer und Recht 650 (in direct response to Zech).

19 Zech (n. 18) 138.

20 See Zech (n. 18) 144–45 (rejecting the incentive theory as a basis for the data producer's right).

21 See, in general, Herbert Zech, 'Information as a Tradable Commodity' in Alberto de Franceshi (ed.), *European Contract Law and the Digital Single Market* (Insentia 2016) 51.

looked important arguments against data ownership. In particular, it did not take into account that, in many instances, the machine-generated digital raw data will immediately go through additional stages of analysis and processing for the very purpose of guaranteeing the functioning of the device. In this regard, the Commission did not explain the relationship of the unstructured raw data with derived[22] or inferred data.[23] Even more importantly, the attempt to reduce the data producer's right to the syntactic level was destined to be futile. In the data economy, the economic value of data derives from the utility of the data in terms of their informational content or functionality. Hence, it is the semantic level that provides the data with value. Data in the digital context should not simply be defined as digital data in the form of bits and bytes but as 'digitally encoded information (or function)'.

Yet, already back in 2017, the Commission realised that – on the semantic level – raw machine-generated data could include personal information. To avoid a conflict with the right to data protection, the Commission therefore tried to limit the debate to 'non-personal' machine-generated data.[24] However, to identify the subject-matter of protection of the data producer's right in this sense, the semantic level of the data, in other words, the meaning or function of the data needs to be taken into account.

To focus on the utility of data on the semantic level is equally important for the object of a data access right. To decide for which data the user of a digital device should have such a right, it is necessary to identify the conflicting interests of this user and the data holder (typically the device manufacturer). This is confirmed by already existing sector-specific access rights of competitors. In these cases, the kind of data the law obliges data holders to grant access to is defined by the specific interest of the competitor claiming data access. In particular, it is the dependence on certain data for remaining in or entering a specific market that justifies access to data. This can be generalised: data access rights in this context serve a particular economic function. This function defines the concrete data that constitute the

22 The term 'derived data' denotes data derived from other data elements using a mathematical, logical or other type of transformation. In this sense, aggregated anonymised health data can be considered as derived data in relation to the original personal health data.

23 Inferred data are generated from statistical correlations, often resulting from big data analyses. Inferred data are probabilistic by nature. An example would be the credit scoring of individual consumers through analysis of large customer-related datasets.

24 European Commission, 'Building a European data economy' (n. 3) 9.

subject-matter of the access right on the semantic level. Accordingly, the law grants independent providers of motor vehicle repair services access to on-board data that these providers need in order to provide their repair and maintenance services.[25]

Equally, if the data access right of the user of the connected device serves the purpose of overcoming a data lock-in, the relevant data should be defined in the light of this purpose. Such interest is not necessarily limited to the first level raw data, which of course also contain certain information, but will often require access to derived or inferred data as information arising from subsequent steps of data processing and analyses.

Conversely, this purpose-oriented understanding of data for designing data access rights also limits the scope of the data access right. This does not rule out that other data access rights may serve different or additional, even non-economic, objectives. This is especially the case for the portability right regarding personal data in Article 20 General Data Protection Regulation (GDPR).[26] While this right may also apply with regard to data collected by connected devices[27] and also serves the purpose of helping the data subject (often a consumer) to switch suppliers,[28] the data portability right applies to any personal data that the data subject has 'provided' to a data controller. Here, beyond the goal of enhancing competition by facilitating the switching of suppliers, this data portability right is justified by the additional goal of guaranteeing data autonomy of the data subject based on fundamental rights considerations.

III. The user of connected devices

With the particular focus on the user of connected devices, this chapter makes a choice as regards the potential holder of the data access right. This choice does not preclude the legislature from also, or alternatively, considering vesting data access rights in competitors in particular.

This chapter uses the term of 'user' in a rather unspecific way. The 'user' does not need to use the device physically. What matters more is the partic-

25 See Arts 6–9 Regulation 715/2007 (n. 9).

26 Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, [2016] OJ L119/1.

27 See the analysis by Drexl (n. 5) 151–153.

28 Ibid. 152.

ular interest a person has in the data generated by the device that justifies access. In this context, both the operator of a car rental service and the customer renting the car could qualify as users of the car, while only the former owns the car and the latter physically uses the car. The same holds true for farming machines that independent service providers physically operate on the land of farmers as their customers. Here, in addition to the service provider – who may typically own the machine – the individual farmer should also be considered a 'user' of the machine to the extent the machine collects data from the farmer's land. Hence, for the question of whether the farmer has a right of access to the data connected machines collect from the farmer's land, it should not matter whether the farmer also owns or physically operates the machine.

In contrast to access rights of competitors, this chapter focuses on the vertical dimension and specifically asks whether the user should have data access rights against the device manufacturer as the de facto data holder. Depending on the specific connected device and the concrete purpose of the use, the holder of the data right will often be a consumer in the sense of European consumer law. Thus, this chapter is also designed as a contribution to the development of European consumer law in the digital era. But it is not limited to consumer law, since connected devices, such as a connected car, smart farming machines or even manufacturing robots used in factories, can equally or will exclusively be used for commercial or other professional purposes.

IV. Data access

Moreover, this chapter uses the term 'data access' in a broad and flexible sense. Upfront, data access is not limited to a right of being informed of what information is contained in a dataset. Nor is it limited to 'portability' in the sense of the data portability right of Article 20 GDPR as a right to 'receive' the data or have the data 'transmitted' at a given point in time. What data access actually requires will depend on the interest that justifies the right. This can also mean that data access requires real-time data sharing.

C. Data access rights as an element of data governance

Data access and sharing will keep markets open and maintain incentives for digital innovation.[29] Yet data access rights should be seen as only one element of a broader, more holistic approach to data governance.[30]

Data governance has to take into account the interests of multiple stakeholders and multiple policy goals. Whatever measure is taken or recommended, including data access rights, these measures need to be devised and coordinated in the framework of such data governance systems. As regards the policy goals, promoting data access and data sharing should not be considered as the final goal. Rather, rights to data access and data sharing are to be advocated as measures that ultimately promote efficient and competitive markets as well as innovation.

Data governance requires a balancing of the interest in data access and sharing with conflicting interests. Most importantly, in a world where connected devices penetrate the private life of individuals, the constitutional right to data protection[31] needs to be taken account of. Since in many cases connected devices will collect both personal and non-personal data, data access rights must not ignore data protection rules. Yet personal data is not the only group of 'sensitive data'. Machine-generated data may also constitute trade secrets of the device manufacturer who has a legitimate interest in being protected against the making available of such data to competitors. This does not necessarily have to exclude data access rights of the users. Yet the nature of data as trade secrets of the data holder may argue for confidentiality obligations of the user to whom access to the data is granted.

Moreover, it is important to understand that the recognition of a right to data access is not sufficient to guarantee data access. Data governance has to include various kinds of measures, whereby legal measures only constitute one set of measures. In general terms, data governance has three – (1) technical, (2) regulatory and (3) organisational – dimensions.

From a technical perspective, data governance and, as part of it, data access and data sharing depend on the availability of many technologies, such as powerful mobile telecommunications technologies. Data access

---

29 European Commission, 'A European strategy for data' (n. 1) 2–3 (specifically referring to the dependence of innovative start-ups and SMEs on access to data and the role of access to data as training data for artificial intelligence).

30 See, in particular, Wolfgang Kerber, 'From (horizontal and sectoral) data access solutions – Towards data governance systems', in this volume.

31 Art. 8(1) EU Charter of Fundamental Rights; Art. 16(1) TFEU.

and data sharing requires data interoperability, standardisation of data formats and access to the use of application programming interfaces (APIs). As regards data protection, data governance has to rely on anonymisation technologies and technologies that prevent deanonymisation. Cutting-edge technologies, such as blockchain technology, may also enhance data autonomy and sovereignty of data subjects as regards their personal data.[32] The lack of such technologies constitutes obstacles to the application and enforcement of data access rights that also respect data protection rules.[33]

As regards the legal dimension, data access rights are part of the legal framework that defines the rights and obligations of the different actors in the data economy. The data governance approach requires the legislatures to take into account the rights and interests of the multiple stakeholders as well as other public interest grounds.[34]

It is on this level where data access rights have to be coordinated with other legal measures including data protection rights and intellectual property rights. As regards the latter, data governance should not blindly give priority to intellectual property protection over data access rights, as seems to be the case under Article 20(4) GDPR.[35] Therefore, it has to be considered a step in the right direction that the European legislature has now given priority to the right to re-use public sector information over government-held intellectual property rights in the framework of the recently revised Directive on Open Data and PSI.[36] Even more, it has to be welcomed

32 See Shraddha Kulhari, *Building-Blocks of a Data Protection Revolution – The Uneasy Case for Blockchain Technology to Secure Privacy and Identity* (Nomos 2017).

33 Data access rights have to take into account such technical obstacles. See, for instance, Art. 20(1) GDPR, which provides that a data subject can claim the transfer of the data in a 'structured, commonly used and machine-readable form'. Accordingly, the data subject depends on the existence of technology that fulfils these requirements.

34 The author of this chapter has proposed a comprehensive theory for regulation in earlier writing. See Drexl (n. 5) 49–59; Josef Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' in Alberto De Franceschi and Reiner Schulze (eds), *Digital Revolution – New Challenges for Law* (C.H. Beck and Nomos 2019) 19, paras 7–41.

35 Rather opaquely, Art. 20(4) GDPR states that data portability 'shall not affect the rights and personal freedom of others'. In favour of a narrow interpretation according to which intellectual property rights of the data controller should not be considered rights of others, Drexl (n. 5) 83–85.

36 Accordingly, only documents in which third parties hold intellectual property rights remain excluded from commercial re-use. See Art. 1(2)(c) and Art. 3(2) Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, [2019] OJ L172/56.

that the European Commission now announces its intent to review EU intellectual property legislation in view of promoting data access and use.[37] In addition, nothing would prevent the EU legislature from adopting regimes on access rights that legally prevail over privately held intellectual property rights. Similar to competition law, such rules could be viewed as 'external' exemptions and limitations that apply horizontally to various intellectual property rights. Such rules would not collide with international treaty obligations in the field of intellectual property to the extent that legislation on access rights is compliant with the three-step test.[38] From a perspective of sound economic regulation, coordinating access rights with intellectual property would require the legislature to balance the diverse positive and negative effects on the incentives for innovation of both intellectual property protection and access rights. As part of this balancing, the legislation would have to take into account that the person seeking, or indirectly benefitting from, data access will often be a follow-on innovator. Moreover, intellectual property rights may prove particularly detrimental where they foreclose use of technologies that need to be used for data sharing. This is why courts should be cautious as regards recognition of copyright protection for APIs.[39]

From an organisational perspective, data access will depend on institutional arrangements concerning standard-setting mechanisms and bodies as well as platforms for the sharing of data. New types of actors can play an important role in enabling data access and sharing, such as independent data trustees, and therefore should be promoted. In particular, data trustees as intermediaries could enhance commercial transactions by assessing the utility of the data for the purposes of the person seeking data access, thereby helping overcome the economic problem of the information paradox. The information paradox is caused by an information asymmetry

37 European Commission, 'A European strategy for data' (n. 1) 13.

38 See Arts 13, 17, 26(2) and 30 Agreement on Trade-Related Aspects of Intellectual Property (TRIPS).

39 This matter is largely unaddressed or unresolved in the different jurisdictions. See, however, the US case *Oracle America, Inc v Google, Inc*, 886 F.3d 1179 (Fed Cir 2018), where the US Court of Appeals for the Federal Circuit held that Google infringed Oracle's copyright by integrating the Java programming language API in its Android operating system (also holding that Google is not able to rely on the US fair use exemption). On Google's request, the US Supreme Court has however granted certiorari and is expected to hear any time soon.

concerning the quality, provenance and value of data.[40] It describes the problem that the person seeking access to information cannot assess the value of the information without getting access to it. However, once somebody has access to the information, this person will no longer be willing to pay a price for access. However, this problem can be solved by intermediaries. A data analytics trustee could be appointed to run sample tests on the quality and utility of the dataset concerned and describe the utility of the dataset for the purposes of the person seeking access in general terms.[41] Furthermore, independent trustees can work as mediators or arbitrators for assessing the reasonableness of royalty rates for access to data.[42] Therefore, they could also play a role for enhancing the effectiveness of data access regimes.

D. Transformation of the markets

The advent of connected devices, building on sensor technology, mobile communication, data analytics and artificial intelligence, fundamentally transforms both the manufacturing process and the markets.

I. Competition-driven innovation

Connected devices are products with increased utility, higher quality and safety as well as convenience. Accordingly, connected devices can be con-

40 As coined by Kenneth J. Arrow, 'Economic welfare and the allocation of resources for invention' in National Bureau of Economic Research (NBER) (ed.), *The Rate and Direction of Inventive Activity* (Princeton University Press 1962) 609.

41 Such market solutions are nowadays considered an option to the claim that exclusive data ownership rights are needed to create workable markets for data. See, in general, Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer, 'The economics of ownership, access and trade in digital data', JRC Digital Economy Working Paper 2017–01 (European Commission 2017) 36. Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil 989, 994, even assumes that the problem could be solved through the data holder by informing the prospective customer in general terms about the data. See also Drexl (n. 5) 136.

42 In the *Microsoft* case, based on EU competition law, the European Commission has ordered the appointment of an independent trustee to play such a role. See, in particular, Case T-167/08 *Microsoft v Commission* ECLI:EU:T:2012:323, para. 102.

sidered as innovation.[43] The most important driver of this innovation seems to be competition. In many instances, connected devices lead to disruptive innovation. Firms understand that if they do not 'digitise' their products, they may well have to leave the market soon.

In particular, pro-competitive advantages explain the success of digitisation of machines in the industrial context, often described as a Fourth Industrial Revolution ('industry 4.0'). For industrial customers, 'smart manufacturing' constitutes both process and product innovation. In terms of process innovation, smart machines allow for predictive maintenance and, hence, avoid down times, thus creating enormous potential for cost savings. This enhances the ability of manufacturers to compete on price even if they produce non-connected traditional goods. In terms of product innovation, smart manufacturing increases the quality of products, preventing technical failures and human mistakes that may otherwise result in the distribution of defective goods.

Connected devices are also sold to consumers. In this regard, increased utility, safety and convenience will typically be among the primary selling points. Yet consumers who are particularly sensitive to data protection may hesitate to buy connected devices that could 'spy' on their private life. Therefore, high standards of data protection should not only be considered as a potential obstacle to digitisation. Data protection rules and their effective enforcement can build trust as a basis for the success of connected devices in consumer markets.

II. Transformation of business models and markets

Connected devices do not only constitute disruptive innovation that has the power to replace the former generation of non-connected devices. Often, they are also disruptive for the business models and the markets in which they are sold.

This transformation is characterised by 'servicisation'. In the case of connected devices, the purchase of a physical device typically comes with a ser-

---

43 Relying on the notion that innovation requires implementation in goods and services that satisfy consumer demand. See OECD, Oslo Manual 2018 – Guidelines for Collecting, Reporting and Using Data for Innovation (4th edn, OECD 2018) 20, where 'innovation' is defined as follows: 'An innovation is a new or improved product or process (or combination thereof) that differs significantly from the unit's previous products or processes and that has been made available to potential users (product) or brought into use by the unit (process).'.

vice. In an industry 4.0 environment, the manufacturer of a smart machine will also provide predictive maintenance to the customer. At times of automated and autonomous driving, the manufacturer of a car also provides attached digital services that may gradually progress in the future from guaranteeing safe and convenient driving to the full provision of a transport service to 'passengers'. Producers of household devices that also sell a kitchen computer may develop into providers of comprehensive household management systems. Energy providers can use connected devices to become operators of facility management systems. And pharmaceutical companies no longer simply sell drugs; digitisation of drugs and smart wearables allow them to become health care providers. In many instances, the manufacturer or the downstream provider of a service may decide to retain the ownership of the device, which then only plays the role of a tool to provide a service.[44]

From a legal perspective, servicisation fundamentally changes the relationship between the end-consumer and the manufacturer. While in the past, end-consumers often bought devices from retailers, without direct contractual contact with the manufacturer, customers are nowadays required to sign additional contracts with the manufacturer of connected devices concerning the use of the embedded software or other digital services. In addition, where a device collects personal data from the end-user and the manufacturer seeks control of these data as the data controller, the manufacturer will additionally have to request consent pursuant to the data protection rules of the GDPR.

Depending on the concrete connected device and the business model chosen, this creates a complex relationship, which is characterised by three features: (1) bundling of multiple transactions regarding different subject matter (sale of the device, provision of digital services, processing and use of personal data);[45] (2) establishment of a long-term relationship with the manufacturer; and (3) triangulation of the relationship between manufac-

44 This is more likely to happen where, as in the case of a connected smoke detector, the connected device is of a lower value or requires constant monitoring. But the same may happen where a user is not in permanent need of the device, such as a farmer regarding certain farming machines or consumers regarding the use of cars.

45 Raising, for instance, the question of whether the provision of personal data could or should be considered a counter-performance for receiving a digital service especially in cases in which the service provider does not claim any monetary remuneration. The debate was especially driven by the use of the term 'counter-performance' in the proposal of the Commission for the Digital Content Directive to extend the scope of application of the Directive to contracts where con-

turer, retailer and final customer across the distribution chain. Triangulation creates legal challenges regarding, in particular, allocation of liability for non-conformity of the goods and services with the contract. In the context of the most recent reform of consumer law, the European legislature decided to allocate contractual liability as regards digital content or digital services that are incorporated in or inter-connected with consumer goods – so-called 'embedded software' and 'embedded services' – in the person of the seller of the device even if another person, such as the manufacturer in particular, supplies the digital content or the digital service.[46] Here, triangulation convinced the European legislature to set aside the fundamental private law principle of privity of contract. The choice to impose liability on the direct trader was not at all obvious and mostly due to the objective to simplify the claiming of rights for consumers.[47]

E. Data access rights as a means to overcome data lock-ins

As mentioned, already in 2017, the Commission, in attempt to launch a debate on the future legal framework of the European data economy, correctly noted that the data collected and generated in an IoT context often constitutes a key input for other innovative services and that access to such data for innovative firms could therefore enhance the data economy.[48] In

---

sumers provide personal data as a 'counter-performance' without undertaking to pay a price. On the private law implications of such concept, see Axel Metzger, 'Data as a Counter-Performance: What Rights and Duties Do Parties Have?' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 2. The final text of the Directive ultimately avoids the use of the term 'counter-performance'. On the reasons for giving up mentioning the term 'counter-performance'. See Art. 3(1)(2) Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, [2019] OJ L136/1. Even under the final version authors argue that consumers 'pay' with data to get a digital service. See Dirk Staudenmayer, 'The Directives on Digital Contracts: First Stepts Towards the Private Law of the Digital Economy' (2020) 2 European Review of Private Law 219, 225–26.

46 Art. 3(3) Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, [2019] OJ L136/28. See in more detail Staudenmayer (n. 45) 231.

47 Staudenmayer (n. 45) 231.

48 European Commission, 'Building a European data economy' (n. 3) 8.

particular, the Commission was concerned that the 'generators of data', obviously referring to the manufacturers of connected devices, could keep these data to themselves to analyse them in 'silos',[49] thereby foreclosing access of innovative firms to downstream markets for data-related services.[50]

As regards the datasets that can be used in downstream markets, a distinction has to be made between aggregated data and individual-level data. On the one hand, the manufacturers use the connected devices to collect, analyse and aggregate data. These aggregated data can be of interest for firms, for instance for the purpose of training artificial intelligence systems, but also for the state or researchers to pursue public interest goals. Yet, in 2017, the Commission focused more on the individual-level data as the data collected by a single device. Indeed, withholding these data would foreclose market access for innovative firms that intend to provide data-related services to the user of such a device. An example would be a service that optimises harvesting by using the data collected by farming machines on the land of a given farmer. Such service could either be offered by the manufacturer of the farming machine or an independent digital service provider.

In general, control over machine-generated data enables the manufacturer of connected devices to bundle other goods and services to the sale of the device. Thus, the provider of a digital household assistant could in principle also tie manifold other household devices, such as the washing machine and the refrigerator, to the sale of the digital assistant. Since, in times of artificial intelligence and autonomous agents, such a household assistant could also take over consumer decisions on the purchasing of secondary goods needed in a household, including food or cleaning materials, such bundling could also extend to many more markets for consumer goods and retailing.

These examples show that, without legal guarantees of access to data, the decision to purchase a particular connected device may lead to a lock-in of the user with regard to many other goods and services. Such data lock-ins raise concerns from the perspective of innovation as well as consumer and competition policy. In particular, the objective of overcoming such data lock-ins should move to the centre of competition policy, to

49 Ibid.
50 Ibid. 9.

keep markets open, to maintain consumer choice and to safeguard incentives for innovation in the digital sector.[51]

As regards the means to overcome such data lock-ins, in 2017, the Commission was considering potential adoption of legislation on a new data producer's right to be vested in the owner or long-term user of a connected device.[52] At that time, the argument was that such right would 'open the possibility for users to utilise their data and thereby contribute to unlocking machine-generated data'.[53] From a consumer policy perspective in particular, it was quite appropriate to rely on the interests of the 'users' of connected devices as potential purchasers of additional connected devices and recipients of secondary digital services to 'un-lock' machine-generated data. However, creating a new exclusive data ownership right would have been the wrong instrument to remedy the market failure of the data lock-in for various reasons.[54] First, the Commission overlooked the fact that a data lock-in can only be expected where the manufacturer enjoys superior bargaining power. Yet property rights are not a suitable means to solve a problem of unequal distribution of bargaining power. A device manufacturer could easily include a clause in its standard contract terms requiring the users of the devices to transfer or license the data producer's right for free.[55] Rather than 'un-locking' data, a data producer's right could thus even strengthen the anyhow existing de facto exclusivity position of manufacturers. Secondly, the data producer's right could considerably distort the working of secondary markets for aggregated data, since a person seeking access to the aggregated data could no longer simply assume that the manufacturer, despite being the de facto data holder, holds all the legal

51 On the competition law dimension, see also Heike Schweitzer and Robert Welker, 'A legal framework for access to data – A competition policy perspective', in this volume.

52 European Commission, 'Building a European data economy' (n. 3) 13.

53 Ibid.

54 For a full evaluation of the data producer's right in this regard see Drexl (n. 5) 132–50.

55 See 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 a European Data Economy"' (2017) para. 18, <www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf> accessed 31 August 2020; Josef Drexl, 'On the Future EU Legal Framework for the Digital Economy: A Competition-based Response to the "Ownership and Access" Debate' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2018) 223, 235.

rights needed to provide data access. In any instance, adoption of exclusive data producer's rights for machine-generated data for the owner or long-term user of connected devices would create the need for rights clearance where third persons seek access to the aggregated data held by the device manufacturer.[56] In sum, rather than solving the problem of data lock-ins, a data producer's right would lead to legal uncertainty and, therefore, impede the development of the digital economy.

This shows that the appropriate legal instrument has to be tailor-made for the specific market failure it is supposed to remedy.[57] Hence, where purchasers or users of connected devices suffer from a lack of data access, the appropriate remedy has to be a data access right. This is not a new insight. Such data access rights, albeit for competitors in secondary markets, are known from sector-specific regulation.[58]

F. Alternative legal instruments

Yet adoption of a data access right of the users of connected devices should also take into account the availability of alternative legal regimes for access. Already today, the data portability right pursuant to Article 20 GDPR provides the owner or long-term user of a connected device with access to personal machine-generated data. However, this right is limited in many regards (at I. below).[59] More importantly, this following section will show that the two legal instruments essential for a functioning market economy, namely, contract law (at II. below) and competition law (at III. below), are insufficient to provide access to machine-generated data. This is not only the case as regards existing rules. Due to the inbuilt limitations of the contract and competition law systems, even potential future reforms would

56 Drexl and others (n. 55) para. 19; Drexl in Lohsse, Schulze and Staudenmayer (n. 55) 235–36.

57 See also Drexl and others (n. 55) para. 21.

58 As in the case of access of independent providers of repair and maintenance services to the on-board data of motor vehicles (see at n. 9, above) or in the case of access of providers of digital payment services to the bank account data of their customers. On the latter, see Art. 36 Second Digital Payment Services (DPS2) 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.

59 On the limitations of this right as regards machine-generated data see Drexl (n. 5) 150–54.

not achieve the goal of providing sufficient data access to the users of connected devices. In addition, the suitability of data access rights of users of connected devices need to be compared with data access rights of competitors (at IV. below). Finally, this following section seeks to clarify the relationship with exceptions and limitations of existing systems of intellectual property protection that may foreclose access to machine-generated data (at V. below).

I. The right to portability of personal data pursuant to Article 20 GDPR

As regards access to data generated by connected devices, the data portability right pursuant to Article 20 GDPR can already provide a data access right in certain instances. Yet this right is not sufficient to achieve the goal of providing data access to the extent that this is needed.[60]

On the one hand, the scope of application of Article 20 GDPR seems to be broader than needed, since it is not limited to data generated by connected devices. Yet the provision is limited to personal data. This will prove insufficient in many instances where the user of a connected device is required to get access to the machine-generated data for receiving a service from a third business operator. For instance, a farmer may be in need of access to the data generated by farming machines to contract with the provider of a digital farm management system. Here, the availability of a data access right should not depend on the debatable question of whether the data related to the soil of the land of an individual farmer makes these data personal data in the sense of the GDPR. It is more important to note that the objective to overcome a data lock-in in such circumstances should not depend on whether the data qualifies as personal data.

Furthermore, Article 20(1) GDPR only applies to personal data the data subject has 'provided' to the controller. Therefore, the major discussion regarding the application of this data portability right in an IoT context mostly concentrates on the extent to which personal machine-generated data can be considered as provided by the data subject. Indeed, the provision seems flexible enough to give it a broad meaning so as to include 'observed' data too. This would guarantee that the data portability right also covers the geolocation data generated by a smartphone or the data on the

60 See in general Drexl (n. 5) 108–10.

bodily functions of a person collected by a fitness tracker.[61] In all such instances, while the data subject is not acting with the intent to provide specific data to the data controller, the data subject fulfils an active element that results in data collection as part of the functionalities of the device and the service provided to the data subject. The extension to such 'observed' data is also needed to realise the full pro-competitive benefits of the data portability right. Thus, the holder of a car registering the driving habits of the driver could rely on the data portability right to benefit from a lower insurance premium when switching the car insurer. Yet the wording of Article 20(1) GDPR can no longer be considered as fulfilled in the case of 'derived' and 'inferred' data, which are generated through additional data processing and data analyses.[62] Such conclusion is supported by a comparison of Article 20(1) GDPR with the data access right in Article 15 GDPR, which, in contrast to Article 20(1) GDPR, does not include a right to claim the transfer of the data. Not limited to 'provided data', this data access right covers all personal data held by the data controller, including derived and inferred data.

In contrast, the data portability right provides a good template for an additional right of access to data generated by connected devices to the extent that Article 20(2) includes a right to claim the direct transfer to another data controller and that the data subject can claim the transfer at any time. Yet the wording of Article 20(1) and (2) GDPR seems to indicate that the right to data portability is limited to the 'transfer' of data, while in the interest of the users of connected devices, it would be important to also include a right to real-time data sharing. Thus, the user of a connected device

61 See Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (13 December 2016, revised 5 April 2017) 9–10, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233> accessed 31 August 2020; Ruth Janal, 'Data Portability – A Tale of Two Concepts' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 59, para. 4.

62 Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (n. 61) 10. This interpretation is broadly accepted in legal writing. See, for instance, Paul De Hert, Vagelis Papakonstaninou, Gianclaudio Malgieri and others, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018) 34 Computer Law & Security Review 193, 200; Lucio Scudiero, 'Bringing Your Data Everywhere: A Legal Reading of the Right to Portability' (2017) 3 European Data Protection Law Review 119, 122–23; Lachlan Urquhart, Neelima Sailaja and Derek McAuley, 'Realising the right to data portability for the domestic Internet of things' (2018) 22 Personal & Ubiquitous Computing 317, 319.

could claim that a third service provider have permanent access to data continuously generated by the device.

II. Contract law

Contract law is an obvious candidate for addressing the issue of access to machine-generated data. Users of connected devices are typically direct or indirect purchasers of such devices.

Given the fact that especially consumers suffering from inferior bargaining power could easily contract away their right to data access, such right should be recognised as a part of mandatory European contract law. Beyond the portability right regarding personal data pursuant to Article 20 GDPR, European consumer contract law also provides for a data access right in Article 16(4) Digital Content and Services Directive (DCSD) as regards non-personal data.[63] Yet this right equally fails to provide sufficient access to data generated by connected devices.

Article 16(4) requires a trader to make available certain non-personal data, namely, 'content … which was provided or created by the consumer when using the digital content or digital service supplied by the trader'.[64] This provision complements the portability right concerning personal data pursuant to Article 20 GDPR and will especially apply in cases where a consumer uploads content, such as pictures, music and other audiovisual content that does not necessarily qualify as personal data in the sense of the GDPR.

Yet the application of the provision is considerably restricted in several regards.[65] Most importantly, it does not apply to data collected through so-called 'embedded' software or services. The provision requires a contract on the 'supply of digital content or digital service'. According to Article 3(4) DCSD, this does not cover the case where digital content or services are 'incorporated in or inter-connected with' a tangible item in such a way that absence of the digital content or digital service would prevent the item from performing its function. The purpose of the provision is to delegate consumer protection as regards connected devices to the regime of the

63 Directive (EU) 2019/770 (n. 45).

64 On the interpretation of Art. 16(4) DCSD, see Axel Metzger, 'Access to and porting of data under contract law: Consumer protection rules and market-based principles', in this volume, Part B.

65 See Metzger (n. 64) Part B.II.

Sale of Goods Directive (SGD).[66] The two Directives are therefore meant to be complementary.[67] According to Article 16 SGD, in case of a malfunctioning of the device, which may also arise from the digital elements of the good,[68] the consumer has a right to terminate the contract according to Article 16 SGD. But unlike Article 16(4) DCSD, this provision does not include a right of access to the data,[69] which may not prevent the Member Stats to provide for a right to claim tranfer of the data under national law.[70]

This shortcoming does not rule out that future reform of EU consumer contract law will create additional access rights for consumers. Yet extending the model of Article 16(4) DCSD to data generated by connected devices would still remain insufficient. First, the right is limited to data that is 'provided and created' by the consumer. As in the context of the data portability right of Article 20(1) GDPR, 'provided data' could be understood in a broad sense, namely, to include 'observed' data that a connected device automatically registers as the result of the use of the device by the consumer.[71] Yet 'derived' or 'inferred' data generated through additional stages of data processing and data analyses could hardly be conceived as data 'provided or created' by the consumer.[72] Secondly, the access right is excluded under the conditions as provided by Article 16(3) lit. a), b) and c) DCSD. In particular, this excludes access to data that 'has no utility outside the context of the digital content or the service'.[73] Since, in the case of con-

66 See, on the scope of application, Art. 3(3) SGD (n. 46).

67 See Staudenmayer (n. 45) 230. This does not exclude that the rights even in case of lack of conformity for embedded software or services under the SGD differ from those granted under the DSCD. On this, see Jozefien Vanherpe, 'White Smoke, but Smoke Nonetheless: Some (Burning) Questions Regarding the Directives on Sale of Goods and Supply of Digital Content' (2020) European Review of Private Law 251, 261.

68 Art. 10(2) SGD.

69 See also the criticism of Metzger (n. 65) Part B.II. However, national law may provide for a right of the purchaser to claim transfer of the data. See Vanherpe (n. 67) 268 (hinting at Art. 3(6) SGD, leaving it to the Member States to define the consequences of termination of the contract).

70 See Vanherpe (n. 67) 268 (hinting at Art. 3(6) SGD, leaving it to the Member States to define the consequences of termination of the contract).

71 Janal (n. 61) paras 7–9; Ruth Janal, 'Data portability under the GDPR: A blueprint for access to rights?', in this volume; Drexl (n. 5) 152.

72 On the interpretation of Art. 20(1) GDPR in this regard, see Article 29 Data Protection Working Party, 'Guidelines on the right to data portability' (n. 60) 10 (regarding the personal customer profile generated through data analyses).

73 Art. 16(3) lit. a) DCSD.

nected devices, data are primarily generated to guarantee the functioning of the device, such rule would have the potential of practically excluding data access to machine-generated data. Thirdly, Article 16(4) DCSD only applies as of the moment of termination of the contract, while in the case of connected devices, the user of the device may well depend on data access especially for the purpose of receiving a data-related service from a third person at any time of the contract execution regarding the connected device.

Accordingly, a contractual access right requires much broader scope of application. Within consumer contract law, the reform should not only be limited to a reform of the Consumer Sales Directive by implementing a right of access to data generated by connected devices without a limitation to personal data and the limitations known from the DCSD. Since connected devices do not reach consumers exclusively through sales contracts, such data access right would need to be enacted for any kind of consumer contract to include any rental or other kind of service contract.[74]

In addition, the abovementioned imbalance of bargaining power resulting in a data lock-in is not limited to B2C relationships. Hence, there is also a need for an access right to data generated by connected devices in B2B contracts. Ideally, such right would have to be mandatory to be effective. This explains why, already in 2017, the Commission started a discussion on the introduction of default contract rules to promote access to data and extend fairness control of contract terms to B2B relations.[75] While Germany in particular has a lot of experience controlling the fairness of B2B contracts, the idea of the Commission did not find sufficient support in the public consultation following the Communication on Building a European Data Economy in 2017.[76] It seems that the Commission has meanwhile moved away from this idea. At least, in 2018, it proposed a reform of the Directive on Consumer Contract Terms that did not include

74 This is another short-coming of the SGD as compared to the DSCD. The latter refrained on purpose to limit the concept of contracts on digital services and content to certain types of contracts, such as sales contracts. See Staudenmayer (n. 45) 224.

75 European Commission, 'Building a European data economy' (n. 3) 12.

76 See European Commission, 'Synopsis Report – Consultation on the "Building a European Data Economy" Initiative' (2017) 5–6 <https://ec.europa.eu/information_society/newsroom/image/document/2017-36/synopsis_report_-_data_economy_A0EFA8E0-AED3-1E29-C8DE049035581517_46646.pdf> accessed 31 August 2020.

an extension of fairness control to B2B contracts.[77] Stakeholders participating in the consultation, inter alia, expressed the concern that the situation differs widely between sectors and that therefore fairness control of B2B contracts could harm the development of innovative business models.[78] In sum, for the time being, it cannot reasonably be expected that the EU legislature would implement protection of businesses against contracting away a right of access to data generated by connected devices any time soon.

But even if contractual protection was created, such rules would only apply where there is a contractual relationship between the user of the device and the de facto data holder. Of course, the legislature could take inspiration from the concentration of the contractual rights against the direct trader selling the devices with regard to contractual liability for defects arising from embedded software or services as implemented in the Consumer Sales Directive.[79] Thus, the trader would be legally obliged to grant data access even where the manufacturer holds the data. Such rule would force the manufacturer to design its distribution systems in such a way as to make its connected devices commercially viable. However, contractual data access claims against retailers are not necessarily a sufficient substitute for direct data access claims against the manufacturer, not least in case of insolvency of the retailer.

Moreover, limiting access rights against the direct trader (retailer) would not sufficiently work in many other instances. The chain of contracts between the manufacturer and the user may be too long to guarantee uncomplicated enforcement of the data access right and may include diverse kinds of – sales and service – contracts, such as in the case of a farming machine where the machine is not owned by the farmer but a service provider. In particular, access rights limited against the direct trader would hardly work where connected devices are resold as used goods by end-users.

---

77 See Art. 3 Proposal of Commission of 11 April 2018 for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EEC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council, Directive 2005/29/EC of the European Parliament and of the Council and Directive 2011/83/EU of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules, COM(2018) 185 final.

78 European Commission, Annex to the Synopsis Report (2017) 21 <https://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf> accessed 31 August 2020.

79 See Art. 3(3) SGD.

The better solution in all those cases are direct data access rights against the manufacturer as the de facto holder of the relevant data. This solution would also be preferable in B2B relationships. Such claims would be possible without entering into a fundamental debate on extending mandatory contract law or unfairness control of contract terms to B2B relations, which would raise many additional issues regarding the fundamental principles of European contract law.

III. Competition law

While data access rights are a new issue for contract law, competition law appears a more appropriate and experienced legal basis for data access rights. Upfront, competition law seems to have several advantages. First, it provides framework regulation that applies horizontally across all sectors of the economy. Secondly, based on the prohibition of abuse of market dominance pursuant to Article 102 TFEU, competition law provides claims outside contractual relations, especially in cases of unilateral refusals to deal. Thirdly, competition law has already acquired relevant experience applying Article 102 TFEU to cases where undertakings refused to grant access to data.[80] And finally, given the underlying market failure of a data lock-in, which excludes market access for other undertakings, the competition law approach seems to be most appropriate concerning the market failure that is in need of being addressed. Therefore, is should not come as a surprise that some commentators have argued that competition law provides sufficient remedies and that, therefore, additional access rights are not needed to provide data access in the IoT context.[81]

However, closer scrutiny argues against this conclusion. As the following analysis will show, application of Article 102 TFEU to a refusal to grant access to data in the modern data economy in general and as regards connected devices in particular comes with many uncertainties and limitations that make competition law in its current form a rather unfit instrument

80 See, in particular, Joined Cases C-241/91 P and C-242/91 P *RTE and ITP v Commission* (‘*Magill*’) [1995] ECR I-743 = ECLI:EU:C:1995:98; T-201/04 *Microsoft* [2007] ECR II-3601 = ECLI:EU:T:2007:289.

81 See Jürgen Kühling and Florian Sackmann, ‘Rechte an Daten – Regulierungsbedarf aus der Sicht des Verbraucherschutzes?’, Rechtsgutachten im Auftrag des Bundesverband Verbraucherzentrale (20 November 2018) 22 <www.vzbv.de/sites/default/files/downloads/2018/11/26/18-11-01_gutachten_kuehling-sackmann-recht e-an-daten.pdf> accessed 31 August 2020.

for enforcing data access.[82] However, this does not exclude a future reform of competition law. Indeed, the conviction has by now widely spread that digitisation and digital business models present major challenges for competition law. Following several recent studies conducted on behalf of the European Commission[83] and national governments,[84] there is now growing consensus that competition law is in need of a fundamental reform. This debate has also reached the political level in several jurisdictions. In Germany, in September 2020, the Federal Government submitted a bill for reforming the national competition law, based on the Act against Restraints of Competition,[85] with the major objective of safeguarding competition in the digital age.[86] The European Commission pursues the same ob-

82 This has already been argued by Max Planck Institute for Innovation and Competition, Position Statement on Data Ownership and Access to Data (16 August 2016), paras 32–38 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2833165> accessed 31 August 2020; Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertization and Access' (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 257, paras 123–51. A similar conclusion was reached in the more recent analysis of the independent Special Advisors to the EU Competition Commissioner. See Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the Digital Era – Final Report' (2019) 8–9 and 98–107 <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf> accessed 31 August 2020.

83 Crémer, de Montjoye and Schweitzer (n. 82).

84 See, for Germany, Heike Schweitzer, Justus Haucap, Wolfgang Kerber and Robert Welke, 'Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen' (29 August 2018) <www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&v=15> accessed 31 August 2020; for the UK, Jason Furman, Diane Coyle, Amelia Fletcher, Derek McAuley and Philip Marsden, 'Unlocking Digital Competition – Report of the Digital Competition Expert Panel' (March 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 31 August 2020 (so-called 'Furman Report'). See also the Australian Competition & Consumer Commission (ACCC), 'Digital Platform Inquiry – Final Report' (June 2019) <www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf> accessed 31 August 2020.

85 *Gesetz gegen Wettbewerbsbeschränkungen* (*GWB*).

86 See the Bill of the Federal Government for the reform of the German Act against Restraints of Competition: Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz) (9 September 2020) <www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&v=6> accessed 15 September 2020.

jective by making first steps for preparing legislation on a 'New Competition Tool' ('NCT').[87]

After analysis of the current EU framework for data access based on Article 102 TFEU, the following analysis will show that the envisaged reforms of German and EU competition law indeed have the potential of enhancing the availability of access claims as regards data generated by connected devices. Yet these reforms would still fail to provide for sufficient data access for users of connected devices because of inbuilt limitations of the competition law framework.

1. Limitations of current EU competition law

Article 102 TFEU provides for a duty to provide access to data under the condition that such a refusal to grant access to data constitutes an abuse of market dominance. Against the backdrop of existing case law, the benchmark for showing that there is dominance of a data holder as well as an abuse in such case is particularly high and fraught with uncertainties.

As regards the first requirement, European courts have confirmed dominance based on the control of information, especially in *Magill*.[88] In this case, complainant Magill sought access to the programming information of the three broadcasting organisations active in the Republic of Ireland and Northern Ireland (RTP, BBC and ITV), which was indispensable for Magill, an independent publisher, to enter the market with comprehensive TV guides. In this situation, it was not possible to consider the programming information held by the different broadcasting organisations as substitutes, as Magill was in need of the programming information of all channels to enter the market. Hence, the correct market analysis has to lead to assuming the existence of three separate upstream markets for complementary programming information in which all three broadcasting organisations individually held monopoly positions.

In other cases of the modern digital economy, however, the situation may be much more complex. In a world of big data, data analytics and artificial intelligence, data are often multi-functional. Therefore, control over

87 European Commission, Inception Impact Assessment – New Competition Tool (NCT) (4 June 2020), <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/new_comp_tool_inception_impact_assessment.pdf> accessed 31 August 2020.

88 Joined Cases C-241/91 P and C-242/91 P *RTE and ITP v Commission* (*'Magill'*) [1995] ECR I-743 = ECLI:EU:C:1995:98, para. 47.

large datasets can provide great economic power in multiple markets. Conversely, extending economic activity to multiple markets increases the ability of digital businesses to predict customer preferences with much higher precision. This explains why especially the Internet platform economy is characterised by conglomerate firm structures. This is also relevant in the IoT context. To sell connected devices is just an additional strategy for the large Internet platform operators, such as Google or Amazon, to increase their knowledge about customer preferences. Due to the potentials of data to provide economic power across very different markets, the focus of the traditional competition law assessment on relevant markets and, subsequently, on market dominance is increasingly being called into question.[89]

Moreover, in the modern data economy, not all cases where an undertaking seeks data access are as clear as in the case of *Magill*, where the complainant depended on access to very specific programming information held by the broadcasting organisations. In the modern data economy, finding out about the utility of large datasets is often of essence for the undertaking seeking data access. In such an environment, where the utility of the data is not that clear, proving market dominance based on data control has to become more difficult.

In an IoT environment, where connected devices collect data through sensors, the petitioner for data access also needs to show that the same data cannot be collected from alternative sources. This leads to the question of how to understand the concept of sole-source data in an IoT context. While it is true that, for instance, connected vehicles of various manufacturers could in principle collect the same information by 'observing' the outside world, the situation of the user of a connected device is very different and resembles more the scenario in *Magill*. For overcoming the data lock-in, the user of a connected device depends on access to the first-level data collected by the concrete device. Yet this does not necessarily suffice to consider the de facto holder of these data a data monopolist. The problem is that the market for connected devices can still be quite competitive. This raises the question of how the relevant upstream market should be defined, as the device market or as a much narrower market for individual-level data linked to a concrete device. Accordingly, to confirm market dominance, the petitioner for data access would have to convince the law enforcer of the latter and, hence, an atomised market structure, where se-

89 This is also confirmed by the reform debate in Germany and on the EU level, as will be shown further below.

parate aftermarkets for the machine-generated data for each and every connected device need to be distinguished.

Secondly, EU case law on refusal to deal establishes a high threshold for abuse. Refusal to grant access to data have to be understood as a sub-category of refusal-to-deal cases. EU courts developed the requirements for an abuse in this regard mostly in cases on refusals to license intellectual property rights, including the *Magill* case, where UK and Irish courts, at least at the time of the refusal, considered the programming information to be protected under national copyright law. The *Magill* judgment hence became essential for guiding the development of a European essential facilities doctrine in intellectual property cases. In the more recent case of *IMS Health* of 2004, which has since remained the lead case of the CJEU, the Court stated four requirements for an abuse: (1) access to the subject-matter of intellectual property is indispensable for the petitioner to operate a particular business. (2) The refusal to license the intellectual property results in an exclusion of competition in a secondary market. (3) The refusal prevents the emergence of a new product for which there is potential consumer demand; and (4) there is no objective justification for the refusal.[90]

Already the first requirement of indispensability creates particular challenges in the context of connected devices. In *Bronner*, the CJEU clarified that access to a resource of a competitor cannot be considered indispensable if there are no 'technical, legal or even economic obstacles capable of making it impossible, or even unreasonably difficult' to duplicate the resource.[91] Thereby, the Court demonstrated considerable reluctance to accept the argument of lack of economic viability too easily. The Court stressed that it is not enough to show that duplication of the resource would not be economically viable against the benchmark of the petitioner's scope of business in the secondary market.[92] Rather, the question is whether it is economically viable to create the resource 'for production on a scale comparable to that of the undertaking which controls the existing product or service'.[93] This seems to indicate a standard for indispensability that does not depend on the size of the petitioner's business and that imposes on the petitioner the burden to make the same investment as that made by the dominant undertaking. Whether such test should also be applied with regard to data generated by connected devices remains unex-

90 Case C-418/01 *IMS Health* [2004] ECR I-5039 = ECLI:EU:C:2004:257, para. 38.
91 Case C-7/97 *Bronner* ECLI:EU:C:1998: 569, para. 44.
92 Ibid. para. 45.
93 Case C-418/01 *IMS Health* [2004] ECR I-5039 = ECLI:EU:C:2004:257, para. 28, with reference to Case C-7/97 *Bronner* ECLI:EU:C:1998: 569, para. 46.

plored for the time being. However, it does not make much sense to require an innovative start-up that specialises in data-related services to also enter the market for connected devices to generate its own data to be able to compete in the downstream service market. The *Bronner* test may make sense for the underlying case where a newspaper publisher sought access to the home delivery system of a competitor. Where access to data generated by connected devices is sought, the courts should also take into account the lock-in situation of customers, which excludes market access of competitors.

The second requirement of exclusion of competition in a secondary market identifies the European essential facilities doctrine as one on exclusionary conduct, whereby the dominant firm excludes competitors from a secondary market by refusing access to the indispensable input.[94] Accordingly, both the data holder and the petitioner for data access have to be active in the secondary (service) market. This creates considerable limitations to the application of Article 102 TFEU. On the side of the petitioner, Article 102 TFEU can be considered as a rule for access rights of competitors on which the legislature could further build for legislation on sector-specific data access rights. But Article 102 TFEU does not provide claims for users – private or commercial ones – of connected devices that are not active in a secondary data-related service market.

On the side of the data holder, the *IMS Health* test also fails if the data holder (manufacturer) is not active in the downstream service market. Whether there can be alternative theories of harm for arguing abuse is unclear and even unlikely for the time being. In *IMS Health*, the CJEU held that it 'suffices' for an abuse that said requirements are fulfilled cumulatively.[95] While this could be understood in the sense that the Court would not accept other sets of requirements for an abuse, it has to be noted that the *IMS Health* cumulative test explicitly refers to cases of a refusal to license an intellectual property right, for which the CJEU generally requires the existence of 'exceptional circumstances' to justify a competition law duty to license.[96] Hence, this standard may not apply where no intellectual property rights are at stake. Moreover, in *Huawei*, the CJEU has meanwhile clarified that there can be other 'exceptional circumstances' than those in *IMS Health* that can equally justify a duty to license.[97] In *Huawei*, the CJEU

94 See also Drexl (n. 82) para. 136.
95 Case C-418/01 *IMS Health* [2004] ECR I-5039 = ECLI:EU:C:2004:257, para. 38.
96 Ibid. paras 35–38.
97 Case C-170/13 *Huawei* ECLI:EU:C:2015:477, paras 47–48.

held that there are also exceptional circumstances in the case of (1) a patent which is essential to a standard fixed by a standardisation body, 'rendering its use indispensable to all competitors which envisage manufacturing products that comply with the standard'[98] and where (2) the patent holder has irrevocably committed to the standardisation body to license on fair, reasonable and non-discriminatory (FRAND) terms.[99] It is quite surprising that the CJEU, in *Huawei*, did not transfer the requirement of exclusion of competition to this new set of exceptional circumstances. However, it would go too far to take it for granted that the CJEU would also apply Article 102 TFEU to cases where the holder of a standard-essential patent (SEP), without being active in the downstream device markets, seeks injunctions against an implementer.[100] In formulating the first element of the *Huawei* exceptional circumstances, the CJEU has at least indicated that only implementers that are 'competitors' of the patent holder can rely on these circumstances. Moreover, at least as part of the reasoning, the CJEU identified competitive harm in terms of exclusion, stating 'the fact that the patent has obtained SEP status means that its proprietor can prevent products manufactured by competitors from appearing or remaining on the market and, thereby, reserve to itself the manufacture of the products in question'.[101]

Against the backdrop of the current case-law, this would mean that also refusals to grant access to data where the de facto data holder and the claimant for data access are not competing in any downstream market, a violation of Article 102 TFEU could only be argued in terms of exploitative abuse. However, such claims are equally unlikely to be successful given the problems of assessing the value of data as a benchmark for the appropriate price for granting data access.[102]

As regards the third requirement of the prevention of a new product (so-called 'new product rule'), the General Court clarified in its *Microsoft* judgment that it only applies where the refusal relates to the licensing of

98 Ibid. para. 49.

99 Ibid. para. 51.

100 However, such extension is to be advocated especially for the use of SEPs on mobile telecommunications standards in an IoT context where it becomes increasingly less likely that the holders of such SEPs will also be manufacturers of all kinds of connected devices in which the standard is implemented. See Beatriz Conde Gallego and Josef Drexl, 'IoT Connectivity Standards: How Adaptive is the Current SEP Regulatory Framework?' (2019) 50 International Journal for Intellectual Property and Competition Law 135, 147–51.

101 Case C-170/13 *Huawei* ECLI:EU:C:2015:477, para. 52.

102 See also Drexl (n. 82) para. 138.

an intellectual property right.[103] Hence, the benchmark for a competition law intervention will be higher where use of data by another person requires the licensing of intellectual property rights. Still European courts have so far left open whether a refusal to grant access to data that are protected as trade secrets also requires the application of the new product rule. Therefore, also from a competition law perspective, it is important that the Commission has now announced a review of the intellectual property systems as regards their impact on data access and use.[104]

Finally, the competition law framework does not necessarily provide the best institutional framework for the enforcement of data access rights. Where the law is enforced by competition agencies, enforcement of Article 102 TFEU only works retroactively by reacting to infringements in the past. In addition, competition law investigations and proceedings on unilateral conduct often take many years, even more so where decisions are subsequently appealed to the courts. In addition, lack of access to data generated by connected devices has the potential of becoming a mass phenomenon that can hardly be addressed effectively by competition agencies. Therefore, especially sector-specific enforcement, which can provide for ex ante regulation, and private enforcement should be the preferred options. Of course, the prohibition of abuse of market dominance under Article 102 TFEU is directly applicable and, therefore, can in principle be enforced by private law courts in the Member States. However, as the analysis shows, application of Article 102 TFEU requires a complex economic assessment of the relevant market and dominance and is fraught with many limitations and uncertainties that could easily deter private parties from going to court.

2. *Proposals for reform of German competition law*

The process of legal reform of competition law in view of the digital economy is most advanced in Germany. There the Federal Ministry for Economic Affairs and Energy published a Ministerial Draft Reform Bill in January 2020.[105] Subsequently, in September 2020, the Federal Government

103 T-201/04 *Microsoft* [2007] ECR II-3601 = ECLI:EU:T:2007:289, para. 334.

104 European Commission, 'A European strategy for data' (n. 1) 13.

105 Referentenentwurf des Bundesministeriums für Wirtschaft und Energie – Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB-Digitalisierungsgesetz) (24 January 2020), <https://www.bmwi.de/Red

adopted the Bill on the 10th reform of the Act against Restraints of Competition to be submitted to the German legislature.[106] Several elements of the Bill, though more broadly reacting to the challenges presented by the digital economy, are capable of promoting data access with regard to connected devices.

The least revolutionary proposal relates to the prohibition of abuse of market dominance and the German essential facilities doctrine as enacted in Section 19(2) No. 4 Act against Restraints of Competition.[107] While the current provision is limited to a refusal to grant access to a dominant undertaking's network or infrastructure facility, the proposal would expressly extend this clause to a refusal to grant access to data. Yet such reform would only amount to a clarification of the already existing legal framework, according to which a refusal to grant access to data could already be considered to be illegal under the general prohibition of abuse of market dominance, of which Section 19(2) No. 4 only provides one example.[108] Nonetheless, it is important to note that the explanatory memorandum of the Bill explicitly refers to the situation of a provider of secondary services relating to the use of a device, such as maintenance or repair services, where the service provider cannot enter the secondary market because the dominant undertaking refuses to provide access to data.[109] However, in conformity with the current application of Article 102 TFEU to such cases, the application of Section 19(2) No. 4 of the Act is and remains restricted to cases of exclusionary abuse, i.e. cases where the undertaking seeking data access is a (potential) competitor of the data-controlling dominant firm. The provision does and will not provide a claim in favour of undertakings as mere users of connected devices.

In addition, Section 19(2) No. 4 of the Act would continue to require a showing of market dominance of the de facto data holder. Yet, based on Section 20(1) of the Act, German law has a long tradition of also protecting the competitive process in cases of mere 'relative market power' ('*rela-*

---

aktion/DE/Downloads/G/gwb-digitalisierungsgesetz-referentenentwurf.pdf?__blob=publicationFile&v=10> accessed 31 August 2020. An unofficial English translation is available at <www.d-kart.de/wp-content/uploads/2020/02/GWB10-Engl-Translation-2020-02-21.pdf> accessed 31 August 2020.

106 Gesetzentwurf der Bundesregierung (n. 86).

107 English translation of the current Act available at <www.gesetze-im-internet.de/englisch_gwb/englisch_gwb.pdf> accessed 31 August 2020.

108 This clarifying function of the proposal is also highlighted in the explanatory memorandum of the Bill; see Gesetzentwurf der Bundesregierung (n. 86) 79.

109 Gesetzentwurf der Bundesregierung (n. 86) 83.

tive Marktmacht') below the threshold of market dominance. This puts German law in a much better position to use competition law as a legal basis for data access rights, where a showing of market dominance can be particularly burdensome. In addition, Section 20(1) is traditionally mostly enforced by private law courts. Another particularity of Section 20(1) is that it is not limited to protecting competitors. Rather, the provision specifically pursues protection in the vertical dimension, i.e. in favour of suppliers and purchasers. Therefore, in contrast to Section 19(2) No. 4 of the Act, Section 20(1) can in principle also be relied upon by undertakings as mere users of connected devices that seek access to data where the refusal to grant access results in unfair impediment to conducting a business or discrimination in the sense of Section 19(2) No. 1.[110]

The Reform Bill seeks to clarify the application of Section 20(1) of the Act as regards data access and, moreover, to extend its scope of protection beyond SMEs. Section 20(1) of the Act defines 'relative market power' as dependence 'in such a way that sufficient and reasonable possibilities of switching to other undertakings do not exist'. Already from this wording it should be clear that the concept of 'relative market power' should also be applicable in cases of data lock-ins. To confirm this explicitly, the Reform Bill proposes the introduction of a new paragraph 1a stating that dependence also exists where an undertaking depends on access to data to conduct its business. The explanatory memorandum of the Reform Bill distinguishes two scenarios of refusals to grant access to data where the rule could apply. The first scenario relates to the relationship between undertakings along the value chain where imbalances of bargaining power prevent sufficient access to data.[111] In this context, the explanatory memorandum explicitly mentions that a refusal to grant access may especially prevent an undertaking from switching to competitors in downstream service markets.[112] This shows that paragraph 1a could particularly be used by the users of connected devices to switch providers of secondary services. The second scenario regards the horizontal cases of data dependence of competitors that so far have not entertained a commercial relationship with the data holder. While not excluding intervention, the Bill states that assessment of the unfairness of the refusal to grant access requires particular scrutiny in these cases. The reason is that German case-law has been very

110 Legally, Sec. 20(1) extends the application of Sec. 19(2)(a), providing for an example of abuse, beyond market dominance to undertakings with relative market power.

111 Gesetzentwurf der Bundesregierung (n. 86) 93–94.

112 Ibid. 94.

reluctant to apply Section 20(1) in cases where the parties have so far not entertained any commercial relationship. In contrast, paragraph 1a would at least go further by explicitly confirming that a refusal to grant access to data can in principle also constitute an unfair impediment to conducting a business where the parties have no prior commercial relationship.[113]

As regards the personal scope of protection, the Draft Reform Act proposes to delete the general limitation of the application of Section 20(1) to SMEs. Thereby, the Bill acknowledges the modern view that the provision addresses a general problem for the competitive process and should therefore not be devised as a remedy that is only available to smaller undertakings.[114] Equally, the explanatory memorandum to the Reform Bill argues that even larger undertakings may depend on smaller operators of platforms that act as gatekeepers in the digital economy.[115] Still, the provision is planned to maintain an explicit requirement of a 'significant imbalance' ('*deutliches Ungleichgewicht*') of power between the parties as part of the concept of relative market power.

The most revolutionary and certainly contentious proposal of the Draft Reform Act concerning the digital economy relates to an additional prohibition in the area of unilateral conduct that addresses abuses of a new category of undertakings, namely, 'undertakings of paramount significance for competition across markets'.[116] The proposal seeks nothing less than to prevent undertakings in the digital economy from tipping markets in such a way that competition is gone for ever. In particular, control over large bulks of data can help digital firms to leverage market power in multiple markets. To preserve competition in such an economy, the newly proposed Section 19a of the Act is specifically designed and most likely to be applied to the operators of Internet platforms rather than to traditional device manufacturers that produce and sell connected devices.

However, it has to be taken into account that platform operators such as Apple, Google and Amazon are also active in IoT-related device markets (Apple's mobile devices, Amazon's home assistant Alexa) or reach out to control data collected by connected devices (such as Google's Android op-

113 Sentence 2 of proposed Sec. 20(1a).

114 Regierungsentwurf des Bundesministeriums (n. 86) 81. Explicitly taking up the arguments of Schweitzer and others (n. 82) 57.

115 Ibid.

116 In German: '*Unternehmen mit marktübergreifender Bedeutung für den Wettbewerb*'.

eration system and Google apps).[117] For these undertakings, connected devices are yet another means for collecting and controlling even more data that can be used for strengthening their position in multiple markets. While Section 19a is not specifically providing for data access rights, the provision contains several aspects that are directly related to data access. On the one hand, access to data is proposed as a criterion for the *Bundeskartellamt*, the German competition agency, to assess whether an undertaking can be qualified as one of paramount significance for competition across markets.[118] On the other hand, Section 19a is also proposed to vest the agency with the power to prohibit conduct that impedes access to data. More specifically, the provision empowers the agency to prohibit the undertaking from 'making the interoperability of products or services or data portability more difficult and thereby impeding competition'.[119]

3. Discussion on the EU level

While the German reform can inspire many other jurisdictions, there can be no doubt that the digital economy regarding connected devices is particularly in need of a coherent regulatory framework on the EU level. Indeed, following the Report of the independent Special Advisers on competition law in the digital economy,[120] the Commission now seems ready to reform EU competition law. Taking up the initiative for a 'New Competition Tool' (NCT), which pursues the goal of addressing gaps in the EU competition rules as regards their application in digital and other markets, the Commission has now made a first step towards the adoption of a new competition law instrument – most likely in the form of a new regulation – by publishing an Inception Impact Assessment.[121]

This Inception Impact Assessment provides a first impression of what can be expected from future legislation. Although it broadly addresses

117 Google is also collecting health-related data in IoT environments through cooperation with pharmaceutical companies. See the merger Decision of the European Commission of 23 February 2018, Case M.7813 – *Sanofi/Google/DMI JV*.

118 Sec. 19a(1) No. 4 Draft Reform Act.

119 Sec. 19a(2) No. 4 Draft Reform Act.

120 Crémer, de Montjoye and Schweitzer (n. 82).

121 European Commission, Inception Impact Assessment – New Competition Tool (NCT) (4 June 2020), <https://ec.europa.eu/competition/consultations/2020_new_comp_tool/new_comp_tool_inception_impact_assessment.pdf> accessed 31 August 2020.

competition problems in the digital sector, the Assessment also touches upon issues related to connected devices and access to machine-generated data. As regards the analysis of existing competition problems, the Commission highlights a structural lack of competition caused, inter alia, by consumer lock-in and lack of access to data.[122] In addition, the Commission justifies the need for the adoption of the NCT on the EU level with the cross-border nature of 'digitally enabled products and services', concluding that intervention on the national level would not effectively address the competition-related problems.[123]

On substance, the Inception Impact Assessment sketches four options.[124] However, at least two of these options are not likely to address the problem of lock-ins regarding the data generated by connected devices effectively. The reason is that both options – Option 1 with horizontal scope of application, Option 2 by adopting a sector-specific approach – are dominance-based and thereby linked with the prohibition of abuse of market dominance pursuant to Article 102 TFEU. Yet they go beyond this prohibition by allowing for intervention against a dominant firm prior to the infringement of Article 102 TFEU.

Option 3 and 4 – again the one following a horizontal, the other one a sector-specific approach – are designed to address market structure-based competition problems that cannot be addressed effectively so far. The common feature of these two options is that they are related to unilateral conduct without being limited to dominant undertakings. Thus, these options seem to acknowledge the insight that the structure of competition can also be negatively affected by unilateral conduct of firms below the level of dominance. This may open the door to legislation similar to Section 20(1) and future paragraph (1a) German Act against Restraints of Competition relying on the concept of relative market power.[125]

As regards the forms of intervention, the Commission envisages behavioural and structural remedies designed to improve the functioning of markets. Indeed, Options 3 and 4 could therefore provide the framework for legislation that allows for intervention where undertakings refuse to grant access to data, especially if one takes into account that the Commission explicitly identifies lack of access to data as a particular form of structural lack of competition. Given the fact that rules allowing for interven-

122 Ibid. 2.
123 Ibid.
124 Ibid. 3.
125 See at sub-section 2 above.

tion below the level of market dominance are very much alien to the European competition law tradition, such legislation would appear as truly revolutionary. Yet it is too early to judge whether and to what extent the European competition law reform will take inspiration from German law. Yet it should be noted that the independent Special Advisors have recommended the Commission adopting specific competition law-related rules to promote access of users to the data collected by machines to protect competition in aftermarkets.[126]

4. Remaining gaps

The analysis shows that there is a clear need and tendency to extend the reach of competition law below the threshold of market dominance to promote data access for the purpose of overcoming data lock-ins. Therefore, the current reform plans and proposals both on the national (German) and on the EU level should be welcomed. Especially the German reform proposal shows that competition law can also be used vertically in cases of refusal to grant data access to undertakings that are not competing in any market with the de facto data holder. This is part of the German tradition to also address impediments of the ability of suppliers and purchasers to conduct their business where such impediments may produce market foreclosure effects. This tradition is especially suited to promoting data access of users of connected devices to machine-generated data controlled by the manufacturer where the latter refuses data access along the value chain by relying on superior bargaining power.

Yet even the abovementioned reforms would not suffice to provide sufficient data access. This is because competition law remains limited to claims of undertakings, while connected devices are also purchased and used by non-commercial players. Most importantly, this includes consumers, but also non-commercial entities, such as the state. It goes without mentioning that the state in particular is among the most important purchasers and users of connected devices, such as in the context of traffic regulation or systems of smart cities. Of course, as part of its purchasing activity, the state can rely on tenders to guarantee sufficient data access. However, data access rights of the state may also be needed where connected devices are integrated in larger infrastructure networks, such as in the context of smart cities, and the state is not the purchaser of such devices.

126 Crémer, de Montjoye and Schweitzer (n. 82) 10.

In sum, there remains a considerable gap between contract law, including mandatory consumer contract law, and the competition law framework that can only be closed by additional data access rights.

IV. Sector-specific data access rights of competitors

Sector-specific regulation can play a particularly useful role to overcome data lock-ins. As regards machine-generated data, the primary example is the regulation of the repair and maintenance market for motor vehicles. For entering and staying in the market, independent service providers depend on access to the on-board data controlled by the manufacturers. In this case, the access right is not given to the final customer – or user of the vehicle – but directly to the independent service provider.[127] More recent EU legislation provides other examples where data access rights are directly vested in providers of secondary data-related services who would otherwise not be able to provide such services to customers. This includes the right of the providers of digital payment services against banks to claim access to the account data of customers.[128] In a similar vein, European legislation obliges the transport operators to make travel and traffic data available through central access points and establishes a right of providers of (multimodal) travel information services to re-use these data.[129]

Indeed, access rights of (potential) competitors in secondary service markets have particular advantages for consumers and other end-users. For them it suffices that access rights granted to competitors, as well as additional measures promoting the pooling and sharing of data such as in the case of travel and traffic data, will indirectly result in innovative data-based services, more choice and alternative offers. Thus, consumers benefit from more competition in secondary markets without having to enforce access rights before the courts.

Yet sector-specific access rights of competitors also have certain shortcomings: first, while they are useful tools to open up markets for secondary services, they do not help where the user personally wants to connect data

---

127 See Arts 6–9 Regulation 715/2007 (n. 9).

128 Art. 36 Second Digital Payment Services (DPS2) Directive (EU) 2015/2366 (n. 59).

129 See Art. 8 Commission Delegated Regulation (EU) 2017/1926 of 31 May 2017 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide multimodal travel information services, [2017] OJ L272/1.

from different devices and sources in its own organisational sphere without relying on a third-party service. This can be an industrial end-user of machines, a farmer, a city authority or also a consumer regarding the digitisation of a private home. Secondly, even where the user may wishes to rely on services by other firms, these services are less likely to be covered by sector-specific regulation. Finally, from a perspective of economic regulation, data access rights to users are less problematic than access rights of competitors. The reason is that 'vertical' data access rights only increase the utility of the connective devices in the interest of users, while data access rights of competitors necessarily come with the risk of unjustified free-riding on the investment of the data holder. Therefore, access rights of competitors, deviating from the general principle that undertakings should not be forced to deal with competitors in downstream markets, are in need of a particular pro-competitive justification.

The latter concern is also hinted at in the current proposal for a reform of Section 20(1) German Act of Restraints of Competition where the Draft Bill proposes to extend the prohibition of unfair impediment of conducting a business, relying on the concept of relative market power, to data dependence. While the Draft Bill explicitly states that the rule can in principle also lead to data access rights of competitors in secondary markets that so far have not entertained any commercial relationship with the data holder,[130] the explanatory memorandum to the Bill clearly expresses that an unfair impediment should only be confirmed cautiously. Thereby it mentions two possible scenarios for application: first, where the dependent competitor, based on the use of the data, generates significant economic value, and, secondly, where access will prevent excessive concentration in the secondary market.[131] This shows that in principle sector-specific regulation is the better approach to data access rights of competitors, since sector specific regulation is better placed to take into account the conflicting interests of data holders and their competitors in the given markets and to devise more targeted and pro-competitive solutions. In contrast, vesting data access rights in the users of connected devices is another way of safeguarding a pro-competitive outcome, even where the end-user will claim transfer of the data to a provider in a downstream service market. Data access will only be claimed where provision of the service by a competitor increases consumer welfare.

130 See at sub-section III.2. above.
131 Entwurf der Bundesregierung (n. 86) 94.

V. Data access and intellectual property

Data access and use has also moved to the forefront of the intellectual property debate. The reason is that re-use of data can potentially infringe intellectual property rights. This explains why intellectual property regimes need to be adjusted in such a way that they will not unduly restrict access and re-use of data. The major debate has so far concentrated on the introduction of additional exceptions and limitations to copyright protection in the case of text and data-mining.[132]

Yet, even if (new) exceptions and limitations apply, intellectual property law will not be an appropriate tool to provide access to data. The reason for this is that data holders can prevent third parties from gaining access, especially by using technological protection measures even where they cannot claim intellectual property protection. This shows that de facto control over data, combined with contract law allowing for controlled sharing of data with others, can in substance produce very similar results as intellectual property.

Likewise, the assertion that intellectual property regimes can serve the third-party interests in data access better since they provide a legal framework for exceptions and limitations, including compulsory licensing systems, is not convincing either. This argument overlooks the fact that access rights can promote data access against de facto data holders without the need of prior recognition of exclusive data ownership rights.

G. Proposal for an unfair competition law approach to data access

The preceding analysis shows that there is the need for a legal framework that provides a right of access of the users of connected devices to the data generated by these devices. This section will first explain this right as part of the unfair competition law (at I. below). In addition, unfair competition law principles can help structure the legal rules governing such data access rights (at II. below).

132 See Arts 3 and 4 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, [2019] OJ L130/92.

I. Why unfair competition law?

The preceding analysis has shown that both contract law and competition law can contribute to enhancing access of the users of connected devices to machine-generated data. Yet both systems have their inbuilt limitations. Data access rights are needed to overcome a problem of data lock-in that occurs due to an imbalance of bargaining power. In the EU tradition, mandatory contract law and unfairness control of contract terms is only available in the case of B2C relationships, while the imbalance of bargaining power can also affect users that are not consumers. Moreover, users of connected devices cannot necessarily rely on a direct or at least an indirect contractual relationship with the manufacturer as the de facto data holder. While not requiring a contractual relationship, competition law fixes particularly high thresholds for intervention especially on the EU level. Whether future reforms can lower such thresholds still remains uncertain. More importantly, competition law can only support data access of undertakings, excluding claims of consumers and other non-commercial entities.

The unfair competition law approach avoids these limitations. The core of European unfair competition law consists in rules of fair trading that apply outside the realm of contract law and seek to protect consumers in particular.[133] Yet European fair trading law has never been limited to protecting consumers. Already in 1984, at the beginning of European harmonisation in the field, the European legislature adopted rules on misleading advertising that were also designed to apply in B2B relationships.[134] More recently, the EU legislature adopted the Directive on fair trading practices in

133 See Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market, [2005] OJ L149/22.

134 Council Directive 84/450/EEC of 10 September 1984 concerning misleading advertising, [1984] OJ L250/17. In 1997, the European legislature added rules on comparative advertising. See Directive 97/55/EC of the European Parliament and of the Council of 6 October 1997 amending Directive 84/45/EEC concerning misleading advertising so as to include comparative advertising, [1997] OJ L290/18. After the adoption of the Unfair Trade Practices Directive (n. 133), the scope of the Directive on misleading and comparative advertising was limited to the protection of 'traders'. See Art. 1 Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version), [2006] OJ L376/21.

B2B relationships in the agricultural and food supply chain.[135] In general, this shows that EU fair trading rules seek to protect any other trading party, whether this is a consumer or a trader, albeit with partially diverging sets of rules.

In addition, application of EU fair trading law is not limited to the pre-sale advertising stage. Already the Unfair Trade Practices Directive of 2005 extended its scope of application beyond practices concerning promotion to also include the sale and supply of products.[136] For data access rights related to connected devices, the new Unfair Trading Practices Directive in B2B relationships in the agricultural and food supply confirms this approach. While the focus of the Directive is on protecting (upstream) suppliers – including agricultural suppliers in particular – and not (downstream) purchasers (as in the case of the users of connected devices), the Directive is informative for rights of access to machine-generated data because of its particular objective. The Directive is specifically designed to address imbalances of bargaining power in the supply chain that result in practices, including contractual arrangements, that are to the advantage of the trader.[137] In other terms, the Directive seems to respond to situations of 'relative market power' as known from Section 20(1) German Act against Restraints of Competition.[138] Therefore, to define its personal scope of application, the Directive fixes maximum turnover thresholds for the suppliers and minimum turnovers for traders as a proxy for the existence of such imbalance of power.[139] This shows that, while in the German tradition, protection against an imbalance of bargaining power in the supply chain can be located within the competition law framework, unfair trading law may provide the better framework in the EU tradition. The latter has the advantage of protecting consumers too.

Integrating data access rights within the realm of EU unfair trading law, as part of larger unfair competition law, is equally convincing on substance. On the one hand, it is for the manufacturer to decide whether and under what technical and legal conditions the users of connected devices will have access to the machine-generated data. The manufacturer is in

---

135 Directive (EU) 2019/633 of the European Parliament and of the Council of 17 April 2019 on unfair trading practices in business-to-business relationships in the agricultural and food supply chain, [2019] OJ L111/59.

136 See the definition of 'business-to-consumers commercial practices' in Art. 3 lit. d) Directive 2005/29/EC (n. 133).

137 Recital 1 Directive (EU) 2019/633 (n. 135). (Emphasis added.).

138 See at F. III. 2., above.

139 Art. 1(2) Directive (EU) 2019/633 (n. 135).

control of the product design, including the data formats and the digital interfaces, which are key for enabling data access. From a legal perspective, the manufacturer as the de facto data holder can decide on the terms and conditions of data access and use. Conversely, downstream users of connected devices have an interest in making full use of the device, including the use of the data generated by the device. Against the backdrop of the data lock-in, triggered by an imbalance of bargaining power, it is most convincing to regulate the terms and conditions of access and use relying on a fairness standard the application of which will be based on a balancing of the interests involved.

Integrating data access rights of users of connected devices in the legal framework of fair trading law also corresponds to the most recent claim of the European Commission to create additional access rights only 'where appropriate under *fair*, transparent, reasonable, proportionate and/or non-discriminatory conditions'[140] and where such rights respond to a 'market failure … which competition cannot solve'.[141] In this sense, legislation on data access rights of the users of connected devices within the realm of EU unfair trade practices law can be identified as competition-based legislation.[142]

As a side note, integrating data access rights of users of connected devices as part of the law against unfair trading practices and, hence, unfair competition is also important from the perspective of applicable law. Connected devices are sold and used in international markets. Characterisation of such access rights as unfair competition law, pursuant to Article 6(1) Rome II Regulation,[143] leads to the application of the law of the 'country where the competitive relations or the collective interests of consumers are, or are likely to be, affected'. Here, where the allegedly unfair trading practice relates to the sale and supply of a data-generating connected device, the applicable law should be considered the law of the country where the connected device first enters the end-user market under the control of the manufacturer (law of the country of first distribution). Accordingly, where the connected device is resold to another country by a user, the applicable law will not change. This makes the applicable law predictable for the manufacturer and still protects users appropriately.

140 European Commission, 'A European strategy for data' (n. 1) 13.
141 Ibid. 13 note 39.
142 See also the claim for such legislation at Drexl (n. 82) para. 122.
143 Regulation (EC) No. 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L199/40.

II. Legal design of the data access right

Beyond what has just been explained, the unfair trading (unfair competition) law approach also influences the concrete legal design of the right of access to data generated by connected devices. The following principles confirm the use of the concepts as defined at the beginning of this chapter,[144] which is not a surprise since those concepts were defined in the light of the interests involved.[145]

(1) The access right should be designed as a legal and non-waivable claim. Since the access right is supposed to react to an imbalance of bargaining power, waivability or assignability would run counter to the objective of this right.

(2) The access right should cover both non-personal and personal data, since the scope of the right is defined by the end-users' interest to make full use of the connected device and the data it generates. Of course, the data protection rules need to be respected. Where data protection rights of third persons are at stake, the holder of the access right can at best claim access to anonymised data. Whether there is an obligation of the manufacturer to anonymise data and whether the manufacturer can claim compensation for the costs should be considered as part of the fairness assessment of the terms and conditions of data access.

(3) Yet the user should not be entitled to claim access to all, or just any, data generated by the connected device. The user can only claim access to data to the extent that the interest in making full use of the device, including the machine-generated data, justifies such access. This includes the use of the data for maintenance and repair purposes, for connecting the device with other devices or for receiving secondary data-based services from third-party service providers. In the light of such purposes, the data access right should not be limited to 'provided' or 'observed' data; it should also extend to derived and inferred data if justified by the concrete legitimate access interest. In addition, the data do not have to be stored in the device. It is the obligation of the manufacturer, albeit in the light of a balancing of interests, to organise data access in such a way that access is also possible to data stored in other places of a larger digital network, such as on a cloud server.

144 At section B. above.

145 The following legal design was initially produced, and explained in more detail than here, in Drexl (n. 6) 154–65.

(4) Flexibility is needed as regards the definition of the 'user' as the holder of the data access right. As already explained above,[146] this concept should also be defined in terms of the legitimate access interest. This will typically include the owner and user of the device. Yet physical use should not be required. It should suffice that the connected device collects and generates data connected with the person, such as personal data or data related to an asset owned or controlled by this person. The latter would capture the case of a farmer's access to the data generated by a farming machine used on the land of this farmer where the latter neither owns nor actively operates the machine.

(5) The data access right should be directed against the manufacturer, who is able to design the device in such a way that users can access the data. In this sense, the manufacturer can also be considered a de facto data holder. This does not exclude access to data stored on servers and devices of other parties as long as the manufacturer has a legal claim to access the data.

(6) In the light of the access interest and purpose, 'data access' should be understood broadly, as already indicated above.[147] Where the holder of the access right seeks a service to be provided by another person, the holder should also be allowed to claim the direct transfer of data to such service provider according to the model of the data portability right of Article 20(2) GDPR. The law should also allow the user as the holder of the access right to mandate the third-party service provider to seek data access on behalf of the user, which would additionally enhance the effectiveness of the data access right. Depending on the purpose, access can hence mean different things: access to the information purely on the semantic level, portability of the encoded data or even data sharing, which would extend the data access claim to real-time data.

(7) In many instances, implementation of the data access right will require conclusion of a contract – in the form of a data licensing agreement – that specifies the terms and conditions of data access and data use according to the fairness principle. In this context, a major question will be whether the manufacturer should be allowed to claim compensation of the costs of making the data available. This issue can be decided in terms of a general provision stating that access to and use of the data has to be grant-

146 At B. III., above.
147 At B. III., above.

ed on fair, reasonable and non-discriminatory (FRAND) terms.[148] In the context of connected devices, however, remuneration for the use of the data is not necessarily justified since the user of the device has contributed to the generation of the data (as so-called 'co-generated data') and, directly and indirectly, will usually pay a price for the purchase or use of the device. Conversely, the manufacturer is in principle able to factor in the costs for making the data available in the price it charges for the sale (or rental) of the device. Hence, a claim for remuneration or compensation should be considered the exception rather than the rule. This does not have to exclude compensation for specific costs, such as costs for anonymisation of personal data. Another complex issue regards the interest of the manufacturer in protecting its trade secrets. In particular, the access claim may relate to technical information regarding the connected device the secrecy of which the manufacturer has a legitimate interest in preserving. Since trade secrets protection in the EU equally follows standards of fairness as part of the larger law against unfair competition,[149] the integration of the data access right in unfair competition law is additionally suitable to coordinate the conflicting interests.

(8) Finally, there is the need to coordinate the access regime with other fields of the law. This is not only the case as regards systems protecting sensitive – personal and (secret) commercial – data, as already covered above. The most important and still open question is the relationship with intellectual property rights. As explained in earlier writing, potential sui generis database rights could especially undermine the working of the data access regime.[150] While Article 20(4) GDPR gives precedence to the rights of others, not sufficiently making clear whether this also relates to intellectual property rights of even the data controller, over the data portability rights concerning personal data, it is suggested here to provide that the data access right should prevail over such sui generis database rights.

148 Examples can be found in sector-specific legislation on data access rights. See, for instance, Art. 8(4) and (5) Delegated Regulation 2017/1926 (EU) on multimodal travel information services (n. 129). These provisions also allow for a charging of 'reasonable and proportionate compensation'.

149 See Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, [2016] OJ L157/1.

150 Drexl (n. 5) 67–85.

H. Conclusion

Users often have a legitimate interest in gaining access to the data that are collected and generated by these devices. Connected devices are technically designed to operate in larger digital networks. Therefore, to enable users to benefit fully from connected devices, access to the data is essential. Users should be allowed to integrate connected devices in 'their' digital networks and to choose freely among providers of data-based services in secondary markets. Yet the market does not necessarily guarantee that the manufacturers of the devices, who decide on the technical design of their products and terms and conditions of their marketing and use, will voluntarily allow access to the data. They may be tempted to remain in control of 'their' data, which they often consider as business secrets, and they may try to tie additional products and secondary data-based services to the sale of their connected devices. To protect the interest of users and to promote competition and innovation in secondary markets, data access rights are therefore needed where users of connected devices suffer from a potential data lock-in.

The analysis of this chapter shows that the law can make use of various means to promote access to data generated by connected devices. Access rights of competitors in secondary data-based service markets can most appropriately be used in the framework of competition-based sector-specific regulation. In addition, contract law and competition law can also enhance data access of users. In the European context, mandatory contract law and/or fairness control of contract terms constitutes the primary instrument to respond to imbalances of bargaining power. Therefore, contractual access rights appear as an appropriate means for data access, where consumers could rely on a direct, or at least indirect, contractual link with the manufacturers as the de facto data holders. Outside the realm of contract law, competition law can in principle provide for a duty to grant access to data. But the traditional focus of competition law on market dominance and exclusion of competitors as harm to competition considerably limits the availability of competition law remedies in case of refusals of access to data generated by connected devices. While reforms of competition law are now being debated and prepared in this regard, consumers and non-commercial entities will not likely to be able to rely on competition law even in the future. This is why this chapter proposes a third horizontally applicable access regime as part of fair trading law. This additional regime is not proposed as the better alternative to contract and competition law. Rather, these three regimes should be considered as complementary, partially overlapping regimes that can be applied for the same pur-

pose of overcoming potential imbalances of bargaining power resulting in data lock-ins.

Data access rights of users as part of fair trading and the broader unfair competition law should build on a balancing of the legitimate interests of both the users and the manufacturers of connected devices and the fairness principle. Equally, legislation on these rights needs to be embedded in a larger data governance framework, whereby from a regulatory perspective, the privacy interest of data subjects in the protection of personal data and the innovation objective of the intellectual property systems also need to be taken into account. The principles of data access rights presented in this chapter could be implemented in different ways. Horizontal legislation – applicable across different sectors of the economy – could be considered, possibly in the form of another European fair trading directive for the digital economy. Such legislation would provide a generally applicable framework that may prove especially important outside of the realm of sector-specific regulation and help policy makers identify the sectors where data access is particularly difficult.

At the same time, the general principles set out in this chapter could also be taken into account in the framework of sector-specific legislation. It has to be noted that individual sectors are characterised by the use of very different connected devices, such as cars in the mobility sector or smart meters in the energy sector. Different connected devices may justify different rules concerning the terms and conditions of access against the backdrop of the fairness principle. In addition, access to the data of different kinds of connected devices will often be embedded in a different technological context as regards the existence of standards for data formats and APIs as technical preconditions of data access.