GRUR International, 72(2), 2023, 120–135

https://doi.org/10.1093/grurint/ikac107
Advance Access Publication Date: 8 October 2022
Article

WOLFGANG KERBER*

Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives

The EU Data Act proposal (DA) seeks to introduce new rights for the users of internet of things (IoT) devices regarding access, use and sharing of the data generated through their use of these devices. This paper presents the results of a first analysis of the effectiveness of this 'user rights' mechanism from a 'law and economics' perspective. It concludes that the DA will not achieve its objectives of (a) empowering the users of IoT devices (especially the consumers), (b) unlocking large amounts of IoT data for innovation (for IoT-related services and across sectors), and (c) contributing to a fair sharing of the value from the generated IoT data. Although the DA correctly identifies the main problem arising from manufacturers' technical design of IoT devices, which grants them exclusive de facto control over the generated IoT data, its proposals for solving it are not close to being sufficient: (1) The proposed user rights mechanism suffers from manifold serious problems which will make it weak and largely ineffective (insufficient scope of data; lacking technical interoperability; high transaction costs, especially through the need for a negotiated contract with FRAND conditions; unclarity regarding data markets). (2) Also, the option for users to gain more control over the use of the IoT data, which operates through the requirement that the data holders can only use the IoT data on the basis of a contract with the users, will not work due to unsolved serious market failure problems in B2C situations. Therefore, all the rights to use the IoT data will end up with the data holders (and leave the consumers with only these weak user rights). The main reason for this negative assessment of the DA is its overemphasis on the protection of the exclusive de facto control position of the data holders. However, it is very doubtful whether in the case of IoT devices, whose price can cover the costs of data generation, any general incentive problem for investing in data-generating IoT devices exists. Therefore, a far-reaching rebalancing in favor of easier and increased data sharing and user empowerment is necessary, especially for enabling more innovation in the data economy.

I. Introduction

Connected internet of things (IoT) devices that generate data are spreading very fast and will lead to the collection of huge amounts of data. They will be present everywhere in the offline world, and will be an essential and unavoidable part of everyone's private life, of business contexts and of the public sphere. The question of how the governance of this data should be designed, i.e. who has control over this data, who can use it, and who can benefit from its value, is a key policy question for the digital transformation of the economy and society.

This paper presents the results of a legal and economic analysis of the European Commission's 'Data Act' (DA) proposal with respect to the governance of data generated in IoT devices.[1] Other aspects of the DA are not covered.[2] The basic idea of the DA is that the users of IoT devices and other firms should have more access to IoT data, which currently are often under the exclusive control of the device manufacturers. The key instrument of the DA for solving this problem is the introduction of new rights for the users of IoT devices to get access to this data and share it with other firms. This should lead to more empowerment of the users, let them benefit more from additional services and unlock IoT data for innovating firms.

The reactions of academics and stakeholders to the DA proposal are very ambivalent. Although many are welcoming the objectives and the basic approach of the DA, there is an increasing awareness that the DA proposal also entails a lot of difficult problems. In addition to many unclear terms and provisions and concerns about the costs of compliance, open questions about the relationship to data protection and trade secret law and the necessity of such a far-reaching horizontal regulation have been raised. Furthermore, more fundamental questions like who should have control over the generated

* Professor of Economics, School of Business & Economics, University of Marburg, Germany; kerber@wiwi.uni-marburg.de. The paper is based upon presentations in the Special Committee 'Data Rights' (GRUR) on 21 March 2022 and the GRUR Expert Round Table on 18 May 2022 and an earlier working paper (8 April 2022).

1 Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final (23 February 2022).

2 The analysis focuses mostly on c II and c III of the DA. Other problems like 'business to government data sharing based upon exceptional need' (c V) or 'switching between data processing services' (c VI) are not addressed in this paper.

data of IoT devices and who should benefit from them have emerged in this discussion.[3]

This paper intends to contribute to this discussion by providing a preliminary analysis of the effects of the provisions in the DA proposal with respect to its objectives. This entails, in particular, an analysis of how the 'user rights' mechanism as the key instrument of the DA will work, and whether it can be expected to be sufficiently effective for achieving its objectives. However, it also requires a broader critical analysis of the effects of the specific model of the governance of IoT data, which the DA applies and which also includes a strong protection of the position of the data holders (based upon incentive arguments). In that respect and also with regard to other problems, questions about market failures will have to be discussed.

Our analysis will show that the DA attempts to solve the relevant problems, and also that the decision for a more user-centric approach to the governance of IoT data has to be welcomed. However, our results will suggest that the DA proposal in its current form will not sufficiently achieve its objectives, especially concerning consumer empowerment, the unlocking of IoT data for innovation and ensuring fairness in the allocation of value from data. Particularly important is that the key mechanism of data access and sharing rights for users can be expected to be too weak and largely ineffective. Important reasons are a too far-reaching protection of the exclusive control of the data holders over this IoT data, and the lack of addressing key problems of the governance of IoT data, e.g. with respect to the initial contract between manufacturers and users and unsolved market failure problems, particularly in B2C contexts.

The paper is structured as follows: a brief section II will present some background on the governance problems of IoT data and the objectives of the DA. Section III introduces the basic architecture of the DA approach to IoT data with its new user rights. The main section IV provides an analysis of the effectiveness of this user rights mechanism, of the incentive effects on data holders and of the contract between manufacturers and users, before summarizing why the DA can be expected to fail to achieve its objectives. Section V draws some conclusions.

II. Data policy, the main problem of IoT data governance and the objectives of the Data Act

1. Background policy discussions

The following past and current policy discussions are important as background to the IoT governance part of the Data Act:

- In its Communication 'Building a European Data Economy' (2017), the Commission for the first time identified the problem of non-personal data that are not reused and shared enough (especially for innovation) as an important policy issue.[4] This led to the current EU data strategy, with its emphasis on the need for more data access and data sharing, which so far has focused on proposals to support voluntary solutions like the Data Governance Act.[5]
- The Communication of 2017 also addressed for the first time the data governance problem of IoT devices (with its manufacturer vs. user problem), which led to the (later abandoned) proposal of an exclusive IP-like 'data producer right' that would have been assigned to the owner or long-term user of an IoT device. This is also closely linked to the academic discussion about new exclusive rights on machine-generated data.[6]
- Parallel to and independent from this discussion, a very controversial policy debate has emerged since 2015 about 'access to in-vehicle data and resources' with respect to connected cars. Aftermarket service providers and other stakeholders in the emerging ecosystem of connected cars challenged the exclusive control of the car manufacturers over access to the data generated in connected cars, and demanded a regulatory solution for protecting competition, innovation and consumer choice on secondary markets. This problem has not yet been solved.[7]

3 See, eg, Inge Graef and Martin Husovec, 'Seven things to improve in the Data Act' (2022) 3 <https://dx.doi.org/10.2139/ssrn.4051793> accessed 31 August 2022; Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' Study requested by the JURI committee (PE 732.266 – May 2022); Josef Drexl and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)' (2022) Max Planck Institute for Innovation and Competition Research Paper No 22-05 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4136484> accessed 31 August 2022 (hereinafter: 'Position Statement of the Max Planck Institute (2022)'); Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach den EU Data Act: Der Entwurf der Europäischen Kommission' [2022] GRUR 953; Louisa Specht-Riemenschneider, 'Data Act – Auf dem (Holz-) Weg zu mehr Daten-Innovation?' [2022] ZRP 137; Louisa Specht-Riemenschneider, 'Der Entwurf des Data Act', Beilage zu [2022(9)] MMR 809; Moritz Hennemann and Bjorn Steinrötter, 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts' [2022] NJW 2022, 1481; see also the many position papers in the 'feedback' (14/03 – 13 May 2022) for the Commission <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-amended-rules-on-the-legal-protection-of-databases_en> accessed 31 August 2022; see for a first Presidency compromise text of the Czech Presidency, Interinstitutional File: 2022/0047(COD) (12 July 2022).

4 European Commission, 'Building a European data economy' COM(2017) 9 final, 13.

5 European Commission, 'A European strategy of data' COM(2020) 66 final (19 February 2020).

6 See Herbert Zech, 'Daten als Wirtschaftsgut - Überlegungen zu einem „Recht des Datenerzeugers"' [2015] CR 737; Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' [2016] GRUR Int 989; Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertization and Access' (2017) 8 JIPITEC 257. See for a critical discussion of the 'data producer right' 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 of Building the European Data Economy" (2017) Max Planck Institute for Innovation and Competition Research Paper No 17-08 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959924> accessed 31 August 2022 (hereinafter: 'Position Statement of the Max Planck Institute (2017)'), and Wolfgang Kerber, 'Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer, *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2017) 109.

7 See C-ITS platform, Final report, 2016; M McCarthy and others, 'Access to In-Vehicle Data and Resources – Final Report' (May 2017); Wolfgang Kerber, 'Data Governance in connected cars: The Problem of access to in-vehicle data' (2019) 9 JIPITEC 310; Bertin Martens and Frank Mueller-Langer, 'Access to digital car data and competition in aftermarket maintenance market' (2020) 16 Journal of Competition Law and Economics 116.

– A parallel sector-specific discussion exists concerning the access of farmers and other agricultural service providers to the data of smart agricultural machines controlled by a small number of agricultural machine producers.[8]
– For many other IoT devices the problem of data access for enabling aftermarket services (including predictive maintenance) and other complementary services has emerged as an important policy issue as well.[9]
– However, in B2B contexts, and much more generally, problems of insufficient data access (e.g. through 'imbalances of negotiation power') to IoT data have been acknowledged as an important issue, in particularly for enabling more innovation.

2. The main IoT data governance problem

The main problem of IoT data governance, which is also acknowledged as such in the DA proposal, can be explained as follows: the data generated through IoT devices can be personal and non-personal data, and are often mixed sets of both types of data. Whereas the personal data are subject to the EU General Data Protection Regulation (GDPR), for most non-personal data generated by IoT devices no '*de jure*' rights exist. The manufacturers of IoT devices, however, can choose a technical design for their IoT devices that gives them exclusive de facto control over all data generated by the use of the device by the firms or consumers who have bought, leased or rented it. This leads to the problem that (a) the users most often do not get access to the data they have generated with their device, and (b) other firms or non-profit organizations etc. who would like to use this IoT data for providing services (e.g. to the same users) or for innovating new services and products do not get access to this data.[10]

This can lead to the following negative effects:

(1) The manufacturers' exclusive control over the generated data can lead to competition problems on secondary markets (aftermarkets and other complementary markets) by foreclosing independent service providers, which also leads to less choice for users with respect to these services and higher prices.
(2) Particularly important are the manifold negative effects on innovation on these and many other markets through the lack of access to this IoT data due to the manufacturers' exclusive (monopolistic) control over the data.
(3) This exclusive control also gives the manufacturers a monopoly position with respect to using and monetizing this data, i.e. only they (and not the users) can benefit from the value of this data. This raises the issue of an unfair sharing of the value of IoT data.

These problems can emerge both in B2B and B2C contexts, although the severity of the problems and the relevant market failures can differ significantly.[11]

3. The main objectives of the DA regarding IoT data

From the memorandum of the DA, the following four main objectives can be identified and described briefly as follows:[12]

1) Empowerment of consumers and businesses to have more control over the use of their IoT data and to benefit from more, better and cheaper products and services on secondary markets (also through more competition).
2) Making more data available to businesses, especially for more innovation (unlocking the wealth of existing data).
3) Fairness in the allocation of value from data among actors in the data economy.
4) Preserving incentives to invest in ways of generating value from data.

These four objectives will be used in this paper for the assessment of whether the DA can be expected to fulfill its tasks regarding IoT data.[13]

III. Basic architecture of the governance of IoT data in the Data Act

The basic mechanism of the DA for achieving these objectives is the introduction of new non-waivable rights of the users to access and share the data they have generated through their IoT devices (Arts. 4 and 5 DA).[14] The mechanism is the same for consumers and businesses as users of IoT devices (B2C and B2B). With these rights the users can get access to all generated data and can use them for all legal purposes.[15] The user also gets the right to share the generated data with third parties (firms or other actors), who can use this data for those purposes that are agreed upon with the users. These rights, however, cover only the generated data themselves (i.e. the raw data), not derived or inferred data.[16] In the DA it is assumed

8 See, eg, Can Atik and Bertin Martens, 'Competition problems and governance of non-personal agricultural machine data: Comparing voluntary initiatives in the US and EU' (2021) 12 JIPITEC 370.

9 See Rupprecht Podszun, *Handwerk in der digitalen Ökonomie. Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen* (Nomos 2021).

10 See DA, 13, and recital 5; for a brief theoretical analysis of this main problem, see Wolfgang Kerber, 'Data-sharing in IoT Ecosystems and Competition Law: The Example of Connected Cars' (2019) 15(4) Journal of Competition Law & Economics 381, 386-88.

11 Additionally, there are other problems like technical hurdles for data interoperability or legal uncertainty about data sharing (eg with respect to data protection, trade secrets); see Impact assessment report (SWD(2022) 14 final), 7-22.

12 See the following quotations in the Explanatory Memorandum: '[…] aim of ensuring fairness in the allocation of value from data among actors in the data economy and to foster access to and use of data' (DA, 2). 'The proposal will help achieve the broader policy goals of ensuring EU businesses across all sectors are in a position to innovate and compete, effectively empowering individuals with respect to their data […]' (DA, 3). 'Facilitate access to and the use of data by consumers and businesses, while preserving incentives to invest in ways of generating value through data. This includes increasing legal certainty around the sharing of data obtained from or generated by the use of products or related services, as well as operationalising rules to ensure fairness in data sharing contracts' (DA, 3). See also the Impact assessment report (SWD(2022) 14 final), and the press release of the EU Commission (23 February 2022).

13 It is not possible here to discuss these objectives in more detail, and how they can be defined and operationalized clearly.

14 See for another concept of a non-waivable data access right 'Position Statement of the Max Planck Institute (2017)' (n 6) and Josef Drexl, 'Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation' (Bureau Européen des Unions de Consommateurs (BEUC) 2018).

15 See recital 28.

16 See recital 14.

that the manufacturer has designed its IoT product in such a way that it gets exclusive de facto control over all generated data, making it the exclusive 'data holder' of the generated data of the IoT users.[17] However, the 'data holders' do not need to be identical with the manufacturers. Although not explicitly discussed, it seems to be clear that the manufacturer can transfer (e.g. 'sell') this de facto control position to other firms. It is therefore the 'data holder' who has the obligation to make the data available to the user or to share the data with other firms according to the wishes of the users. These rights of the users should enable them to use this data themselves and benefit from services that can be provided through sharing this data, as well as enable other firms to innovate (new products and services). The DA emphasizes that these user rights do not diminish in any way but rather complement the rights of data subjects from EU data protection law regarding personal data.[18] This also may imply that the DA de facto extends these rights on personal data, e.g. with respect to continuous and real-time data access and data sharing (if applicable).[19]

It is important that exercising the rights of the users to share their IoT data with a third party (TP) requires a negotiated agreement between the data holder and the TP about the conditions under which the TP can use this IoT data. This entails the negotiation of fees for the use of the IoT data and of a number of additional conditions, e.g. confidentiality agreements with respect to the protection of trade secrets and technical measures for protecting the data.[20] Therefore, this contract can be interpreted as a 'licensing agreement' between the data holder and the TP. It seems that the users cannot directly share the data with the TP, e.g. by transferring the data they have gotten access to, without a 'licensing agreement' between data holder and TP.[21] The user only seems to have the right to request the data holder to conclude such a 'licensing agreement' with the TP, and it is the user who can decide for which purposes this IoT data should be used by the TP. The purpose in this licensing agreement does therefore depend on the contract between the user and the TP.[22] Although the DA also uses the term 'data portability' in this context in analogy to the data portability right of Art. 20 GDPR,[23] the entire legal architecture of this triangle between data holder, user and TP is very different from the usual notion of a data portability right, due to this negotiated 'licensing agreement' between the data holder and the TP.[24]

An essential part of this user data sharing mechanism in the DA is that the data holders are not free in setting the fees and conditions for making the data available to the TP but have to comply with FRAND conditions ('fair, reasonable and non-discriminatory terms').[25] The fees should serve as 'reasonable compensation' for the data holders. This leads to an upper limit for the fees for the TP but also implies that the DA acknowledges the right of the data holders to get 'reasonable compensation' for the use of the data by the TP.[26] For supporting small and medium-sized enterprises (SMEs), these fees are reduced through limiting them to 'the costs directly related to making the data available'.[27] For settling disputes about the determination of these FRAND terms, the DA introduces a new dispute settlement mechanism.[28]

The DA does not directly address what the manufacturers and data holders can do with the non-personal data. So far the data holders can use their de facto control over the data for using the data themselves or for letting other firms use this data, i.e. selling (the access to) this data on data markets or sharing them with other firms. The DA explicitly clarifies that the manufacturers and data holders do not have 'de jure' rights on this generated IoT data, and also insists that the DA does not confer any new rights on them.[29] However, we will see below that the DA acknowledges the de facto control position of the data holders and protects this position with a number of rules.

Article 4(6) DA stipulates that the 'data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user'. This is a significant statement. It is assumed that an initial contract has been concluded between the manufacturer (or seller) of the product and the user. Although this contract seems to be crucial for the rights that data holders have with respect to their use of the IoT data, the DA does not say much about this contract.[30] From the entire context of the DA, however, it seems that the DA assumes that the users agree in this initial contract that the manufacturers or data holders get all rights to use and commercialize this non-personal data for the entire lifetime of the IoT device (and presumably also to sell this data holder position to other firms). This would imply that the users are left only with the data access and data sharing rights that the DA grants to them in Arts. 4 and 5 (and which the users cannot waive in such a contract). Since the DA is nearly entirely silent about this contract, many open questions remain; we come back to this issue below in section IV.4. Our following analysis is based upon this assumption that the users agree in this initial contract to such far-reaching rights for the data holders, at least in B2C situations.

17 For 'the control that the data holder effectively enjoys, de facto or de jure, over data generated by the product' as the key 'starting-point' of the problem, see recital 5, last sentence.

18 art 1(4) DA; see also recital 7.

19 See recital 31; see for the interpretation 'Position Statement of the Max Planck Institute (2022)' (n 3) para 293.

20 arts 8, 9, 11 DA.

21 The text of the DA is not entirely clear about this.

22 art 6(1) DA.

23 See recital 31.

24 See also 'Position Statement of the Max Planck Institute (2022)' (n 3) para 69.

25 art 8(1) DA and recital 5. It should be noted that these rules are part of c III of the DA, which not only applies to the new user sharing right in the DA but to all situations where a data holder is obliged to make data available to a data recipient through legislation in the EU.

26 art 9(1) DA, and recital 42.

27 art 9(2) DA.

28 art 10 DA.

29 See recitals 5 and 19.

30 See art 3, and recitals 23 and 24.

IV. Effects of the Data Act

This chapter has the task of analyzing the expected effects of the rules in the DA in relation to its objectives. In a first step, the most important provisions of chapter II DA will be analyzed in more detail (section IV.1.); in a second step, these insights will be used toward assessing the expected effectiveness of the data sharing mechanism (section IV.2.). Section IV.3. will critically analyze the effects on the incentives of the data holders, and whether incentive problems justify the approach of the DA. Section IV.4. will address the initial contract between manufacturers and users (especially consumers) and discuss its problems. After a brief discussion of fairness, section IV.5. will summarize the effects on the objectives of the DA.

1. A more detailed analysis of these user rights

A key precondition for the entire user rights mechanism is the obligation of manufacturers in Art. 3 DA to design and manufacture IoT devices 'in such a manner that data generated by their use are, 'by default, easily, securely and, where relevant and appropriate, directly accessible to the user'.[31] This is a far-reaching and potentially burdensome requirement for the technical design of all IoT devices. It is combined with a list of pre-contractual information obligations about the data that are generated: whether they are generated 'continuous[ly] and in real-time'; whether the manufacturer 'intends the use the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used';[32] who the data holder is; and how the user may access the data. It is not clear to what extent these transparency requirements limit the options of the manufacturers (and data holders) to change over time what data is generated, with whom this data is shared and for which purposes it is used. In a dynamic data economy, there is need for some flexibility regarding the generation and use of the data from such durable products as IoT devices. However, there are no rules in the DA on adapting this contract over the lifetime of the IoT device, although we have long-term contractual relationships between manufacturers (data holders) and 'locked-in' users.[33]

Article 4 encompasses the right of users to access and use the generated IoT data. By simple request of the user, the data holder should make the data available to the user 'without undue delay, free of charge and, where applicable, continuously and in real-time'.[34] For what purposes can the users use the generated IoT data? From the text of the DA, the users seem to be very free in terms of how they use the data they get access to. It is only necessary to 'preserve the confidentiality of the trade secrets' (also through technical measures) and respect any rights from EU data protection law with regard to personal data.[35] As to the purposes themselves, there seems to be only one limit: the 'user shall not use the data obtained […] to develop a product that competes with the product from which the data originate'.[36] With regard to the sharing of data with third parties (Art. 5 DA), it is important that the users are not allowed to share this data with firms that have been designated as gatekeepers according to the Digital Markets Act in order not to further increase their economic power through more data.[37]

'*In situ*' access to data: It is particularly important that recitals 8 and 21 emphasize that the data access right of Art. 4 (and also the data sharing right of Art. 5) does not imply that the data holder has to transfer a copy of the data to the user (or the TP) to make the data available. It might be sufficient for the data holder to make the data accessible on a server of the manufacturer or a cloud service provider:

> '[…] may be designed to permit the user of a third party to process the data on the device or on a computing instance of the manufacturer'.[38]

These are so-called '*in situ* data access rights' – with the idea to bring the algorithms to the data instead of bringing the data to the algorithms. In recent policy discussions these '*in-situ* data access rights' have been viewed as an interesting new option for how to implement data access and data sharing.[39] These '*in situ* data access rights' can have considerable advantages with respect to the various risks of data transfers. However, they also imply that the data holders can technically remain in control of the data, and that the solutions for data access and data sharing are no longer linked to a data transfer (as a flow of data) or the option of users (or TPs) to combine them freely and easily with other data. Since it seems that in the DA the data holders can unilaterally decide whether the data are made available only '*in situ*' (and the DA even seems to recommend this solution),[40] this option is a huge step for the data holders concerning how they can protect their control over the generated IoT data. Therefore, it is necessary to analyze more deeply whether and to what extent '*in situ* data access rights' limit the usability and value of the data that are made accessible and shared. This option also requires very sophisticated regulatory solutions for impeding the ability of the data holders to monitor the use of the data by the users and TPs, and use these insights for their competition with users or TPs.[41]

The exclusive control of the data holders over the data is further strengthened in the DA through additional rules such as Art. 5(4) DA ('not deploy coercive means or abuse evident gaps in the technical infrastructure of

31 art 3(1) DA; see also recital 19.

32 art 3(2)(d) DA.

33 For 'lock-in' of the users, see DA, 13.

34 art 4(1) DA; see also recitals 23 and 24.

35 art 4(3) and (5) DA.

36 art 4(4) DA. This seems to be narrowly defined to the IoT device itself, and does not prohibit using the data for competition on aftermarkets, even if the manufacturers also offer those services (see recital 28). For a critical discussion see Leistner and Antoine (n 3) 89.

37 art 5(2) DA and recital 36; see for the problem of data power also below section IV.3.

38 Recital 21.

39 See for the recent discussion on '*in situ* data access rights', eg Bertin Martens and others, 'Towards Efficient Information Sharing in Network Markets' (2021) TILEC Discussion Paper No DP2021-014 <https://dx.doi.org/10.2139/ssrn.3956256> accessed 31 August 2022.

40 See recital 8; for a critical discussion of this option see 'Position Statement of the Max Planck Institute (2022)' (n 3) para 66, and Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3) 816.

41 Perhaps art 4(6) and art 5(5) might be applied to this problem; see also recital 29. For this problem neutral data trustee solutions could also provide good solutions.

the data holder designed to protect the data in order to obtain access to data'). Particularly important is that the 'data holder may apply appropriate technical protection measures, including smart contracts, to prevent unauthorised access to the data and ensure compliance with […] the agreed contractual terms for making data available' (Art. 11(1) DA), and the requirement of data recipients in the case of 'unauthorised use or disclosure of data' to 'destroy the data […] and end the production, offering […] and use of goods, derivative data or services produced on the basis of knowledge obtained through such data' (Art. 11(2) DA). It is important to note that these protection measures do not focus only on the protection of trade secrets but on the generated IoT data themselves. This protection in the DA of the de facto exclusive control over the IoT data by the data holders resembles to some extent the protection of IP rights. We will come back to this issue below in section IV.3.

One of the key questions is for what purposes the users can share the data with TPs. Using this data for aftermarket services for IoT devices and other downstream services directly related to IoT devices seems to be unproblematic and is repeatedly mentioned in the DA. But what about purposes beyond these services? Particularly interesting is whether the purpose in the contract between the user and the TP can also be the 'selling' of the access and use of the data on 'data markets'? This could happen in different forms:

(1) A service provider (e.g. a repair service chain) could get access to the IoT data of consumers as part of the performance of a service but also use this contract to collect and aggregate the data from many of its consumers for developing larger data sets, which could in turn be used in developing new innovations or training algorithms. If this is included in the contract between the consumer and the TP, then this use of the data is part of the purpose.
(2) Another option is that an intermediary collects this data for the purpose of building aggregated data sets through contracts with the consumers directly. The use of these data sets could then be sold to other firms for innovations. Since no direct service to the user is performed, the intermediary may have to offer monetary incentives.
(3) The users could also directly sell the generated IoT data to other TPs on data markets, e.g. also via providers of data intermediation services (Data Governance Act).

According to the text of the DA, much seems to be possible.[42] It is not clear, however, whether the DA intends to go so far. If the DA wants to make much more generated IoT data available – also across sectors – for innovations by other firms (especially startups, SMEs, etc.), then this should be possible. This would lead to much more liquidity in the data markets by increasing the supply. The DA, however, does not mention 'data markets' once, which is surprising if unlocking data for more innovation is a main objective of the DA. But making this data available for data markets might be a problem for data holders, because this can lead to competition on the data markets, which can endanger the profits of the data holders from selling access to the same data.[43] It is therefore an important question that has to be clarified: does the 'purpose' of how the data is used by TPs, which the users can define, also include the option for the users to sell the use of this IoT data on data markets?[44]

2. Effectiveness of the data sharing mechanism?

A key question in the assessment of the effects of the Data Act is whether this user rights mechanism can be expected to be effective in practice. Will it lead to more, better and cheaper services for IoT users (also through protecting and enabling competition on secondary markets), and will it lead to the innovation of many new products and services by making much more IoT data available to innovating firms?

The negative experiences with the data portability right of Art. 20 GDPR, which so far has not fulfilled the expectations of more competition, more innovation and a solution to lock-in problems through lowering switching costs, are well known and also explicitly acknowledged in the DA.[45] Why should this mechanism of user-initiated data sharing work better than Art. 20 GDPR? Important advantages of the 'user rights' in the DA are that (a) the scope of the data also covers 'observed' data; (b) it 'mandates and ensures the technical feasibility of third-party access for all types of data coming within its scope';[46] and (c) it allows for making data available continuously and in real time (Art. 5(1) DA). Therefore, the data sharing mechanism of the DA avoids some of the problems of the data portability right of Art. 20 GDPR. These advantages also refer to personal data, which can be very helpful for mixed data sets. However, there is also a long list of problems that can be expected to impede the effectiveness of this data sharing mechanism.

a) Negotiation problems, obstacles and disputes

A first group of problems relates to the barriers and costs that are caused by the specific rules for using this user rights mechanism: although it is clarified in Art. 5(1) DA that the data holder has to make the data available to a TP 'without undue delay' and 'of the same quality as is available to the data holder', the specific conditions of the

42 See recital 28 ('[…] also stimulate the development of entirely novel services making use of the data, including based upon data from a variety of products and services') and recital 35 (with respect to providers of data intermediation services as TPs).

43 However, the data holder would still get 'reasonable compensation' for such a 'selling' of the data on data markets. It is not clear, however, what it would imply for the 'licensing agreements' between data holders and TP, and for 'reasonable compensation', if selling and reselling of this data would be possible.

44 See for a position that explicitly rejects that the users can use their data sharing right to monetize this data 'Position Statement of the Max Planck Institute (2022)' (n 3) para19.

45 See recital 31 with its comparison of these user rights with the data portability right of art 20 GDPR; see for the problems of the data portability right of art 20 GDPR Jan Krämer, Pierre Senellart and Alexandre de Streel, 'Making Data Portability more effective for the Digital Economy' (2020) CERRE report June 2020.

46 See recital 31.

47 Recital 39 emphasizes very clearly the importance of the 'principle of freedom of contract' in this context.

'licensing agreement' have to be negotiated between the data holder and the TP.[47] These negotiation processes can lead to considerable problems, disputes and costs:

(a) The DA does not clearly define the scope of the data that are covered by the data sharing right of the users. In fact, the covered data might be very narrow, because not only derived and inferred data are excluded but also 'data resulting from any software process that calculates derivative data from such data'.[48] It is not clear what types of generated data remain to be covered, because nearly all relevant generated data are somehow processed data.

(b) The data is also not required to be made available in standardized formats and by using standardized and open technical interfaces. Therefore, ch. II of the DA does not solve the problem of 'data interoperability' with respect to sharing IoT data.

(c) It remains unclear in the DA what 'making available' of IoT data means exactly. This is closely related to the above discussion about '*in situ*' data access.[49]

(d) Another source of disputes will be the question of what data must be made available for the specific purpose for which the data should be used (according to the contract between the user and the TP). Data holders can be expected to try to limit the data made available as much as possible.

(e) Particularly difficult problems will arise with respect to the issue of the protection of trade secrets. This is already one of the big issues in the current discussion about the DA. One of the main problems is that it is very difficult to determine *ex ante*, i.e. before litigation in courts, whether certain data of the data holders are trade secrets. This can lead to the problem that data holders can easily claim, without clarification, that the data that should be shared are trade secrets and require far-reaching confidentiality agreements and technical protection measures. The Commission tries to deal with this problem, but their solution is itself controversially discussed. Important is that the legal uncertainty about trade secret protection and how the DA deals with this problem in its data sharing mechanism can lead to large and difficult-to-solve disputes which can impede its effectiveness considerably.[50] Disputes can also arise with respect to the question of how far-reaching the confidentiality agreements and the technical measures need to be for protecting trade secrets, as well as for the technical protection measures for the data themselves. Another issue regards the specific modalities for '*in situ*' access to the data.

(f) Difficult problems can also arise with regard to personal data and compliance with the GDPR. Legal uncertainty about the delineation between personal and non-personal data and other compliance issues in data protection law can lead to many disputes about the requirements for data sharing agreements as well as to high transaction costs both for data holders and third parties.[51]

(g) The modalities of 'fair, reasonable and non-discriminatory terms' of the licensing agreement can also lead to manifold problems. Whereas, e.g. in the PSD2 and in Art. 20 GDPR it is clarified that, generally, the fee is zero, here the data holder can charge a 'reasonable' fee. It is not hard to predict that it will become one of the most controversially discussed issues in the DA: what is a 'reasonable compensation' and how is it calculated?[52] The experience with FRAND solutions in IP law show the difficulties of such bilateral negotiations.[53]

At first sight, it is commendable that the DA offers a new dispute settlement mechanism.[54] However, this is a voluntary mechanism and only deals with the task of the 'determination of fair, reasonable and non-discriminatory terms'. It does not deal with the other above-mentioned problems like the appropriate scope of the data,[55] trade secret protection (confidentiality agreements), technical measures or the modalities of '*in situ* access' to data. Here, either regular court proceedings are necessary and/or the involvement of the (as yet non-existent) enforcement agencies of the Member States.[56] It is very unclear whether this leads to a fast and effective enforcement.

In sum, this discussion shows that providing access to the IoT data of users might face large obstacles, (transaction) costs (fees, negotiation costs, solving of disputes, technical protection) and delays, which might make this mechanism for third parties potentially very expensive and slow. Data holders might find many ways to make the use of this data sharing right practically hard and therefore unattractive for users and TPs.

b) Limited scope and usability of shared IoT data and lacking technical interoperability as problems for services on secondary markets

A second group of problems relates to the question of how useful this set of generated IoT data is for TPs that want to offer additional services on secondary markets (like repair services) or for new innovations. Two different types of problems can be distinguished:

(a) *Insufficient scope of data*: A big problem will be that the scope of the data that can be made available through these user rights might be too small. Although it also encompasses observed data as well

48 Recital 17; the reason is that 'such software process may be subject to intellectual property rights'.

49 See 'Position Statement of the Max Planck Institute (2022)' (n 3) para 65.

50 See Leistner and Antoine (n 3) 86-88; 'Position Statement of the Max Planck Institute (2022)' (n 3) paras 277-88.

51 It can be expected that the parallel application of the GDPR and the DA on data sharing agreements about IoT data will lead to a lot of so far underexplored problems with regard to the relationship between both legal regimes.

52 Since the incentives for generating data (recital 42) constitute the rationale for 'reasonable compensation', all the problems regarding the existence and extent of incentive problems of data holders (discussed below in section IV.3.) will emerge again in the set of criteria about the calculation of 'reasonable compensation'.

53 See Leistner and Antoine (n 3) 103; more generally, Peter Picht, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, further EU Digital Regulation Acts, and Competition Law' (2022) Max Planck Institute for Innovation and Competition Research Paper No 22-05 <https://ssrn.com/abstract=4076842> accessed 31 August 2022.

54 art 10 DA.

55 For extending the dispute settlement mechanism also to the scope of data, see Graef and Husovec (n 3) 3.

56 art 31 DA.

as non-personal and personal data and allows for continuous and real-time access, the exclusion of all inferred and derived data can lead to a data set that might be much too narrow to enable TPs to offer additional services to the users like repair or predictive maintenance services on downstream or adjacent markets of other new IoT-related services. For many of these services, it is not sufficient to have only access to raw data; processed, inferred and derived data might also be necessary.[57] Often it will also be necessary that the TP not only has access to the individual data of the user but also to aggregated IoT data from many users (for innovation or providing a high-quality service). As already discussed below, it is unclear whether and to what extent TPs can build up aggregated IoT data sets with this user rights mechanism. It is also hard to see how with this user rights mechanism large data sets can emerge which are suitable for training algorithms.

(b) *Lacking technical interoperability*: Another important problem is that for many aftermarket and other complementary services for IoT devices, it is necessary for the TP to also have technical access to the IoT devices, i.e. access to proprietary tools and software is needed for the provision of the service. The DA only deals with data access problems, not with technical interoperability. Many IoT devices are designed by the manufacturers as technically closed systems with no technical interoperability. In all of these cases, repair and other complementary services cannot be offered to the users by TPs, even if they would get access to sufficient data.[58]

The example of connected cars: These two types of problems can be shown in the example of access problems with regard to connected cars. In the EU the car manufacturers use the so-called 'extended vehicle' concept, which leads to their exclusive control over (a) all data generated by the connected cars, and (b) the technical access to the car (closed system with no interoperability). This ensures that the car manufacturers have a gatekeeper position for the ecosystem of connected driving with regard to all markets on which services are provided that require either access to the generated car data or technical access to the car. The reason is that without a contract with the car manufacturers, independent service providers cannot offer their services on these secondary markets to the car users. This leads to negative effects on competition, innovation and consumer choice on the secondary markets.[59] How would the DA help to solve these problems? The DA would only allow the car users to share the raw data that are generated in connected cars with independent service providers. In this example, it is clear that access to this data would not be sufficient, e.g. for repair and maintenance service providers, and it also would not offer a solution for technical interoperability. Article 5 DA is therefore not a suitable solution. Hence it is not surprising that the Commission has started a policy initiative for an additional sector-specific regulation for ensuring 'access to vehicle data, functions and resources' that is intended to complement the horizontal DA. This sector-specific regulation would focus primarily on solving these two types of problems, namely sufficient access to vehicle data and to technical functions and resources of connected vehicles.[60]

Overall, due to an often too narrow scope of this data set and no provisions for solving problems of technical interoperability, it is very doubtful whether this data sharing right of Art. 5 can really help independent service providers offer their services to the users or develop new innovative services on secondary markets.[61] In addition, even if independent service providers can offer these services, it is unclear whether due to all the obstacles and costs of this mechanism undistorted competition (a level playing field) can be ensured between the services offered by the TPs and competing services by the manufacturers. Without enabling and protecting effective competition on secondary markets, the DA will not achieve its objective of facilitating more, better and cheaper services for the users.[62]

c) Conclusions

Due to this long list of problems, the entire mechanism for sharing IoT data via requests of the users might be a very weak and largely ineffective mechanism. This might lead to the danger that only a very limited amount of data will be made available to independent service providers and innovating firms. This again implies that the benefits for the users of IoT devices from this data access and sharing rights might remain very limited, leading to the problem of very low incentives for using these rights. The situation might perhaps be better in B2B than B2C contexts, but this would require a much deeper analysis.

The effectiveness of this user rights mechanism could increase if (1) the scope of the non-personal data covered by the DA would be broadened, and if it would be clarified that the data sharing right of the users could also be used for 'selling' access to this data to TPs (e.g. data intermediaries) who could aggregate this data and 'sell' the use of these data sets on free data markets, and if (2) these user rights were combined with a much more clearly regulated approach with respect to the scope of

57 Regarding the problem of the scope of data, see Leistner and Antoine (n 3) 14-16, 84; 'Position Statement of the Max Planck Institute (2022)' (n 3) paras 20-25.

58 Therefore, demands have been made that the provisions about data and technical interoperability in ch. VIII DA should also be extended to data access and data sharing of IoT data. See, eg, Leistner and Antoine (n 3) 117, and 'Position Statement of the Max Planck Institute (2022)' (n 3) para 66. However, mandating technical interoperability can also lead to trade-offs with product differentiation and innovation (Wolfgang Kerber and Heike Schweitzer, 'Interoperability in the Digital Economy' (2017) 8 JIPITEC 39, 42).

59 See Kerber, 'Data Governance in connected cars: The Problem of access to in-vehicle data' (n 7) 316-25 (with a market failure analysis).

60 See Public consultation on the revision of the vehicle type-approval (Regulation (EU) 2018/858) with regard to access to in-vehicle generated data for the purpose of providing vehicle-related and mobility services <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Access-to-vehicle-data-functions-and-resources_en> accessed 31 August 2022, and for a discussion of solutions as submission to this Public consultation Wolfgang Kerber and Daniel Gill, 'Revision of the vehicle type-approval regulation: Analysis and recommendations' (21 June 2022) <http://dx.doi.org/10.2139/ssrn.4174028> accessed 31 August 2022.

61 It would be necessary to analyze empirically for all the relevant IoT devices, whether, eg, repair and maintenance services are technically possible with the sharing of this set of generated IoT data.

62 See DA, 13, and recital 28.

data, fees, contracts, processes of data sharing (e.g. initiation through third parties), technical protection measures, etc., which could significantly reduce transaction costs and mitigate disputes. This, however, would require a much higher level of regulation, and a regulator who can make decisions about these issues.[63] The other option is to complement such a weak data sharing mechanism with a larger number of additional sector- or ecosystem-specific regulations which can solve these problems in a much more targeted way, also by additionally using direct access rights of other firms to data, functions and resources of IoT devices (as discussed in the example of connected cars). This is linked to the discussion about the advantages and problems of horizontal vs. sector- or problem-specific solutions for the governance of data and IoT devices.[64]

3. Effects on data holders and the incentive problem

A key role for the basic architecture of the Data Act is played by the incentives for manufacturers and data holders for investing in data-generating IoT devices and extracting value from the data. One of the strengths of the DA is that it tries to balance the effects of these new user access and sharing rights for unlocking data for innovation with these incentive effects for manufacturers. However, this section will show that for the generated data of IoT devices these incentive arguments are unclear and questionable. They do not justify the far-reaching protection of the exclusive de facto control position of the manufacturers and data holders, and the high hurdles for the sharing of IoT generated data (see sections IV.1. and IV.2.). In section IV.3.a) it will be argued why – despite these additional data access and sharing rights of users – the DA can be seen as a legislative act that might strengthen the exclusive de facto control of manufacturers over the generated IoT data, and might lead to a de facto introduction of IP-like exclusive positions over non-personal data. Section IV.3.b) will show why, with respect to IoT data, such a general incentive problem that would justify an exclusive position of data holders does not exist. After explaining additional potential negative effects of such de facto IP-like exclusive positions on IoT data (section IV.3.c)), far-reaching conclusions are drawn that question basic assumptions of the architecture of the DA.

a) Strengthening the exclusive de facto control of data holders over IoT data: Does the DA introduce an IP-like 'exclusive position' over non-personal data?

The thesis that the DA strengthens the de facto control over IoT data by (large) data holding companies seems to be in direct contradiction to what the Commission seems to intend by introducing the additional access and sharing rights of users. Yet the following reasons make it likely that the position of data holders will be strengthened:

(1) So far, the manufacturers and data holders have a de facto exclusive control position over all IoT data and – with respect to the non-personal data – can use this data as they wish, e.g. for monetizing it in order to increase their profits. Although it is true that these new user rights theoretically would limit this exclusive control by the data holders, their position is not much endangered due to the weakness of this user rights mechanism.[65]

(2) In section IV.1., we already have seen that the DA wants to strengthen the protection of the data of the data holders with a number of specific rules in a way that resembles to some extent the protection of IP rights. The contracts between the data holders and TPs are close to licensing agreements with far-reaching protections that allow the data holders to keep the exclusive control over the data ('*in situ*' access, technical protection measures and additional rules like Art. 11(2) DA). However, from an economic perspective, the decisive point is: as long as the data holders can protect their exclusive de facto control over the data by technological measures, this exclusive control position is economically to a large extent equivalent with being granted legal exclusive IP-like rights on this data. Therefore, the data holders do not need 'absolute rights' ('*inter omnes*') for this data, as long as they have exclusive control over this data through technological measures.[66]

(3) Most important, however, is that with the DA the legislator would, for the first time, decide that such a de facto control position over this non-personal data, and the ensuing de facto possibilities for how to use the data, may be justified and therefore also politically and legally recognized as legitimate. So far, the data holders have only a de facto 'power' position that they have won through a specific technical design of their IoT device. Whether this exclusive 'de facto control' over the data (and its implications) should be recognized by the society is an open legal and political question which has not been decided yet.[67] The DA would give legitimacy to this exclusive de facto control over the data, and therefore would de facto introduce a protection of this data, which has similar economic effects as an IP-like exclusive right. This would be a very significant political and economic success for data holders.[68] From this perspective, the data holders would get much more from the Data Act than the users with their de facto weak user rights.

63 So far, data access and portability solutions have only worked well if they were combined with 'thick' regulation like, eg, the PSD2 (opening bank account data) and the old phone number portability in telecommunication regulation.

64 See Wolfgang Kerber, 'From (Horizontal and Sectoral) Data Access Solutions Towards Data Governance Systems' in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data Access, Consumer Interests and Public Welfare* (Nomos 2021) 441.

65 See the last section (IV.2.) and the following section (IV.4.) about the initial contract between manufacturers and users.

66 See Wolfgang Kerber, 'Specifying and assigning "bundles of rights" on data. An economic perspective' in Franz Hofmann, Benjamin Raue and Herbert Zech, *Eigentum in der digitalen Gesellschaft* (Mohr Siebeck 2022) 151, 162.

67 ibid 176.

68 See also Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3) 810.

(4) The justification for such a strong protection of the IoT data of the data holders in the DA is the argument that this is necessary for 'preserving incentives to invest in ways to generate value through data'.[69] This fits perfectly to such an IP interpretation of the rules for protecting the data of the data holders: the rationale for the exclusive rights in IP law (patent, copyrights) has always been the need to give incentives for investing into the 'production' of innovations and creative works. However, such an IP rationale for an exclusive monopolistic position for non-rivalrous intangible goods has also always implied the need for a proper balancing between the necessary incentives and the benefits of a broad use of such a non-rivalrous good.[70] Therefore, it is necessary to analyze this incentive problem in a deeper way.

b) To what extent do manufacturers have incentive problems for generating and collecting IoT data and extracting value from them?

It is very surprising that the EU Commission emphasizes this incentive problem so much in the DA. In the entire discussion about IoT devices there have been no concerns or any evidence for an underinvestment in IoT devices, or that manufacturers would not use enough sensors, microphones or cameras when designing their IoT devices (or not collect enough data with them). On the contrary, there is a broad consensus in the discussion that the use of IoT devices will continue to spread fast in all types of situations, and that the generated and collected IoT data will increase exponentially in the foreseeable future.[71]

It is true, however, that far-reaching obligations for opening privately held data (for giving other firms or public institutions access to this data) can have negative effects upon the incentives for the generation of data. It is therefore appropriate, in cases of mandatory data access and sharing solutions, to carefully investigate the implications for the generation of data. Since the beginning of this discussion, it has been emphasized that the costs of collecting data can be very different: collected data can be a mere by-product of other activities (with very low costs of data collection), whereas for other data much higher investments in data generation might be necessary. Due to the different costs of data collection, a proper balancing between ensuring sufficient data collection incentives and the benefits from making the data available to other firms (e.g. for innovation) will lead to very different results as to whether rules for mandatory data sharing should rather favor an easy and cheap sharing of data or put the focus more on the need for incentives. Therefore, a 'one-size-fits-all' approach is not appropriate, which means more differentiation is needed.[72]

What can be said specifically about the incentives for data generation and collection regarding IoT devices in the context of the DA? This would certainly require deeper analyses of the different types of IoT devices. However, the following general arguments seem to be relevant for all IoT devices:

(1) *User rights*: The 'user rights' of Arts. 4 and 5 DA refer only to the generated IoT data themselves (i.e. the raw data) but not to derived and inferred data. This implies that the incentives for investments of the data holders for extracting value from the collected data are not undermined by these rights, because the data holders do not have to give access to or share the derived and inferred data or other insights from analyzing this data. What is changing, however, is that other firms also get the chance to analyze the generated data, i.e. the user rights might lead to competition regarding extracting value from the data, with manifold positive effects on innovation (if the user sharing rights mechanism would work well).

(2) *Users are paying a price for the IoT device*: However, most important is that in most cases the users have bought the IoT devices and are therefore owners of these devices. Independent of the legal question of whether it is at all legally allowed that the owner of a device does not have access to and control over the data that are generated by her own use of her device,[73] the user as owner has bought the device from the manufacturer and therefore has paid a price, which on well-functioning markets incentivizes the manufacturer to offer products that are attractive for the users. If consumers and business users would like to have an IoT device which collects and processes certain data, because this increases their benefits from these devices, then the users are certainly willing to pay their share of the investments that the manufacturers have to make to develop and produce these data-generating IoT devices. If data generation through additional sensors is benefitting the users, then manufacturers have sufficient incentives for investing in the sensors of these IoT devices and the systems for processing this data. It might well be that the costs of setting up and running these systems are large, but no reason can be seen from an economic perspective why these firms cannot include these costs into their calculation of the price for this IoT device (as they also include many other costs they bear). Therefore, it is not clear at all why there should be a general incentive problem for investing in data-generating IoT devices, because the price for the IoT device can include these costs.[74,75]

(3) *Generating data that do not benefit the users*: The incentive problem might be different for those data generated and collected through the IoT device which do not increase the benefits for consumers. Without additional incentives, manufacturers might not invest

69 DA, 3.

70 See Kerber, 'Specifying and assigning "bundles of rights" on data. An economic perspective' (n 66) 164.

71 See Sector inquiry into consumer Internet of Things. Final report, COM(2022) 19 final, 2.

72 See, eg, Heike Schweitzer and others, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen* (Nomos 2018) 161 and 171; Jason Furman and others, 'Unlocking digital competition. Report of the Digital Competition Expert Panel' (March 2019) 75 <https://nottingham-repository.worktribe.com/OutputFile/3958107> accessed 31 August 2022.

73 This can be puzzling for non-lawyers.

74 From an economic perspective this is not different in the case of leasing or renting the IoT device.

75 This is even true for the additional costs of the manufacturers and data holders that are caused by the new user access and sharing rights. They too can be covered by the price of the product.

into the generation and collection of this type of data. Allowing the manufacturers (and data holders) to get exclusive control over all data generated by the IoT device and to use this data would then lead to large incentives for generating and collecting many additional IoT data that do not benefit the users any more, but can serve as additional sources of revenue for the data holders.[76] Then the economic rationale in the market for the design of IoT devices changes to generating as much data as possible, and not how to design the device to the benefit of the consumers or business users. This might raise serious concerns about the implications for the protection of privacy of consumers (and also the 'privacy' and trade secrets of business users) and lead to fears that IoT devices might evolve into 'spying or surveillance devices'.[77] It is not clear whether the DA also wants to incentivize the generation and collection of such additional data, which are not necessary for the functionality of the IoT devices.[78] Since the DA proposal would set incentives for the generation of such IoT data, these potentially controversial issues should be discussed carefully. It might also lead to additional arguments for the need for more empowerment of users regarding meaningful control over what types of data are collected by their IoT devices and how this data is used (see section IV.4.).

c) Potential negative effects of strengthening the exclusive de facto control over IoT data for competition and innovation through larger data power and data concentration

Strengthening exclusive de facto control positions of data holders increases the dangers of data monopolization, the emergence of gatekeeper positions in IoT-related ecosystems and, generally, larger data concentration and data power. The negative effects of the exclusive control of manufacturers over the generated IoT data on competition in aftermarkets and other downstream markets of IoT devices are already directly acknowledged in the DA, because solving these problems is one of its stated objectives.[79] However, additionally, more problems can emerge. The possibility of manufacturers to sell their data holding position (and therefore the data streams from their IoT devices) can lead to the emergence of specialized large data companies who build up entire portfolios of data streams from different IoT devices, combine them (also with other data) and extract value from these huge sets of data.[80] This can lead to entirely new forms of data concentration and data power in the digital economy, with potentially unforeseen positive and negative effects.[81]

It is particularly possible that the large gatekeeper companies (as defined in the DMA), whose economic power is already based upon their huge data power, could also get control over many data streams from IoT devices by buying the data holder position from IoT device manufacturers (or making exclusive contracts with them about the use of this data). It is surprising that in the DA the users of generated IoT data are not allowed to share their data with gatekeeper companies benefitting from additional services, but there are no limitations for manufacturers and data holders on selling access to this data or even the entire data holder position to large tech companies like Amazon, Google or Apple.[82] Therefore, the strengthening and legitimization of the exclusive control position of data holders over IoT data can also benefit the large tech firms by allowing them to increase their data power, which also could be used for manifold strategies with negative effects on competition and innovation.[83]

d) Conclusions

(1) Taking into account incentives for data generation regarding IoT devices is important from an economic perspective. However, these few reflections have already shown the complexity and dubiousness of this incentive argument.[84] Since users pay a price for the IoT device, it is not clear why the incentives for investing in the generation and collection of data should be too low, as long as the data increase the benefits of the users from these devices.[85] Although it cannot be excluded that specific incentive problems can emerge in certain situations or regarding certain types of data, the assumption in the DA of a general incentive problem with respect to IoT data is simply wrong.

(2) Therefore, the DA places too much weight on this incentive argument in the balancing between data holders and TPs who want to use the data for providing services to the users or for the innovation of new services. The DA should attach much more

76 This is very close to the well-known problem that platforms collect a lot of data from users which are not necessary to improve the services themselves, but allow the platforms to make additional profit (eg through targeted advertising).

77 This will be particularly problematic due to the ubiquity and unavoidability of data collection by IoT devices in the future.

78 In the Impact assessment report (SWD(2022) 14 final), statements can be found that might suggest such an interpretation: 'The Data Act's general aim is to maximize the value of the data in the economy and society by ensuring that a wider range of stakeholders gain control over their data and that more data is available for use, while maintaining incentives for data generation and collection' (ibid 26).

79 It is the exclusive de facto control of the car manufacturers over the generated car data that leads to its gatekeeper position in the ecosystem of connected driving (see section IV.2.b)).

80 Such specialized data companies can also emerge through the aggregation of IoT data via the new user rights of the DA, if this mechanism would work well.

81 From an economic perspective this 'tradability' of IoT data streams can also have many positive effects for the creation of value from data.

82 See again art 5(2) DA and recital 36, in which it is also clarified: 'This exclusion of designated gatekeepers from the scope of the access right under this Regulation does not prevent these companies from obtaining data through other lawful means'. For critical discussions of art 5(2) DA see 'Position Statement of the Max Planck Institute (2022)' (n 3) para 92.

83 Neither the DMA nor traditional competition law is well-suited for dealing with such forms of data concentration.

84 This problem is certainly more complex than described here; it will be important to analyze these incentives in much more detail from an economic perspective.

85 This also can have far-reaching implications for the calculation of 'reasonable compensation' in art 9 DA, because compensation is only necessary as far as an incentive problem exists. Therefore, demands to eliminate the 'reasonable compensation' for generated IoT data can find support from an economic perspective. See for such a demand 'Position Statement of the Max Planck Institute (2022)' (n 3) para 72 (also based upon the argument that the price can cover these costs) and also Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3) 823.

weight to the benefits of making them widely available. Establishing a much less restrictive regime for 'unlocking' this IoT data with less obstacles and costs of data sharing would have manifold positive effects on innovation, competition and benefits for users without endangering the incentives for the generation of IoT data.

(3) The tendency of the Data Act to acknowledge and legitimize the de facto exclusive control position of manufacturers (and data holders) over the generated IoT data through this incentive argument might have potentially far-reaching, long-term negative effects for innovation in the entire data economy. The DA should be very cautious not to introduce (intentionally or unintentionally) a 'de facto' (not: 'de jure') 'exclusive position' on IoT data, which resembles (with respect to its economic effects) an exclusive IP-like right on non-personal data.[86] The DA should also not appear to make a first important step into such a direction. From this perspective, it is also problematic that the DA seems to encourage the manufacturers to design their IoT devices in a way that gives them exclusive control over all generated IoT data.[87]

4. The key role of the initial contract between manufacturer and user

So far we have not properly considered the initial contract between the manufacturer (seller) and the user of the IoT device. The DA clearly states that the data holders can only use any non-personal data of the IoT device on the basis of a contractual agreement with the user.[88] This would imply that the de facto control position of the data holders over the generated IoT data itself would no longer be sufficient to allow the data holders to use the data for themselves (e.g. for improving the IoT device) or for sharing it with others (e.g. for money). All these uses would need a contractual agreement with the user. This is a significant legal change from the current situation, where the data holders need consent for processing personal data but not for the use of non-personal data. It is surprising that this legal change is not directly discussed in the DA. Less surprising is that this contract has emerged as one of the key issues in the discussion. In the DA, however, the Commission reassures the manufacturers that 'the limitation of the manufacturer's […] freedom to contract and conduct a business [through these new rights of the users] is proportionate and mitigated by the unaffected ability of the manufacturer […] to also use the data, insofar it is in line with the applicable legislation and the agreement with the user'.[89] Therefore, the DA seems to assume that the data holders can expect to have the same possibilities for using and monetizing the data as before, except for the limitations through the new non-waivable user rights of Arts. 4 and 5 DA.

Since there are only a few pre-contractual transparency requirements in the DA,[90] it can be assumed that otherwise there is freedom of contract between the manufacturer and the user.[91] However, the entire reasoning of the DA seems to assume that the users will accept a contractual agreement in which the users agree that the manufacturer can use all generated non-personal IoT data for all kinds of uses, including selling them and extracting value from them (and also transferring the data holding position to other firms). Since IoT devices both in B2C and B2B contexts are usually sold on markets with competition between IoT device manufacturers, it is unclear why the DA assumes without any discussion such an asymmetric allocation of the rights for using the IoT data as the expected outcome on these markets. Why is it not discussed that (a) the users could also be paid directly for allowing the data holders' use of the data or that (b) the contract could also encompass terms that the data should not be used for certain purposes (e.g. targeted advertising) or (c) not be shared with certain types of firms (e.g. Google or Facebook)? This would imply that the users can also make granular choices about how the data holders use their IoT data. Why is it assumed that the contract about the use of the IoT data is valid for the entire lifetime of the IoT device, cannot be terminated (locked-in user) and is not limited?[92]

From an economic perspective, it can be expected that in many B2B situations negotiations will take place about the questions of whether and to what extent manufacturers (and data holders) get rights to use the generated IoT data by way of such contracts. In many instances the users will demand far-reaching exclusive control over this IoT data, and this can be efficient; or they might agree that both of them can use the data. One important option is that in the sales contract of a smart machine the buyer as user also gets the de facto control position over the data, i.e. that the user itself is the data holder. Therefore, in B2B contexts – depending on economic conditions, competition and negotiation power – very different allocations of such rights to use the IoT data can be expected; and in most cases, such B2B agreements based upon freedom of contract will lead to efficient (and also fair) solutions. In B2B contexts such asymmetric allocations of the rights to use the data, in which the user will only have the user rights of Arts. 4

86 See als Specht-Riemenschneider, 'Data Act – Auf dem (Holz-)Weg zu mehr Daten-Innovation?' (n 3) 137.

87 We should not issue such 'blank cheques'. Instead, the development of other data governance models for IoT devices, which do not rely on 'exclusive de facto control' over the generated IoT data, should also be encouraged.

88 art 4(6) DA.

89 DA, 13.

90 See again art 3 and recital 24.

91 See for an explanation of this contract Dirk Staudenmayer, 'Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz' [2022] EuZW (forthcoming).

92 Although in recital 24 the DA explicitly clarifies that this 'Regulation should not prevent contractual conditions, whose effect is to exclude or limit the use of the data, or certain categories thereof, by the data holder', this looks more like a reference to exceptional cases. For demands regarding the collection of non-personal data, limitations of the use of this data by the data holder and of the duration of the contracts, see Verbraucherzentrale Bundesverband (vzbv), 'Verbraucher:innen beim Data Act im Blick behalten' (13 May 2022) 13 <https://www.vzbv.de/sites/default/files/2022-05/22-05-13_vzbv-Stellungnahme_Data-Act.pdf> accessed 31 August 2022.

and 5 DA, might be more the exception than the regular case.[93] It cannot be seen that we have a pervasive market failure problem in B2B situations.

This can be very different, however, in B2C contexts. If consumers buy a connected car, smart home devices, fitness trackers or smart watches, etc., it can be expected that they have the same information and behavioral problems with the non-personal data that they have already had for a long time with respect to 'notice and consent' solutions regarding their personal data.[94] Consumers will not read and understand long contracts about the use and sharing of this data, and do not know the value of this data. It can thus be expected that they agree to all terms and conditions when buying the IoT device. The manufacturers (or sellers) will therefore not offer different options for granular choices about the use of this data, leaving the consumers only with the choice of either buying the IoT device and accepting the exclusive use of this data by the data holders or not buying it at all ('take it or leave it'). Due to these information and behavioral problems of the consumers (and perhaps also deceptive and manipulative behavior of the sellers), it cannot be expected that competition might work sufficiently to make these rights to use the data a relevant parameter of competition between the manufacturers of IoT devices (in a similar way to how competition usually does not work with respect to privacy-friendly terms regarding personal data).

The Data Act does not address (or at least discuss) this expected market failure of information and behavioral problems of consumers with regard to the use of non-personal IoT data in the initial contract between manufacturers and consumers.[95] Only the above-mentioned pre-contractual transparency requirements in Art. 3 can be interpreted as an additional consumer protection measure. It is surprising that the DA entails a number of provisions that have the explicit task of protecting the users against exploitation through TPs regarding the sharing of user data (against coercing, deceiving and manipulating the users, also through 'dark patterns', as well as against 'profiling' the consumers),[96] whereas no such consumer protection measures exist for the much more important initial contract between manufacturers and users, which decides the entire allocation of the rights for the use of generated IoT data over a long period of time. Therefore, the DA seems to assume that 'freedom of contract' is working with regard to this contract, although at the same time the DA itself expects – as described above – that the consumers accept such 'buy-out' contracts, in which the data holders get all the rights for using the generated IoT data and the consumers are only left with the non-waivable user rights of Arts. 4 and 5 DA.

This contract is 'the elephant in the room' of the Data Act. On the one hand, the provision that data holders can only use the data if this use is based upon a contract with the users is theoretically a big step for the empowerment of consumers with respect to their IoT data, because without their consent the data holders cannot use them. On the other hand, the DA does nearly nothing to help the consumers use this theoretically strong position for exercising more control over their IoT data, e.g. for determining how data holders can use the data or for getting a share of the revenues that data holders generate through extracting value from this data or monetizing them on data markets. Helping to solve this market failure problem would be a big contribution to the empowerment of consumers, but the DA grants the consumers only these weak access and sharing rights for their generated IoT data. In addition to decisions on how data holders can use the generated IoT data, consumer empowerment could also imply more control over what data are generated with the IoT device, e.g. also with respect to data that are not necessary for the functionality of the device.[97] In the current version the DA does little to enable consumers to make meaningful decisions about the data generated by their use.

Another main problem with this contract between data holder and user is that it also might not be a good solution to replace the exclusive control of the data holders with the exclusive control of the users, if we take into account the objective of unlocking non-personal data for innovation. It is not clear whether users, and especially consumers, are in the best position to make this data sufficiently available to other service providers and innovators, although data intermediaries and data markets might provide much help in that respect. Therefore, the question emerges how more consumer empowerment can be combined with the objective of making more non-personal data available for innovation. One approach could be that both the data holders and the users could use and even monetize the generated IoT data independently from (and in competition with) each other, i.e. that both actors would have rights to use these IoT data to a certain extent (e.g. for specific purposes) also without an agreement between them. This would limit the key role of this initial contract between data holders and users for the use of the data. It is not possible to analyze and discuss here the

93 It is not easy to explain why in the DA in B2B situations only the users get rights to access and share the IoT data but not the manufacturers. In B2B contexts manufacturers can also be dependent on the buyers of their IoT devices, and therefore might not get even access to IoT data for improving their own device. This can happen, eg, to manufacturers of IoT devices that are used as components in other products, eg connected cars. Here, a non-waivable right of the manufacturers for using this data might be an interesting solution. The fairness provisions in B2B relationships in c IV of the DA will not help in these cases. See for the problem of component providers Federation of German Industries (BDI), 'Statement. EU Data Act Proposal' (13 May 2022) 12 <https://english.bdi.eu/publication/news/eu-data-act-proposal-digital-transformation-data-use/> accessed 31 August 2022.

94 See as overviews OECD, 'Consumer Data Rights and Competition – Background note' (29 April 2020) 35-37 <https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf> accessed 31 August 2022; Erika Douglas, 'Digital Crossroads: The Intersection of Competition Law and Data Privacy' (2021) Temple University Legal Studies Research Paper No 2021-40 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880737> accessed 31 August 2022; see with regard to the DA Podszun and Pfeifer (n 3) 960; Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3).

95 It also cannot be found in the impact assessment of the DA. In Staudenmayer (n 91) it is confirmed that the DA intentionally leaves it to the market. One small exception in the DA is recital 25, in which for the specific case of agricultural data (smart agriculture) it is admitted that 'contractual agreements might be insufficient to achieve the objective of user empowerment' with the consequence of recommending the granting of 'granular permission options'. This recital questions indirectly the entire 'freedom of contract' approach with regard to these contracts.

96 art 6(2(a) and (b) DA; see also recitals 34 and 35.

97 See for an analysis of this market failure problem and possible consumer protection solutions (like avoiding buy-out contracts) Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3) 816-20.

manifold ways how such an approach could be designed, and how the interests of data holders, users and third parties/innovators could be balanced in an appropriate way. However, these discussions show that we might need a more sophisticated approach to the specification and assignment of rights for the use of generated IoT data than basing it mainly on a contractual arrangement (with freedom of contract) between data holders and users, as in the DA proposal.[98]

5. Effects of the Data Act on fairness: a few remarks

The DA does not discuss or explain what its objective of 'fairness in the allocation of value from data among actors in the data economy' means. Likewise, this paper will not try to do this.[99] From our discussion in the last section (IV.4.) it follows that in B2C contexts it can be expected that – due to the very asymmetric allocation of the rights to use the IoT data between data holders and consumers in the initial contracts – nearly all of the value of the generated IoT data will be allocated to the manufacturers and data holders, and only a small share of this value will accrue to the consumers (via their presumably weak and ineffective user rights). A particularly strange specific result regarding fairness is that if users are sharing their IoT data, e.g. with a repair service provider, to benefit from their user rights, they have to pay for their own data because the service provider, who has to pay 'reasonable compensation' for using this shared data to the data holder, will include these fees into its price for the service.[100] Overall, it is very unclear why the Commission thinks that such an asymmetric distribution of value from IoT data in B2C contexts should be deemed fair.

The situation might be different in B2B situations because here no pervasive market failures can be identified. It is, however, also up to discussion whether the specific rules of Art. 13 DA against unfairness of contractual terms in data sharing between businesses with respect to SMEs can solve fairness problems with respect to the allocation of value from data between such firms.[101]

6. Summary: failure of the DA proposal to achieve its objectives

The analyses in section IV lead to the conclusion that it has to be expected that the DA proposal of the Commission will not achieve its objectives:

(1) *Empowerment of consumers and business users*: Due to this weak 'user rights' mechanism and the unsolved market failure problems with regard to the initial contract, the empowerment of consumers with regard to making decisions about their IoT data is very limited. It is also very doubtful whether consumers and business users will benefit much from additional, better and innovative services and from lower prices through more competition, e.g. on aftermarkets.

(2) *Making more IoT data available for businesses, especially for innovation*: Through the presumably very ineffective data sharing mechanism of the users it also cannot be expected that the DA will lead to the 'unlocking' of large amounts of data for enabling more data-driven innovation, especially also across sectors. In particular, it is not clear how this mechanism enables third parties to get access to large aggregated data sets, or would lead to additional supply of IoT data to data markets.

(3) *Fairness in the allocation of value from data among actors in the data economy*: It cannot be seen that the DA contributes in any significant way to this objective.

(4) *Preserving incentives to invest in ways of generating value from data*: From an economic perspective it is very unclear whether a general incentive problem and therefore a danger of underinvestment in the generation of IoT data exists. Therefore, the strong emphasis on the exclusive de facto control of the data holders over the generated IoT data in the DA is not justified. It leads to the danger of an over-protection of this data with negative effects on competition, innovation and the users of IoT devices.

V. The Data Act proposal: some conclusions and recommendations

It has to be welcomed that the Commission is trying to address the large unsolved problems regarding the governance of IoT data. The Commission has correctly identified the exclusive control of manufacturers (data holders) over IoT data as the key problem for the lacking data access of IoT users and for the insufficient availability of data to innovating firms. Therefore, the objectives of unlocking more IoT data for innovation and giving the users, especially the consumers, more access to and control over the IoT data that they are generating with their devices (consumer empowerment) are particularly important. Also, fairness with respect to the allocation of the value of the IoT data among the actors of the data economy is a highly relevant (albeit difficult) objective. Very important is also that the Commission rejects the approach to grant exclusive rights of access and use of non-personal data, and emphasizes that 'a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use'.[102] From an economic perspective the Commission

98 For a broad discussion about this contract with very different suggestions, see, eg, Leistner and Antoine (n 3) 92-95, 'Position Statement of the Max Planck Institute (2022)' (n 3) paras 44-54; Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3) 816-20.

99 See for recent discussions of fairness in the Digital Markets Act Wolfgang Kerber and Louisa Specht-Riemenschneider, 'Synergies Between Data Protection Law and Competition Law' (*verbraucherzentrale Bundesverband*, 30 September 2021) 65-67 <https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf> accessed 31 August 2022.

100 This might be an additional reason to question or limit the payment of 'reasonable compensation' by TPs to the data holder.

101 See art 13: unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise.

102 Recital 6. For the approach of using a 'bundles of rights' concept to analyze very different models of governance of data as such a 'general approach', see Kerber, 'Specifying and assigning "bundles of rights" on data. An economic perspective' (n 66).

is also right to apply a comprehensive concept of governance of IoT data, which tries to balance (a) benefits of unlocking data for more services, competition and innovation and (b) more consumer empowerment with an alleged need to provide enough incentives to manufacturers (data holders) for investing in the generation of IoT data. The problem, however, is that the basic architecture and the concrete design of the DA proposal does not constitute a proper balancing between these objectives, leading to the negative assessment regarding the fulfillment of its objectives.

What are the reasons for this failure? Most important is that the key problem of the exclusive control of the manufacturers over the generated IoT data is not solved through the provisions of the DA. Due to the weakness and ineffectiveness of the user rights mechanism and the lack of solutions for the market failures regarding the initial contract for the use of IoT data by the data holders, the exclusive position of the data holders over the IoT data will remain largely intact, with only very limited effects for empowering the consumers and a failure to unlock large amounts of IoT data to enable more services and innovation through third parties. It is not clear whether the overly strong protection of the data holders' exclusive position over IoT data is the result of a wrong (over-optimistic) assessment of the effectiveness of the proposed user rights mechanism or whether this result is intended because the Commission thinks that the incentive problems of the manufacturers (and data holders) regarding investment in generating IoT data are so large that such nearly exclusive monopolistic control over this data is necessary.[103]

In section IV.3., our analysis showed that it is very doubtful that any general incentive problem for generating IoT data exists, because these costs might be covered by the price of the IoT devices. However, without a large incentive problem, an optimal balancing between the objectives would favor the unlocking of data for innovation much more strongly and ease any concerns about a larger control of the users over this data. It also would call into question the need for the negotiated agreements between data holders and third parties (including 'reasonable compensation') and the high hurdles and technical protection measures regarding the shared data, which contribute to the presumably low effectiveness of the user right-based data sharing mechanism in the DA. Therefore, a substantial and far-reaching rebalancing of the DA is necessary, from the protection of data holders to the empowerment of the users (especially consumers) and, in particular, to the objective of unlocking IoT data for innovation.

This article has focused on the analysis of the effects of the DA proposal of the Commission. It does not discuss policy recommendations and possible amendments, although the results indicate the main problems that should be dealt with. In addition to those, a few other suggestions should also be made for the policy discussion:

(1) It is necessary to have a much clearer analysis of the market failure problems with regard to the governance of IoT data, and what the effects of the proposed solution in the DA would be. This has not been done in a sufficient way. Much more (including economic) research is necessary here.
(2) Such an analysis would clearly show that the data governance problems of IoT devices are very different between B2C and B2B situations. Therefore, it can be suggested that the DA might need (perhaps very) different solutions for B2C and B2B, and that a uniform solution (as in the current proposal) will fail to lead to effective and proportionate results in both types of situations.[104]
(3) It is surprising that the DA assumes that the data governance model, in which the manufacturers get exclusive control over the IoT data, is the 'natural' model, and therefore solutions can only be sought in such additional access and sharing rights, which only try to limit this de facto exclusivity position but do not challenge or prevent it: why should manufacturers not design and sell IoT devices which directly give the users control over the generated data? Why should the data that are generated by IoT devices not be entrusted to a neutral data trustee that grants access to and shares the IoT data according to fair and non-discriminatory terms with different stakeholders?[105] For more user empowerment and innovation, it might be very important to also develop and encourage data governance solutions for IoT devices which avoid using the 'exclusive de facto control' position of data holders as an essential element of the solution, because it is exactly this element that causes the access problems for users and innovating firms.
(4) All these arguments strongly suggest that we should be very cautious that the DA does not prescribe overly uniform and harmonized solutions for the governance of IoT data. Since it is already clear that the DA will have to be complemented with a number of sector-specific regulations for better-targeted and more effective regulatory solutions, the DA should not limit the scope for such solutions too much. In a similar way, it is also

103 Another possible interpretation could be that the Commission also pursues with the DA industrial policy objectives by supporting (large) European manufacturers of IoT devices. If this is the case, it would be helpful for the discussion to be transparent about it.

104 See for the complex data access problems in B2B situations within 'larger, multipolar networks' Leistner and Antoine (n 3) 75, and regarding the differences between B2B and B2C situations ibid 77-81.

105 See also Specht-Riemenschneider, 'Der Entwurf des Data Act' (n 3) 819. In the policy discussion about data in connected cars, these alternative solutions have been discussed. It was shown why they could be superior to the 'extended vehicle' concept of the car manufacturers, which is close to the model that the Data Act is favoring. See the TRL study (n 7), Kerber, 'Data Governance in connected cars: The Problem of access to in-vehicle data' (n 7), and for a recent discussion of alternative governance models for the mobility data of connected cars (with a specific emphasis on data trustee solutions) Louisa Specht-Riemenschneider and Wolfgang Kerber, 'Designing Data Trustees – A Purpose-based Approach' (Konrad Adenauer Stiftung 2022) 53-73 <https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees.pdf/3523489b-2611-a12a-f187-3e770d1a9d94?version=1.0&t=1647261611824> accessed 31 August 2022.

very important that the DA does not unduly pre-empt the scope of the Member States to develop and experiment with new, innovative (and so far unknown) data governance solutions, e.g. also with respect to data trustee solutions and public interest considerations.

ACKNOWLEDGEMENTS

I would like to thank, in particular, Daniel Gill, Rupprecht Podszun, Louisa Specht-Riemenschneider, Herbert Zech, Annika Stöhr, Bertin Martens, Peter Picht, Matthias Leistner, Josef Drexl and many others for valuable feedback on earlier versions and many insights from discussions.