(Version: 8 April 2022)

Governance of IoT Data:
Why the EU Data Act will not fulfill its objectives

Wolfgang Kerber*

Abstract: The EU Data Act proposal intends to introduce new rights for the users of IoT devices for access to and sharing of the data (with third parties) that are generated through their use of these devices. This paper presents a first, preliminary analysis of the effectiveness of this "user right" mechanism. Its result is that under the proposed rules this mechanism for data access and data sharing can be expected to be weak and largely ineffective, i.e. the DA will not achieve its objectives of empowering the users regarding their IoT data, making much more data available for innovation, and a fair sharing of the value from the generated IoT data.

The DA correctly identifies the main problem that the manufacturers can get through their technical design of the IoT devices exclusive de facto control over the generated IoT data. The proposed "user rights" mechanism, however, suffers from serious problems: (1) Insufficient scope of data and lacking technical interoperability, which will not enable the provision of many services (or ensure competition on aftermarkets). (2) Many hurdles and high transaction costs through the need for a negotiated contract between data holder and third party with negotiated FRAND access, technical protection measures, and the option to only offer "in-situ" access to the shared data. (3) It is unclear to what extent the "user rights" mechanism can be used for making more data available to data markets. It can be expected that users will get only limited benefits from these rights, and no significant stream of data will be "unlocked" for innovation.

The main reason for these weak user rights mechanism is a very restrictive set of rules in the DA for data sharing that protect the exclusive de facto control of data holders and tends to lead to a IP-like protection of the data. The DA is justifying and legitimizing this protected exclusive control of IoT data with the argument of preserving incentives for generating IoT data. However, such a general incentive problem does not exist, because, e.g., IoT devices with data-generating features are sold and users have paid for them. Linked to this problem who has control over the IoT data and benefit from them is another key issue. Although the DA stipulates that data holders can only use the generated IoT data on the basis of a contract with the users, it does not help to empower the users (particularly the consumers) to use this theoretically strong position for exerting meaningful control over the use of their IoT data. Instead, the DA seems to assume and accept that all the rights of using their generated IoT data are ending up with the data holders. leaving consumers with only these weak user rights. Such a market outcome suggests serious market failures.

The Data Act proposal raises serious fundamental issues that need much deeper analysis and discussion, also on a political level.

Key words: Data Act, Internet of things, data access, data sharing, data governance

JEL classification: K11, K21, K24, L86, 034

---

* Professor of Economics, School of Business & Economics, University of Marburg, kerber@wiwi.uni-marburg.de. The paper is based upon a presentation in the Special Committee "Data Rights" (GRUR) on March 21, 2022. I want to thank, in particular, Daniel Gill, Rupprecht Podszun, Louisa Specht-Riemenschneider, and Herbert Zech for valuable feedback on a first draft, as well as the participants of the Special Committee "Data rights" and many others, with whom I could discuss the Data Act, for very helpful insights.

1. Introduction

Connected IoT devices that are generating data are spreading very fast, and will lead to the collection of huge amounts of data. They will exist everywhere in the offline world, and will be an essential and unavoidable part in the private life of everyone, in business contexts, and in the public sphere. The data generated by IoT devices will be at least as important as the data collected through digital platforms. The question of how the governance of these data will be designed, who has control over these data, who can use them, and who can benefit from the value of these data, is a key governance question for the digital transformation of the economy and society.

This paper presents the results of a first, preliminary analysis of the "Data Act" proposal of the EU Commission with respect to the governance of data generated in IoT devices.[1] Other aspects of the Data Act (DA) are not covered.[2] The basic idea of the DA with respect to IoT data is that both the users of IoT devices and other firms should have more access to the IoT data (for benefitting from more services and enabling innovation), 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 of the users of IoT devices to get access to these data and share them with other firms.

The main aim of the paper is to analyze this mechanism of additional data access and sharing rights of the users, in order to provide a preliminary assessment whether the DA can achieve its objectives with respect to the data generated by the users with their IoT devices. This requires, on one hand, a legal analysis about the rules of the DA (and their interpretation), and, on the other hand, an economic analysis of the expected effects of these rules, with respect to the solution of the current problems with the governance of IoT data.

The overall results of this paper are the following:

(1) Although the DA attempts to solve the relevant issues, and the decision for a more user-centric approach for the governance of IoT data is to be welcomed, the DA cannot be expected to achieve its objectives.

(2) Particularly important is that the key mechanism of data access and sharing rights of the users can be expected to be weak and largely ineffective, also due to a too far-reaching protection of the exclusive control of the data holders over these IoT data.

(3) Key rules in the Data Act are unclear and need clarification, as well as key issues of the governance of IoT data are not addressed. This refers, in particular, to the initial contract between manufacturers and users, and unsolved market failure problems in B2C contexts.

(4) The Data Act proposal raises a number of complex problems, which require a much deeper analysis and broad discussion. Legislators should take their time and not rush into making fast decisions.

---

[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 (23.2.2022).

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

The paper is structured as follows: A brief section 2 will provide some background of the governance problem of IoT data and present the objectives of the DA. Section 3 introduces the basic architecture of the DA approach to IoT data with these new user rights. The main section 4 entails an analysis of the effectiveness of this user rights mechanism, of the (incentive) effects on data holders, and the contract between manufacturers and users as neglected key issue in the DA, before summarizing why the DA can be expected to fail to achieve its objectives. The final section 5 draws some conclusions.

2. Some background, the problems to be solved regarding IoT data, and the objectives of the Data Act

Background policy discussions

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

- The Communication "Building a European Data Economy" (2017) was a key starting-point, because it recognized the problem of non-personal data that are not reused and shared enough (esp. for innovation) as an important policy issue.[3] This led to the current EU data strategy with its emphasis on the need for more data access and data sharing (non-rivalry of the use of data), which so far has focused on proposals to support voluntary solutions.[4]

- This Communication also addressed for the first time the data governance problem of IoT devices (with its manufacturer vs. user problem), which led to the 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.[5]

- Parallel and independent from this discussion, a very controversial policy discussion has emerged since 2015 about the "access to in-vehicle data and resources" with respect to connected cars. Aftermarket service providers but also other stakeholders in the emerging ecosystem of connected cars have challenged the exclusive control of the car manufacturers over the 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 been solved until today.[6]

---

[3] European Commission, "Building a European data economy" COM(2017) 9 final, 13. Comm (2017)

[4] European Commission, "A European strategy of data", COM(2020) 66 final (19.2.2020).

[5] See Zech, Daten als Wirtschaftsgut - Überlegungen zu einem "Recht des Datenerzeugers", CR 2015, 737; Kerber, A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRURInt, 2016, 989; Drexl, Designing Competitive Markets for Industrial Data – Between Propertization and Access, JIPITEC 8, 2017, 257.

[6] See C-ITS platform, Final report, 2016; TRL, Access to In-Vehicle Data and Resources – Final Report, 2017; Kerber, Data Governance in connected cars: The Problem of access to in-vehicle data, JIPITEC 9, 2018, 310; Martens/ Mueller-Langer, Access to digital car data and competition in aftermarket maintenance market, Journal of Competition Law and Economics 16, 2020, 116.

- The need for solving the problem of data access for enabling aftermarket services (including predictive maintenance) and other complementary services has increasingly emerged as an important problem with respect to many other IoT devices.[7]

- A parallel discussion to the connected cars has emerged (also in many other countries) about 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 ("ag-data").[8]

- Also in many other B2B contexts, problems of insufficient data access (also through "imbalances of negotiation power" between firms), and not enough reuse of data and data sharing, have emerged as important policy issues.

Main problems that have to be solved

What are the main data governance problems with respect to IoT data? The data generated through IoT devices can be personal and non-personal data, and are often mixed sets of both types of data. Personal data are subject to EU data protection law (GDPR) and the data protection rights will remain fully applicable to personal IoT data.[9] However, for many non-personal data generated by IoT devices, no "de jure" rights exist. The manufacturers of IoT devices, however, can choose a technical design of their IoT devices that gives them an exclusive de facto control over all data that are generated by the use of the device by firms or consumers, who have bought, leased, or rented the IoT device. 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 these IoT data for providing services (e.g., also to the users) or for the innovation of new services and products, do not get access to these data.

This can lead to the following negative effects:

(1) The 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 of users with respect to these services and higher prices.

(2) Particular important are also negative effects on innovation on these and many other markets through the lack of access to these IoT data, which also represents an inefficient under-utilization of these data.

(3) The exclusive control over the data also gives the manufacturers a monopoly with respect to using and monetizing these data, i.e. that only they (and not the users) can benefit from the value of these data. This raises the issue of an unfair sharing of the value of IoT data.

---

7 See Podszun, Handwerk in der digitalen Ökonomie. Rechtl,icher Rahmen für den Zugang zu Daten, Software und Plattformen, 2020.

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

9 Art. 1(4) DA; see also recital 7.

These problems can emerge both in B2B and B2C contexts, although the severity of the problems and the relevant market failures can differ significantly.[10]

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:[11]

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**.

In this paper we will use these four objectives for our preliminary assessment whether the DA can be expected to fulfill its tasks regarding IoT data.[12]

3. 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 inalienable rights of the users to access and share the data that they have generated through their IoT devices (Art. 4 and 5 DA). 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.[13] The user also gets the right to share the generated data with third parties (firms or other actors), who can use these 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) but not derived or inferred data.[14] In the DA it is assumed that the manufacturer has designed

---

[10] Additionally, there are also other problems regarding technical hurdles for data interoperability and legal uncertainty about data sharing (e.g. with respect to data protection, trade secrets).

[11] See the following quotations: " ... 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).

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

[13] See recital 28.

[14] See recital 14.

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. However, the "data holders" need not be identical with the manufacturers. Although not explicitly discussed, it seems that the manufacturer can transfer (e.g., "sell") this 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 these data themselves and benefit from services that can be provided through sharing these data, as well as allow other firms to innovate new products and services. The DA emphasizes that these user rights do not diminish in any way the rights of data subjects from EU data protection law regarding personal data but complement them.[15] This also implies 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).[16]

It is important that 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 these 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.[17] 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.[18] The user only seems to have the right to request from the data holder to conclude such a "licensing agreement" with the TP, and it is the user who can decide for which purposes these 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 third party.[19] Although the DA also uses the term "data portability" in this context in analogy to the data portability right of Art. 20 GDPR,[20] 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 third party.

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-like conditions ("fair, reasonable and non-discriminatory terms").[21] 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 of getting "reasonable compensation" for the use of

---

15 See recital 7.

16 See recital 31

17 Art. 8 DA.

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

19 Art. 6(1) DA.

20 See recital 31.

21 Art. 8(1) DA. It should be noted that these rules are part of chapter 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.

the data by the TP.[22] For supporting SMEs, these fees are reduced through limiting them to "the costs directly related to making the data available".[23] For settling disputes about the determination of these FRAND terms, the DA introduces a new dispute settlement mechanism.[24]

The DA does not directly address what the manufacturers and data holder 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 these data, i.e. selling (the access to) these 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 these generated IoT data, and also insists that the DA does not confer any new rights on them.[25] 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.

Art. 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.[26] 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 commercialise these non-personal data for the entire life-time of the IoT device (and can presumably also sell this data holder position to other firms). This would imply that the users only have these inalienable rights for data access and data sharing that the DA grants to them (and which the users cannot waive in such a contract). Since the DA is nearly entirely silent about this contract, it is not clear whether this interpretation is correct. We come back to these contracts later in section 4.4 of this article. Our following analysis is based upon this interpretation, i.e. that users agree in this initial contract to such far-reaching rights for the data holders, at least in B2C situations.

4. Effects of the Data Act

This chapter has the task of analyzing the effects of this basic user rights mechanism in the DA. In a first step, the most important provisions of chapter II of the DA will be analyzed in more detail (section 4.1), before using these insights, in a second step, for assessing the expected effectiveness of the data sharing mechanism in practice (secton 4.2). Section 4.3 will critically analyze the effects on the incentives of the data holder (and to what extent an incentive problem exists). Section 4.4 will address the (already mentioned) initial contract between manufacturers and users, and discuss its problems. The final section 4.5 will summarize the effects on the objectives of the DA.

---

22 Art. 9(1) DA, and recital 42, where it is emphasized that "reasonable compensation" is necessary "to incentivise the continued investment in generating valuable data".

23 Art. 9(2) DA.

24 Art. 10 DA.

25 See recitals 5 and 19.

26 See Art. 3, and recitals 23 and 24.

4.1 A more detailed analysis of these user rights

A key precondition for the entire mechanism is the obligation of manufacturers in Art. 3 DA that all IoT devices have to be "designed and manufactured, ..., 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."[27] This is a far-reaching requirement for the technical design of all IoT devices. It is combined with pre-contractual information obligations about the data that are generated (including whether continuous and in real-time), whether the manufacturer "intends the use of the data itself or allow a third party to use the data and, if so, the purposes for which those data will be used",[28] 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 are generated, with whom these data are shared, and for which purposes they are used. In a dynamic data economy there is the need for some flexibility regarding the generation and use of the data from such durable products as IoT devices. There are no rules in the DA on adapting this contract over the life time of the IoT device, although we have long-term contractual relationships between manufacturers (data holders) and "locked-in" users.[29] It is unclear whether data holders may retain the right to change provisions unilaterally.

Art. 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".[30] For what purposes can the users use the generated IoT data they get access to? From the text of the DA, the user seems to be very free in this regard. 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.[31] For the purposes itself 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".[32] With regard to the sharing of data with third parties (Art. 5 DA), it is important that the users are not allowed to share these data with firms that have been designated as gatekeepers according to the Digital Markets Act for not further increasing their economic power through more data.[33]

"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 third party) for making the data available. It is sufficient that the data holder makes 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

---

27 Art. 3(1) DA; see also recital 19.

28 Art. 3(2)(d) DA.

29 For "lock-in" of the users, see DA, 13.

30 Art. 4(1) DA; see also recitals 23 and 24.

31 Art. 4(3) and (5) DA.

32 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 offer also those services (see recital 28).

33 Art. 5(2) DA and recital 36; see for the problem of data power also below section 4.3.

instance of the manufacturer".[34] 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 discussions these "in-situ data access rights" have become well-known as a new option how to implement data access and data sharing.[35] These "in-situ data access rights" can have 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 data access and data sharing are not any more linked to a data transfer (as a flow of data) and the option of users (or TP) to combine them freely and easily with other data. Since it seems that the data holders can unilaterally decide, whether the data are made available only "in-situ" (and the DA even recommends this solution!),[36] this option to deny any free flow of the data is a huge step for protecting the exclusive control of the data holders over the generated IoT data. Therefore, it is necessary to analyze much deeper 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 that data holders monitor the use of the data by the users and TP, and use these insights for their competition with users or TP.[37]

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 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 later in section 4.3.

One of the key questions is for what purposes the users can share the data with TP. Using these data for aftermarket services for IoT devices and other downstream services directly related to the IoT device 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) can get access to the IoT data of consumers as part of the performance of a service but uses this contract also to collect and aggregate the data from many of its consumers for developing larger data sets,

---

[34] Recital 21.

[35] See for the recent discussion on "in-situ data access rights", e.g. Martens/Parker/Petropoulos/Van Alstyne, Towards efficient information sharing in network m (TILEC Discussion Paper No. DP2021-014), available at SSRN: https://dx.doi.org/10.2139/ssrn.3956256.

[36] See recital 8.

[37] Perhaps Art. 4(6) and Art. 5(5) might be applied to this problem; see also recital 29. For this problem also neutral trustee solutions could provide good solutions.

which can be used for developing new innovations or training algorithms. If this is included in the contract between the consumer and the TP, then it is not clear why this should be a problem.[38]
(2) Another option would be that an intermediary collects these 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 TP 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.[39] It is, however, not clear whether the DA wants to go so far. What would this imply for the "licensing agreements" between data holders and TP, and for "reasonable compensation", if selling and reselling of these data would be possible? If the DA wants to make much more generated IoT data available for innovations by other firms, esp. also start ups, 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. One potential problem for allowing the sale of using these data by the users is that this can lead to competition for the data holders on the data markets, which can endanger their profits from selling access to the same data.[40] As a consequence, the data holders can be expected to be opposed to such an interpretation what users can do with their generated IoT data. It is therefore an important question that has to be clarified: Does the "purpose" of how the data are used by TP, which the users can define, also include the option for the users of selling the use of these IoT data on data markets?

4.2 Effectiveness of the data sharing mechanism in practice?

Another key question in the assessment of the Data Act is whether this user right mechanism will 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 the innovation of new 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 for more competition, innovation, and solving lock-in problems through lowering switching costs, are wellknown and also explicitly acknowledged in the DA.[41] Why should this mechanism of user-initiated data sharing work better

[38] Then it is also not necessary that the data are deleted directly after performing the service to the consumer, as otherwise stipulated in Art. 6(1) DA.

[39] See the 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).

[40] However, the data holder would still get "reasonable compensation" for such a "selling" of the data on data markets.

[41] 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 Krämer/Senellart/de Streel, Making Data Portability more effective for the Digital Economy (2020) CERRE report June 2020.

than Art. 20 GDPR? Important advantages of the "user rights" in the DA compared to Art. 20 GDPR are that (a) the scope of the data covers also "observed" data, (b) "mandates and ensures the technical feasibility of third party access for all types of data coming within its scopel",[42] and (c) 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. Important is that these advantages also refer to personal data, which is very helpful for the problem of mixed data sets. There is, however, also a long list of problems that can be expected to impede the effectiveness of this data sharing mechanism.

Negotiation problems, obstacles, and disputes

(1) A first group of problems relates to the barriers and costs that are caused by the specific rules for using this user right mechanism: Although it is clarified in Art. 5(1) DA that the data holder has to make available the data to a TP "without undue delay" and "of the same quality as is available to the data holder", the specific conditions of the "licensing agreement" have to be negotiated between the data holder and the TP.[43] This negotiation process can lead to considerable problems, costs, and disputes:

(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".[44] It is not clear what types of generated data remain to be covered.

(b) The data are also not required to be made available in standardised formats and by using standardised and open technical interfaces.

(c) Another source of disputes will be the question what data are necessary to 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.

(d) Difficult disputes can also arise about what types of these generated IoT data are protected by trade secrets, how far-reaching the confidentiality agreements and the technical measures need to be for protecting trade secrets, as well as the technical protection measures for the data themselves. Another issue are the specific modalities for "in-situ" access to the data.

(e) Also the modalities of the "fair, reasonable, and non-discriminatory terms" of the licensing agreement can lead to manifold problems. Whereas, e.g., in the PSD2 and in Art. 20 GDPR it is clarified that 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

42 See recital 31.

43 Recital 39 emphasizes very clearly the importance of the "principle of freedom of contract" in this context.

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

discussed issues in the DA what a "reasonable compensation" is, and how to calculate it.[45]

At first sight, it is commendable that the DA offers a new dispute settlement mechanism.[46] However, this is a voluntary mechanism and it 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,[47] 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 (so far not existing) enforcement agencies of the Member States.[48] It is very unclear whether this leads to a fast and effective enforcement. This discussion shows that getting access to the IoT data of users might face large obstacles and (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. Since there is no regulatory authority that can directly make decisions for solving these problems, data holders have many options to make the use of this data sharing right practically hard and unattractive for TP.

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

(2) Another group of problems refers to the question how useful this set of generated IoT data are for TP that want to offer additional services on secondary markets (like repair services) or for new innovations. Two different aspects can be distinguished:

(a) *Insufficient scope of data:* A big problem will be the scope of the data that can be made available through these user rights. Although it also encompasses observed data, non-personal and personal data, and allows for continuous and real-time access, the exclusion of all inferred and derived data (and even data calculated through software) can lead to a data set that might be much too narrow for enabling TP to offer additional services to the users like repair or predictive maintenance services on downstream or adjacent markets. For many of these services, it is not sufficient to have only access to raw data, also processed and derived data might be necessary. Often it will also be necessary that the TP does not only have access to the data of the user, for whom it provides a service, but it might need access to aggregated IoT data from many users (for providing a high-quality service). As already discussed, it is unclear whether and to what extent TP can build up aggregated IoT data sets with these user data, or whether they can combine these data with other data or sell such aggregated data sets on free data markets. It is hard to see how with this mechanism large data sets can emerge, which are suitable for training algorithms.

---

45 Since the rationale for "reasonable compensation" are the incentives for generating data (recital 42), all the problems regarding the existence and extent of incentive problems of data holders (discussed below in section 4.3) will emerge again in the set of criteria about the calculation of "reasonable compensation".

46 Art. 10 DA.

47 For extending the dispute settlement mechanism also to the scope of data see Graef/Husovec, Seven things to improve in the Data Act, 2022, 3, available at: https://dx.doi.org/10.2139/ssrn.4051793.

48 Art. 31 DA.

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

The problem of "access to in-vehicle data and resources" in 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 with regard to all markets within the ecosystem of connected driving, on which services are provided that require either access to the generated car data or technical access to the car. This gatekeeper position implies that independent firms might need a contract with the car manufacturers for getting such access for being able to 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.[49] 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 these data would not be sufficient, e.g., for repair and maintenance service providers, and it also would not offer a solution for technical interoperability. Art. 5 DA is therefore no suitable solution for this well-known problem "access to in-vehicle data and resources" of connected cars. Therefore, there is already a wide consensus that this horizontal regulation of the DA has to be complemented by an additional sectoral regulation. Shortly after the publication of the Data Act proposal, the Commission has opened a public consultation with the explicit aim to hear views what additional rules about data access and technical access to the car are necessary for such an additional sector-specific regulation that should complement the Data Act.[50]

Overall, due to an often too narrow scope of this data set (only raw data) and no provisions for solving problems of technical interoperability, it is very unclear whether the sharing of these sets of generated IoT data by the users according to Art. 5 DA will really help independent service providers to offer their services to the users or even to develop new innovative services on secondary markets. Therefore, it would be necessary to analyze in a very concrete way with respect to all relevant IoT devices, whether, e.g., repair and maintenance service are technically possible with the sharing of this set of generated

---

[49] See Kerber, Data-sharing in IoT Ecosystems and Competition Law: The Example of Connected Cars, Journal of Competition Law & Economics 15(4), 2019, 381, 390-396.

[50] See Public consultation on the revision of the Union legislation on 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. In my view such a regulation has to ensure that a) all data sets are shared (with FRAND conditions) that are necessary for providing additional services in the ecosystem of connected cars, and b) also the technical interoperability is ensured (on FRAND terms). See Specht-Riemenschneider/Kerber, Designing Data Trustees – A Purpose-based Approach (Konrad Adenauer Stiftung) 2022, 61-63, https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees.pdf/3523489b-2611-a12a-f187-3e770d1a9d94?version=1.0&t=1647261611824

IoT data. In addition, even if independent service providers can offer these services, it is very unclear whether due to all these obstacles and costs of this mechanism undistorted competition (levelling-the-playing-field) can be ensured between the services offered by the TP and competing services by the manufacturers. Without enabling and protecting effective competition on secondary markets, the DA will not fulfill its objective of leading to more, better, and cheaper services for the users, which the DA wants to achieve and expects.[51]

Conclusions

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

The benefits from these user rights mechanism could increase, if (1) the scope of the data covered by the DA would be broadened, and clarified that the data sharing right of the users can also be used for "selling" access to these data to TP who can aggregate these data and "sell" the use of these data sets on free data markets, and (2) these user rights are combined with a much clearer regulated approach regarding scope of data, fees, contracts, processes of data sharing (e.g., initiating it by third parties), technical protection measures etc., which could reduce transaction costs and mitigate disputes significantly. This, however, would require a much higher level of regulation, and a regulator who can make decisions about these issues.[52] The other option is to complement, in a much more systematic way, 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 (as this is already discussed in the example of connected cars and has been implemented in the PSD2). This leads to the discussion of the advantages and problems of horizontal vs. sector- or problem-specific solutions.[53]

---

51 See DA, 13, and recital 28.

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

53 See Kerber, From (Horizontal and Sectoral) Data Access Solutions Towards Data Governance Systems, in: Drexl, Data Access, Consumer Interests and Public Welfare, 2021, 441.

4.3 Effects on (incentives of) manufacturers and data holders

Strengthening and justification of the exclusive de facto control of data holders over IoT data

This paper claims that the Data Act can also lead to a strengthening of the current de facto control of IoT data by (large) data holding companies. At first sight, this seems to be in direct contradiction to what the Commission seems to intend, e.g. by granting the above-discussed access and sharing rights of users. Yet, the following reasons make it likely that the position of data holders is 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 these data as they wish, e.g. for monetizing them in order to increase their profits. Although it is true that these user rights theoretically limit this exclusive control of the data holders, their position is not much endangered due to the weakness of this user right mechanism (see last section 4.2).

(2) In section 4.1, 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 third parties 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). The decisive point is: As long as the data holders can protect their exclusive 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 these data. Therefore the data holders do not need "absolute rights" ("inter omnes") for these data, as long as they have exclusive control over these data through technological measures.[54] This is the reason why these technological protections (including the option to give only "in-situ access") are so important for the data holders in the Data Act.

(3) Most important, however, is that with the Data Act the legislator would, for the first time. decide that such a de facto control position over these non-personal data, and the ensuing de facto possibilities how to use these data, may be justified and therefore also politically and legally recognized as legitimate. Right now many data holders may think that these data are "their" data, and that they should be free how to use the data (like with many other assets they own). So far, however, 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" of the data (and its implications) should be acknowledged by the society is an open legal and political question, which has not been decided yet.[55] The Data Act seems to give legitimacy to this exclusive de facto control over the data, and therefore would introduce de facto a protection of these data that has similar economic effects as an IP-like exclusive right. This would be a very significant political and economic success for data holders.

(4) What is the justification for such a strong protection of the IoT data of the data holders in the DA? It is the argument that this is necessary for "preserving incentives to invest in

---

54 See Kerber, Specifying and assigning "bundles of rights" on data. An economic perspective, in: Hofmann/Raue/Zech, Eigentum in der digitalen Gesellschaft, 2022, 151, 162.

55 Ibid, 176.

ways to generate value through data".[56] 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 for giving 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 as data also implies the need for a proper balancing between these incentives and the benefits of a broad use of this non-rivalrous good.[57] Therefore, it is necessary to analyze in a deeper way this incentive problem.

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 Data Act. 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.

It is true, however, that far-reaching obligations for opening privately held data (for giving other firms or public institutions access to these 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 investigate carefully the implications for the generation of data (also with respect to the need for high-quality data sets). Since the beginning of the discussion about data access and data sharing, it has however always been emphasized that the costs of collecting data can be very different: On one hand, collected data can be a mere by-product of other activities (leading to very low costs of data collection), whereas for other types of data much higher investments in data generation might be necessary. If the costs of data collection are low, then a proper balancing between ensuring sufficient data collection incentives and the benefits from making the data available to other firms (e.g. for innovation), would lead to data sharing solutions that favor as much data sharing as possible; whereas in the case of very high data collection costs such a balancing would lead to a much more cautious approach regarding the conditions of mandatory data sharing. Therefore a "one-size-fits-all" approach is not appropriate, and thus it is necessary to differentiate.[58]

What can be said about the incentives for data generation and collection regarding IoT devices in the context of the Data Act? This would certainly need deeper analyses of the different types of IoT devices. However, some general arguments can be made that might be relevant for all IoT devices:

---

[56] DA, 3.

[57] See Kerber (bundles of rights) (fn.54), 164.

[58] See, e.g., Schweitzer/ Haucap/Kerber/Welker, Modernisierung der Missbrauchsaufsicht für marktmöchtige Unternehmen, 2018, 161 and 171; Furman et al, Unlocking digital competition. Report of the Digital Competition Expert Panel, 2019, 75.

(1) The "user rights" of Art. 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 these data. What is changing, however, is that also other firms get the chance to analyze the generated data, i.e. the user rights might lead to competition regarding extracting value from the data (if the user sharing rights mechanism would work well, which might not be the case).

(2) *Relevance of the price of the IoT device:* In most cases the users have bought the IoT devices and are therefore owners of these devices. Independent from the legal question, 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,[59] 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 consumers. If consumers and business users would like to have an IoT device, which collects and processes certain data, because this increases the benefits for the users, 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 important for the benefits that the users can get from using the devices, then manufacturers have sufficient incentives for investing in the sensors in these IoT devices. Therefore it is not clear why a general incentive problem should exist, because it can be expected that the price for the IoT device would include these costs.[60]

(3) *Incentives for generating additional data:* This might be different, however, for those data that are generated and collected through the IoT device, but which do not increase the benefits for consumers. Without additional incentives, manufacturers might not invest in the generation and collection of this type of data. Allowing the manufacturers (and data holders) to get exclusive control over all data that are generated by the IoT device and to use these data, would then lead to large incentives for generating and collecting through IoT devices also many data that do not benefit the consumers any more, but can serve as additional sources of revenues for the data holders.[61] Therefore the crucial question is whether the Data Act also wants to incentivize the generation and collection of such additional data, which do not increase the benefits for the consumers (or business users) regarding the functionality of the IoT devices. If the DA does not want this, then these incentives through the DA can be expected to lead to an over-investment into the generation and collection of data. If, however, the Data Act wants that also many additional data are generated and collected,[62] very serious normative questions will have to be asked. Then the main economic rationale for the design of IoT devices might be how to generate as much (valuable) data as possible, and not how to design the

59 This can be puzzling for non-lawyers.

60 This is not different in the case of leasing or renting the IoT device.

61 This is very close to the well-known problem that platforms collect a lot of data from users, which are not necessary for improving their services to the users, but allow them to make additional profit (e.g. through targeted advertising).

62 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).

device for the benefits of the consumers or business users. This will, for example, raise difficult questions about the implications for the protection of privacy of consumers (and also the "privacy" and trade secrets of business users), and can lead to fears that IoT devices might evolve into "spying or surveillance devices".[63]

Strengthening the exclusive de facto control over IoT data for (large) data holders can lead to more data power and data concentration

Another problem that is not addressed in the DA relates to the question, whether this strengthening of the exclusive de facto control of manufacturers and data holders over the generated IoT data by the Data Act can also have negative effects on competition and innovation through more data power and data concentration. The negative effects of the exclusive control of manufacturers over the generated IoT data on competition on aftermarkets and other downstream markets of IoT devices are already directly acknowledged by the DA, because solving these problems is one of the objectives of the DA. As we have seen in section 4.2, 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 with all its negative effects on competition on secondary markets. However, particularly interesting is the additional question whether the possibility of manufacturers to sell their data holding position (and therefore the data streams from their IoT devices) will 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. This can lead to entirely new forms of data concentration and data power in the digital economy, with so far unknown positive and negative effects. 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 get control also over many data streams from IoT devices by buying the data holder position from IoT device manufacturers. It is a bit surprising that in the DA the users of generated IoT data are not allowed to share their data with gatekeeper companies (in the meaning of the DMA) for benefitting from additional services, but that there are no limitations for manufacturers and data holders to sell access to these data or even the entire data holder position to large tech companies like Amazon, Google, or Apple.[64] Therefore, the strengthening and legitimizing of the exclusive control position of data holders over IoT data might also benefit the large tech firms by allowing them to increase their data power, which could be used also for manifold strategies that might have negative effects on competition and innovation.[65]

---

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

64 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".

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

Conclusions

Taking into account incentives for data generation and data collection regarding IoT devices is important from an economic perspective. However, already these few reasonings have shown the complexity of this incentive argument.[66] Let us summarize briefly our preliminary results:

(1) Since users pay a price for the IoT device, it is not clear why there should be too low incentives for investing in the generation and collection of data, as long as these data increase the benefits of the users from these devices. This fits to the empirical observation that IoT devices are spreading rapidly in all contexts and huge amounts of data are generated and collected. 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 is simply wrong.[67] On the contrary, there also might be too large incentives, leading to over-investments into generation and collection of IoT data (as well as to additional dangers for privacy).

(2) From this perspective, the DA gives a much too large weight to this incentive argument in the balancing between different objectives, especially between data holders and TP that would like to use the data for providing services to the users or for innovation of new services. Hence the DA should weigh the benefits of "unlocking" these IoT data by making them widely available much higher than this is done in the current version of the DA. Establishing a much less restrictive regime for data sharing with less obstacles and costs would have manifold positive effects on innovation, competition, and benefits for users without endangering the incentives for the generation of IoT data. Also the potential danger of more data power and data concentration is an important argument to favor more data shaaring and less exclusive control over the 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 effects for the entire data economy. In combination with a number of new provisions in the DA, which strengthen and protect this de facto exclusive control of the data holder, the DA seems to introduce a "de facto" (not "de jure") exclusive "right" on data, which resembles to some extent (at least with respect to the economic effects) an exclusive IP-like right on data. It is puzzling that the DA, on one hand, clearly insists that the data holders do not get any legal "rights" on these data,[68] and, on the other hand, protects the de facto exclusive position of the data holders in a way that leads economically to similar effects "as if" they have exclusive IP-like right on these data.

---

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

67 Also the impact assessment of the Data Act offers no reasonings that support the general existence of such an incentive problem with regard to IoT devices: The fact that data generation and collection causes costs is not enough for arguing that a market failure exists.

68 See again recital 5.

4.4 The initial contract between manufacturer and user: "The elephant in the room"

What has not been considered in the analysis of the DA so far, is 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.[69] This would imply that the de facto control position of the data holders over the generated IoT data itself would not allow the data holders any more to use the data for themselves (e.g., for improving the IoT device), or for sharing it with others (e.g., for money), or for extracting value from them through data analytics. 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 personal data but not for non-personal data. It is surprising that this legal change is not directly discussed in the DA. 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."[70] Therefore the DA seems to assume that the data holders can expect to have the same possibilities for using and monetizing the data than before the DA except for the limitations through the additional inalienable user rights.

Since there are only a few pre-contractual transparency requirements in the DA,[71] it has to be assumed that otherwise there is freedom of contract between the manufacturer and the user. However, the entire reasoning of the DA seems to assume that the users will accept a contractual agreement with manufacturers, 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 sold on markets with competition between IoT device manufacturers, it is very unclear why the DA assumes without any discussion such an asymmetric distribution of the rights for using the IoT data as the expected outcome on these markets. Why is it not discussed that the users could also be paid directly for allowing the data holders' use of the data, or that the contract could also encompass terms that the data should not be used for certain purposes (e.g. targeted advertising), or not shared with certain types of firms (e.g. Google or Facebook), i.e. that the users can also make granular choices regarding the IoT data they are generating?[72] Why is it assumed that the contract about the use of the IoT data is valid for the entire life-time of the IoT device and cannot be terminated (user lock-in), or that it is not possible that the user can decide to switch to another data holder after a certain period of time.[73]

---

69 Art. 4(6) DA.

70 DA, 13.

71 See again Art. 3 and recital 24.

72 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 referring to exceptional cases.

73 For example, we could also think about the option that an owner of an IoT device can switch to another firm for holding the data of her device (in a similar way, as switching between different platforms). Such options are not discussed in the DA.

From an economic perspective, it can be expected that in many B2B situations negotiations will take place about the question, whether and to what extent manufacturers (and data holders) get in such contracts rights to use the generated IoT data. It can be expected that in many instances the users will demand far-reaching exclusive control over these IoT data, and this can be efficient. It also might well be that they agree that for certain categories of data both actors can use the data. One important option is also 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. In B2B contexts, depending on economic conditions and competition (and also negotiation power), very different allocations of such rights to use the IoT data can be expected in such contracts. In most cases, such B2B agreements based upon freedom of contract will lead to efficient (and also fair) solutions. In B2B contexts such asymmetric distributions of the rights to use the data, in which the user will only have the user rights of Art. 4 and 5 DA, can be expected to be the exception and not the regular case.[74] It is not so easy to claim that we have a pervasive market failure problem in B2B contexts.

This, however, can be very different in B2C contexts. If consumers buy a connected car, a smart TV, fitness trackers, or smart watches etc., it can be expected that they have the same information and behavioral problems with the non-personal data as they already have for a long time with respect to "notice and consent" solutions regarding their personal data.[75] Consumers will not read and understand long contracts about the use and sharing of these data, and do not know the value of these data. It therefore can 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 these data, leaving the consumers only with the choice of either buying the IoT device and accepting the exclusive use of these data by the data holders or not buying it. Due to this 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 for making these rights to use the data a relevant parameter of competition between the manufacturers of IoT devices (in a similar way as also competition does usually not work with respect to privacy-friendly terms regarding personal data).

The Data Act does not address 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. 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 TP regarding the sharing of user data (against coercing, deception, and manipulating the users, also through "dark

---

74 It is not easy to explain, why in the DA in B2B contexts only the users get rights for access and sharing the IoT data but not the manufacturers. In B2B contexts also manufacturers can be entirely dependent on the buyers of their IoT devices, and therefore might not get even access to data for improving their own device. This might be true, e.g., for manufacturers of IoT devices that are used as components in other products, e.g. connected cars. The fairness provisions in B2B relationships in Ch. IV of the DA will not help in these cases.

75 See as overviews OECD, Consumer Data Rights and Competition - Background note, 2020, 35-37; Douglas, Digital Crossroads: The intersection of competition law and data privacy (July 2021).

patterns", as well as "profiling" the consumers),[76] whereas no such consumer protection measures exist for the much more important initial contract between manufacturer and users, which decides about the entire bundle of rights for the use of generated IoT data over a long period of time. Although all experiences we have with contracts about the provision of data through consumers suggest that significant market failures can be expected, the DA does not even discuss this issue.[77] 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 that the data holders get all the rights for using the generated IoT data in those contracts, and are only left with the inalienable user rights granted to them by the DA.

This contract is "the elephant in the room" of the Data Act. On one hand, the provision that data holders can only use the data, if this is based upon a contract with the users, seems to imply that the IoT data that the user have generated with their devices are "their" data, because without their consent the data holders cannot use them. This is theoretically a big step for the empowerment of consumers with respect to their IoT data. On the other hand, the DA does nearly nothing to help the consumers to use this theoretically strong position for exerting more control over their IoT data, e.g., for what data holders can use the data, or for getting a share of the revenues that data holders generate through extracting value from these data or monetizing them on data markets. Helping to solve this market failure problem would be a big contribution to the empowerment of consumers. Instead of addressing how to empower consumers with respect to these contracts with the manufacturers, the Data Act limits its ambitions for the empowerment of consumers to granting them the de facto weak access and sharing rights for their generated IoT data. As a consequence, the Data Act fails to empower the consumers to get control over the data that they are generating with their IoT devices.

Therefore, it is not surprising that it can be expected that 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 these 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, for benefitting from their user rights, they have to pay for their own data: Although the request to share the data is free of charge for the users, the service provider has to pay "reasonable compensation", which from an economic perspective can be expected to raise the price for the service to the user.[78] Overall, the Data Act does also not achieve its objective of ensuring fairness in the allocation of value from data among the actors of the data economy, in particular in B2C contexts. For B2B contexts, deeper analyses would be necessary, also with respect to the effectiveness of

---

[76] Art. 6(2(a) and (b) DA; see also recitals 34 and 35.

[77] It also cannot be found in the impact assessment of the DA. 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 granting also "granular permission options". This recital questions indirectly the entire "freedom of contract" approach with regard to these contracts. It might be a starting-point for a deeper analysis of the problems and amendment proposals.

[78] Therefore, one small proposal for improving the DA is that the service provider has not to pay "reasonable compensation", if the service is performed for the user. This would avoid that the user has to pay for its own IoT data.

the additional rules in Ch. IV of the DA against unfairness of contractual terms in data sharing between businesses with respect to SMEs.[79]

4.5 Summary: Why the Data Act will not fulfill its objectives

An important result of this preliminary analysis is that this mechanism of user rights for access and sharing of the IoT data that users have generated can be expected to be weak and ineffective: The set of generated IoT data that can be shared (raw data) will in many cases not be sufficient for providing additional services or enable innovation. In addition, there are too many obstacles and costs through technical and legal restrictions for protecting the data of the data holders. This has large consequences for the fulfillment of the objectives of the DA, which can be summarized as follows:

(1) Empowerment of consumers and business users: Due to this weak "user rights"-mechanism regarding access / sharing of the IoT data with TP (section 4.2), and the unsolved market failure problems with regard to the initial contract between manufacturers and users the empowerment of the consumers with regard to making decisions about the use and sharing of their IoT data is very limited. It also remains very unclear whether consumers will benefit much from additional and better services in the context of their IoT devices and from lower prices through more competition, e.g., on aftermarkets.

(2) Making more IoT data available for businesses, especially for innovation: Through the weak and ineffective "user right" mechanism for sharing the generated IoT data of users, it can be expected that the DA will rather lead to a "small trickle of data" instead of a "broad data stream" for enabling more data-driven innovation. It is not clear how with this mechanism third parties can obtain large aggregated data sets. Therefore the objective of "unlocking" large amounts of data for innovation and the data economy will not be achieved.

(3) Fairness in the allocation of value from data among actors in the data economy: Neither the DA nor this paper has discussed what fairness means regarding the allocation of value from IoT data. The result that the DA assumes about the sharing of the value from data, namely that nearly all the value of the IoT data can be extracted by the data holders due to the very asymmetric distribution of the rights to use the generated IoT data between data holders and consumers, does not suggest that the DA contributes to the fairness of the allocation of value from the data, at least in B2C contexts.

(4) Preserving incentives to invest in ways of generating value from data: Our analysis has shown that from an economic perspective it is entirely unclear whether and to what extent a general incentive problem and a danger of underinvestment in the generation of IoT data (or the extraction of value from these data) exists. Therefore, the strengthening of the exclusive de facto control of the data holders over the generated IoT data in the DA is not justified and leads to the danger of an over-protection of these data, which (similar to too strong IP rights) can have negative effects on competition, innovation, and the users of IoT devices. It also can aggravate the problems through data concentration and data power.

---

[79] See Art. 13: Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise.

The need for rebalancing between the objectives ...

From an economic perspective the Commission is right to view the question of the governance of IoT data as a balancing problem between the incentives of the generation and collection of IoT data, and the manifold benefits from using these data (as non-rivalrous goods) as much as possible. This is also the basic approach in the law & economics of IP rights regarding intangible non-rivalrous goods. The Commission is also right in its insistence that "a general approach to assigning access and usage rights on data is preferable to awarding exclusive rights of access and use".[80] The Commission is also right in seeing the exclusive control of manufacturers as the key problem for access of IoT users and making enough data available to the innovating firms.

The problem, however, is that the provisions of the Data Act do not lead to a proper balancing between preserving the necessary incentives, which are not a general problem, and the huge benefits of making more data available to innovating firms, and strengthening the empowerment of the consumers, and a fair sharing of the value from these data. Therefore any improvements of the DA should focus on rebalancing this tradeoff for enabling more innovation, consumer empowerment, and fairness regarding the sharing of the value from the data of the IoT users, instead of further strengthening the exclusive control of manufacturers and data holders over the IoT data of users. On the contrary, the preliminary results of this paper suggest that the exclusive de facto control of the data holders should be weakened, and to a much larger extent than the DA is proposing it in the current version of the DA.

5. Some conclusions and perspectives

This paper is only a limited and preliminary assessment of the effects that can be expected from the Data Act proposal of the EU Commission. Its primary task is to contribute to the understanding of the Data Act, stimulate the discussion and help to trigger deeper and broader analyses of these questions, also from an economic perspective. Since this is one of the first papers about the DA proposal, many other papers will be published soon, which will analyse it from very different perspectives, and will contribute many other valuable insights, which could not be considered here. Therefore, I am very cautious in this early phase of the discussion with respect to a general assessment of the DA proposal, also regarding the important question, whether the DA proposal can be seen as a good starting-point, which only has to be improved through a number of proper amendments in the further legislative process, or whether a different approach should be chosen. A broader discussion of policy conclusions is beyond the scope of this paper.

The main results of the paper that we cannot expect that the DA will fulfill its objectives were summarized in section 4.5. They need not be repeated here. In the following, only a few additional issues will be mentioned, which from the perspective of this paper also need much deeper analysis and discussion.

---

[80] Recital 6. For the approach to use the "bundles of rights" concept for analyzing very different models of governance of data as such a "general approach", see Kerber (bundle of rights) (fn.54).

(1) *Horizontal approach of the DA:* One big problem is the horizontal approach of the DA, i.e. that the same rules should apply for all IoT devices and for B2B and B2C contexts. Despite similar problems of not enough data access and data sharing, in B2B and B2C contexts very different questions and market failure problems arise. From an economic perspective it might therefore be better to have different sets of rules for generated IoT data in B2B and B2C situations. Also the IoT devices themselves differ very much, and therefore it will not be surprising that the topic of additional sector-specific or even device-specific sets of rules will emerge in the discussion about the IoT rules of the DA.

(2) *Alternative data governance models:* It is very surprising that the Data Act does not discuss different data governance models for IoT data. The DA assumes without any discussion that the model, in which the manufacturers get exclusive control over the generated IoT data is the only possible data governance model for IoT devices. This is simply wrong and ignores that also other important and realistic options exist, which might be superior to the model that the DA favors and seems to want to establish as the "regular" IoT data governance model for all IoT devices. Why should manufacturers not design and sell IoT devices, which give the users directly the 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 for different stakeholders?[81] The discussion about the Data Act should be extended to other data governance models for IoT devices.

(3) *Harmonised rules for IoT data governance:* Dealing with the first two questions is very relevant, because the DA also claims the need for harmonised rules in the EU, and therefore also sets a framework that will limit (a) further sector-specific regulation at the EU level, and (b) also what the legislators on the Member State level can decide on the governance of IoT data.[82] Since there are very different options how to design the governance of data of IoT devices, which do not rely on exclusive de facto control over data by manufacturers and data holders and give the users and/or neutral data trustees the control over the data, or use other so far still unknown data governance solutions, we should be very cautious that the Data Act does not lead to a pre-emption of other creative solutions for governance of IoT data, especially also on the Member State level.

(4) Overall, the Data Act raises fundamental questions about the legal framework of the data economy: Who should have control over the vast amounts of IoT data (and how to limit potential data power positions), how and by whom can these data be used under what conditions, and how should the value that can be extracted from these data be shared in society? This includes also the relationship to the protection of privacy and the governance of personal data. The Data Act should not only be seen as another regulatory project for helping with specific problems of data access and data sharing, rather it is a key legislative project that requires to enter into a more fundamental discussion on these issues (both at the academic and the political level).

---

81 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 (2017) (fn.6), Kerber (2018) (fn.6), and for a recent discussion of alternative governance models for the mobility data of connected cars (with a specific emphasis on data trustee solutions) Specht-Riemenschneider/Kerber (Designing Data Trustees) (fn.50), 53-73.

82 See recital 4.