

Eckardt, Martina; Kerber, Wolfgang

Article — Published Version

Property rights theory, bundles of rights on IoT data, and the EU Data Act

European Journal of Law and Economics

Provided in Cooperation with:

Springer Nature

Suggested Citation: Eckardt, Martina; Kerber, Wolfgang (2024) : Property rights theory, bundles of rights on IoT data, and the EU Data Act, European Journal of Law and Economics, ISSN 1572-9990, Springer US, New York, NY, Vol. 57, Iss. 1, pp. 113-143, <https://doi.org/10.1007/s10657-023-09791-8>

This Version is available at:

<https://hdl.handle.net/10419/315227>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.


If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



<http://creativecommons.org/licenses/by/4.0/>



Property rights theory, bundles of rights on IoT data, and the EU Data Act

Martina Eckardt¹ · Wolfgang Kerber² 

Accepted: 14 December 2023 / Published online: 19 January 2024
© The Author(s) 2024

Abstract

With the advance of smart IoT devices (Internet of Things) the amount of valuable data will increase dramatically. With its recently enacted Data Act (DA) the EU introduces new data access and sharing rights for the users of IoT devices. This article analyzes how the DA will change the bundle of rights on non-personal IoT data regarding who can control, access, use, share, and monetize this data. In a first step, we apply the property rights theory (esp. the approach of Barzel) for explaining the status quo of IoT data governance. Here the manufacturers can get through the technical design of their IoT devices exclusive de facto control over IoT data ("capture" of data). In a second step, we analyze how the DA changes this de facto bundle of rights in order to unlock more IoT data for innovation, competition, and empowerment of users. Since the DA is not very clear and partly contradictory, three different concepts for the design of this bundle of rights are analyzed and compared: A data holder-centric IP-like concept, a user-centric concept, and the concept of co-generated data. The article analyzes all three concepts from an economic perspective including relevant market failures regarding IoT data in B2B and B2C contexts. For achieving the objectives of the DA, especially regarding unlocking of data for innovation, bundles of rights should be chosen which reject notions of exclusivity and enable broad access and sharing of IoT data. The enacted Data Act, which still clings too much to the exclusivity of data and includes too many hurdles for data sharing, cannot be expected to contribute much to achieving these objectives.

Keywords Internet of Things · Data access · Data governance · EU Data Act · Property rights theory · Bundle of rights

✉ Wolfgang Kerber
kerber@wiwi.uni-marburg.de

Martina Eckardt
martina.eckardt@andrassyuni.hu

¹ Andrassy University Budapest, Budapest, Hungary

² School of Business and Economics, Philipps University of Marburg, Marburg, Germany

JEL Classification K11 · K24 · L86 · O33 · O34

1 Introducing new rights on IoT data: the Data Act

The digital transformation of the economy and society can be understood as a Schumpeterian technological and economic revolution. The "Internet of Things" (IoT) with its manifold data-generating and smart IoT devices represents a new wave of disruptive innovations that lead both to deep structural changes and a further exponential increase in collected data. Since data has become a new and valuable key resource through this digital revolution, the question of new (property) rights, i.e. who can control, use and draw value from this data, has become one of the main issues with respect to the necessary coevolution of the legal framework for the digital economy. Whereas for personal data—at least in the EU—the already existing data protection law with its set of rights of data subjects can be applied,¹ an entirely new data policy discussion developed about non-personal data for which so far often no legal rights exist. Due to the non-rivalrous character of data, the discussion has shifted fast from first ideas about introducing exclusive property on data to introducing more data access and data sharing rights for making more data available for innovation and competition.² The recently enacted Data Act (DA) in the EU³ will introduce new rights for users of IoT devices to access, use, and share IoT data. Therefore, the DA is an important step in the evolution of new bundles of rights on non-personal IoT data.

In its proposal the EU Commission has seen the main problem of the current governance of IoT data in the fact that often the manufacturers of IoT devices can get through their technical design of these devices exclusive de facto control over data generated by the IoT devices of the users. As a consequence, neither the users of these IoT devices nor other firms can get enough access to this data.⁴ This has negative effects on the use and sharing of this data which can impede data-driven innovation and economic growth. The main instrument of the DA for solving this problem

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016.

² See Zech (2016), Kerber (2016), Drexl (2017), European Commission (2017), European Commission (2020).

³ In February 2022 the European Commission (2022) published its Proposal for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (Data Act), COM(2022) 68 final (23 February 2022) (Draft DA). In November 2023 the final version of the Data Act was enacted. See Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023. This article focuses only on those provisions in the DA that are relevant for the governance of IoT data (ch. II and III) and will refer both to the proposal of the Commission (Draft DA) and the enacted Data Act (DA).

⁴ See Draft DA, Explanatory Memorandum, 13, and DA, recital 20.

is the introduction of new legal rights for the users of IoT devices. These encompass (1) a right for users to access and use the data generated by their IoT devices (Art. 4 DA), and (2) a right to share this data with other third parties for purposes determined by the users (Art. 5 DA). This right refers to raw and "pre-processed" IoT data but not to derived and inferred IoT data.⁵ These new user rights for IoT data will be introduced both in B2C and B2B situations. In addition, the DA stipulates that manufacturers (and, more generally, data holders)⁶ are only allowed to use the non-personal IoT data based upon a contractual agreement with the users (Art. 4(13) and (14) DA). So far, manufacturers are free to use the non-personal data under their *de facto* control without the need of such a contract, i.e., without getting explicit consent by the users. This is different for personal IoT data, for which EU data protection law applies, i.e. data holders do already currently need "consent" of the data subjects according to Art. 6(1)a GDPR, if they want to process, use, or share this data. However, the new user rights are partly broader than the existing rights on personal data.⁷ With the introduction of these new user rights the Commission wants to achieve the following objectives⁸: more "empowerment" of users, a fairer allocation of the value from IoT data, and more innovation through the "unlocking of data", especially regarding additional IoT-related services, like repair and maintenance services. However, also the incentives for investing in data-generating IoT devices by the manufacturers should not be undermined.

The introduction of these new user rights and this contract between the data holders and the users will lead to a far-reaching change of the bundle of rights assigned to the manufacturers (data holders) and users of IoT devices. The policy discussion about this DA proposal, however, has shown that it entails a lot of difficult and unsolved problems.⁹ There is a lack of clarity and many ambiguities regarding definitions, provisions, and the relationship to other laws (in particular, to data protection law and trade secret law, which we will not analyze in this article).¹⁰ A main concern in the discussion is that these new user rights might be too weak and ineffective for achieving the objectives of the DA, especially regarding more innovation through unlocking of data and with respect to more user empowerment.¹¹ This

⁵ See DA, recital 15, and Wiebe (2023a, 1570).

⁶ Data holders have the factual control over non-personal IoT data. This position can be held by the manufacturers but also by other actors. For the legal definition see Art. 2 (13) DA.

⁷ Although the new rights of the users refer both to non-personal and personal IoT data, it is unclear to what extent the DA can influence the use and sharing of personal IoT data, because in cases of conflict the rules of the GDPR will always prevail (Art. 1 (5) DA). This relationship with EU data protection law and resulting problems will not be analyzed in this article. See for this topic, e.g., Specht-Riemenschneider (2023).

⁸ See Draft DA, Explanatory Memorandum, 2–3.

⁹ For the discussion about the Data Act proposal, see e.g., Graef and Husovec (2022), Leistner & Antoine (2022), Kerber (2023a, 2023c), Drexler et al (2022), Specht-Riemenschneider (2022, 2023), Hennemann & Steinrötter (2022, 2023), Metzger & Schweitzer (2023), Schweitzer et al (2022), Podszun & Offergeld (2022), Martens (2023), Krämer (2022), Wiebe (2023a).

¹⁰ The protection of trade secrets of the data holders was a big issue in the discussion, leading to a strengthening of their protection in the final version of the DA. See for the relationship to trade secret protection and EU database rights Wiebe (2023b).

¹¹ See, e.g., Leistner & Antoine (2022, 14–16), Kerber (2023a), and Krämer (2022).

might also be a consequence of the lack of a clear and consistent concept about the bundle of rights which the DA wants to establish. Instead, different and incompatible concepts seem to be used that lead to considerable inconsistencies and contradictions.¹² In addition, the DA and the design of its new user rights are not based upon a clear economic analysis.

The objective of this article is to contribute to the analysis of the governance of non-personal IoT data and the DA by applying the bundles of rights approach from an economic perspective. We will analyze, discuss and compare the current status quo of de facto control of data holders over IoT data, with three stylized concepts for the bundle of rights that can be found (often in a vague and implicit way) in the text of the DA proposal, the policy discussions about it, and the finally enacted DA: (1) Particular important is a data holder-centric concept, which views the manufacturer (or the data holder) as the de facto "owner" of the non-personal IoT data in some analogy to the owner of an IP right. (2) In an alternative concept, which was strengthened in the final version of the DA, the rights on non-personal IoT data are assigned to the user (as owner of the IoT device). (3) Much discussed was also the concept of co-generated data. It starts with the notion that manufacturers and users are contributing to the generation of the data, and that therefore both of them should have rights to use, share, and monetize the co-generated IoT data. We will analyze both the status quo and these three stylized concepts regarding their design of the bundle of rights on non-personal data, their economic rationale, relevant market failures, and their effects with regard to the objectives of the DA.

Property rights theory will help us in several respects: Its approach to analyze sets of rights regarding a resource, which can be assigned to different actors, enables to conceive a wide range of different designs of bundles of rights for achieving solutions that fit to the specific characteristics of data. For the question how such a bundle of rights on non-personal IoT data should be designed, it is also necessary to take into account potential market failures as well as the options for solving them. Property rights theory also allows us to understand economically the key role of exclusive de facto control over IoT data without having any legal rights on it as well as what kind of role strategic decisions of the manufacturers about the technical design of IoT devices play for "capturing" the valuable IoT data. Through the application of the bundles of rights approach to this example of IoT data, this article also makes a methodological contribution on how to analyze in a more systematic way the issue of data rights in the digital economy.¹³

The structure of the paper is as follows. Section 2 introduces briefly the property rights theory, the bundles of rights approach, and how it can be applied to data. Section 3 analyzes the key role of exclusive de facto control of manufacturers over IoT data, and the unclear basic approach of the DA for dealing with it. In the main Sect. 4, the above-mentioned three stylized concepts for the bundles of rights on non-personal IoT data are analyzed, assessed, and compared with each other. The

¹² In the final phase of the legislation (trilogue) some significant changes have been made, which might lead to more contradictory interpretations of the DA.

¹³ For a first attempt to analyze the recent policy discussions about rights on data from a property rights and bundles of rights perspective, see Kerber (2022).

final Sect. 5 entails conclusions about the application of the bundles of rights approach on data and a brief assessment of the enacted DA.

2 Property rights theory, the bundles of rights approach, and their application to data

When the property rights theory was developed in economics in the US in the 1960s and 1970s, it focused, on the one hand, on the emergence of property rights as a positive theory. On the other hand, it asked how property rights should be specified to set incentives for achieving optimal outcomes from a normative point of view.¹⁴ Whereas the early property rights theory was much dominated by the objective of economic efficiency, also innovation (dynamic efficiency), distributional objectives (equity) and fundamental values of a society can be taken into account. The property rights theory deconstructed “property” into a bundle of rights regarding a resource. Of particular importance are the right to access a resource, the right to use it and its yields (*usus fructus*), the right to exclude others from accessing and using it, the right to decide on how to manage and transform it, and the right to transfer it to others by selling, leasing or renting it. From a policy perspective, the optimal design of such a bundle of rights is analyzed in particular in regard to how such a set of rights should be specified and to whom these rights should be assigned to. From a Coasean perspective, it also has to be taken into account that the initial design and allocation of a bundle of rights on a resource, e.g. by a legislator or court, is only important in the case of positive transaction costs and market failures. Otherwise markets can be assumed to lead to an efficient reallocation of these rights.¹⁵

The bundles of rights approach, which in many variants is also used in legal research,¹⁶ has the advantage of enabling to design a wide range of different options of how rights on resources are specified and assigned. Traditional concepts of private property on physical goods (with rivalry in its use) usually assign the entire bundle of rights exclusively to one “owner”. However, the different rights of such a bundle can also be assigned to different actors or to the state or to a group of individuals, like, e.g., in the complex institutional solutions regarding common pool resources.¹⁷ Intellectual property rights (IPR) (patents, copyrights) that grant exclusive rights on new technological innovations or creative works also fit into the bundles of rights approach. Although innovations are non-rivalrous in use, it is generally assumed that there might be an incentive problem for investing efforts in generating them because of positive externalities (knowledge spillovers and copying). This

¹⁴ For seminal papers and overviews about property rights theory, see Coase (1960), Demsetz (1967), Furubotn & Pejovich (1972), Alchian & Demsetz (1973), Eggertson (1990), Barzel (1997), Demsetz (2002), and Harris (2020).

¹⁵ See Coase (1960).

¹⁶ For a short, but concise comparison between the legal and economic perspectives with additional references, see Mello (2016); for a recent overview about the legal bundles of rights discussion in the context of data, see Szilágyi (2021, 216–229).

¹⁷ See, e.g., Schlager & Ostrom (1992) and Ostrom (2000, 352–379).

provides a rationale for granting temporary exclusive rights to an innovator, before the innovation is put into the public domain and anybody can use it freely.¹⁸

Data is also a resource that is non-rivalrous in use and which also might require spending costs for generating it. Therefore it is not surprising that analogies to the just described IP rationale emerged with respect to non-personal data.¹⁹ It depends on the specific technology applied whether data can be freely accessed or whether access by others can be excluded partly or entirely (e.g. through technical protection measures). The costs of generating data as well as the benefits from using it (data-driven innovation) might be very different for different types of data and in different contexts and sectors. Therefore, a wide range of different bundles of rights might be optimal, defining who should control, access, use, share, and draw value from data.²⁰ At one extreme, non-personal IoT data could be put in the public domain allowing anybody to access and use it (open data). At the other extreme, the bundles of rights could be assigned exclusively to individual actors implying an exclusive property-like right on data. For many applications, however, better solutions might be intermediate ones: For example, access rights could be assigned to certain groups and/or for certain purposes. Bundles of rights could be assigned to all actors that have contributed to the generation of the data (co-generated data) or to neutral data trustees who are entrusted with the data to enable non-discriminatory access to other potential users. All in all, it depends on the technological and economic conditions (including market failures and transaction costs) which data governance solutions might be best from the perspective of social welfare and, more broadly, society.²¹

3 The basic approach of the Data Act and the role of exclusive de facto control over data

3.1 The status quo of the governance of non-personal IoT data

For understanding how the DA with its new rights for users will change the existing bundle of rights on IoT data, it is necessary to analyze the existing status quo regarding who can currently control, use, share, and draw value from this non-personal IoT data. There is a broad consensus, also stated in the DA, that so far no legal rights exist with respect to non-personal IoT data.²² However, the manufacturers usually design their IoT devices technically in a way that gives them exclusive de facto control over the generated IoT data. Therefore they can exclude others from accessing,

¹⁸ For the Law & Economics of IP rights, see e.g., Lévêque and Ménérier (2004).

¹⁹ For a comparison of the application of the bundles of rights approach to physical property, intellectual property, and data, see Kerber (2022, 152–164).

²⁰ The approach to personal data in the EU with its strong sets of rights for data subjects does also fit into such a bundles of rights concept, because it also can include "fundamental values".

²¹ For an overview about the economics of data and data governance, see Martens (2021), Kerber (2021).

²² See DA, recital 20. Under certain conditions non-personal data can be protected as trade secrets, which, however, only protects against misappropriation.

using, and sharing it.²³ This exclusive de facto control by the manufacturers has been recognized as a decisive feature of the current status quo both in the Draft DA and in the ensuing academic discussion. It enables the manufacturers to exclusively extract value from the non-personal IoT data, e.g., through “licensing” them to other firms or through data analytics. Although the manufacturers do not have any legal rights regarding this data, they can use them in a similar way “as if” the data is their exclusive “property”. Thus, by choosing a specific technical design, IoT manufacturers can de facto “appropriate” this data and its value.²⁴ Therefore the question arises how this de facto control over non-personal data can be understood from the perspective of the property rights theory and the bundles of rights approach.

3.2 De facto control over IoT data from a property rights theory perspective

The relationship between technological evolution and legal evolution can be very complex. Disruptive technological innovations like smart IoT devices open up entirely new economic opportunities and business models, which however also might need a legal coevolution for solving new problems that have not existed before.²⁵ Such innovations can also lead to the generation of a new valuable resource like non-personal IoT data. This, in turn, sets incentives for economic actors to get control over these resources in order to use and draw value from them. However, as research on the emergence of property rights has made clear, generating and enforcing new property rights can be a complex process with large costs.²⁶ Therefore, also other instruments than legal protection by property rights might be useful solutions to secure control over economically valuable resources. This has been shown empirically with regard to the emergence of property rights on land in the US by a number of studies. They show that, e.g., power in form of force, e.g. through collective action for defining and enforcing boundaries of a territory, as well as technological innovations that help to exclude others by reducing the costs of exclusion (“barbed wire”, Anderson & Hill 1975) can be important determinants for the evolution of property rights.²⁷ An important conclusion from this property rights literature is that legal rights are not always necessary for getting exclusive control over a valuable resource which enables its holder to use and extract value from it.

Barzel has developed an approach which addresses this relationship between legal rights and the factual power position of actors (misleadingly called by him

²³ Well-known examples are connected cars and smart farm machinery where the manufacturers of these IoT devices can achieve this control by transmitting the IoT data to proprietary servers. Access to this data is only possible with the permission of the manufacturers. See with respect to connected cars Kerber (2018, 2019) and to smart farm machinery Atik & Martens (2021).

²⁴ See also Kerber (2023a, 128–131).

²⁵ For this relationship from an evolutionary economics perspective, see Eckardt (2001, 2011), and with respect to the digital revolution, see Kerber (2023c).

²⁶ See, e.g., Libecap (1989) and Anderson and Hill (2003).

²⁷ For a detailed analysis on the role of technology for the evolution of property rights, see Umbeck (1981), Anderson and Hill (2003), and also Yandle & Morris (2001).

“economic rights”).²⁸ It is the combination of both instruments that determines the de facto existing set of options regarding who can use and draw economic benefits from a resource. This implies, on the one hand, that a de facto exclusive position, e.g., through technological control, can be a substitute to a direct assignment of exclusive legal rights to the holders of a resource. On the other hand, de facto control can also be very important if exclusive legal rights exist, but are not (well-) enforced. Then both instruments complement each other in ensuring that a holder of such rights can exclusively use this resource, also through de facto excluding others. It also follows from Barzel’s approach that economic actors have incentives to invest economic resources for getting de facto control over new valuable resources, for which so far no legal rights exist or are not well-enforced if the economic value from using them is larger than the costs for “capturing” these resources.

Therefore, Barzel provides an approach from the property rights perspective that can be used for analyzing the wide-spread activities of digital platforms, IoT manufacturers, and many other firms for “capturing” this new valuable resource “data” in the digital economy in order to exploit it economically. Technological control through the technical design of platforms, IoT devices, and technological protection measures (TPM) can therefore play a key role in getting and keeping de facto exclusive control over data in digital contexts.²⁹ As far as no legal rights exist (or are not well-enforced like in the case of personal data), these firms can use such “capturing” strategies for de facto “appropriating” this data to get a property-like exclusive position on them through technological control. According to Barzel these firms have gotten exclusive “economic rights” on this data, even if they have no legal rights.³⁰ These processes can be interpreted as part of the evolution of property rights in the digital economy.

This is exactly how also the above described status quo of the bundle of rights on non-personal IoT data can be explained (see Sect. 3.1). The exclusive de facto control over non-personal IoT data is the result of the specific technical design of the IoT devices by the manufacturers. It allows them the exclusion of others (especially the users as owners of the IoT devices) from this data and thus to “capture” the value of this data. In that respect, the manufacturers of IoT devices are the “de facto owners” of the non-personal IoT data. They are free to use, share, and monetize this data as well as sell this exclusive technical control position to others. Therefore, getting exclusive legal rights on this IoT data is not necessary for the manufacturers as long as technological control serves as a well-functioning substitute for such rights.³¹

²⁸ See Barzel (1997, 2015).

²⁹ See for the significant role of technical de facto control over IoT data also Ullrich (2020, 475–484), Fia (2021, 186), and Noto La Diega (2023) who analyzes also other “enclosures” of IoT data through IP rights.

³⁰ For the controversial discussion about Barzel’s terminology to call such factual power positions over resources “economic rights”, see Cole & Grossman (2002), Hodgson (2015), and Barzel (2015).

³¹ For the more fundamental problems that follow from the fact that technological design can replace law, see the discussion about “code is law” (Lessig 1999). For the problem that through technological design, e.g. users of copyright-protected works can be deprived of certain rights, see Specht-Riemenschneider (2019).

From this current state of the governance of IoT data several important implications can be derived:

- (1) From an economic perspective, it is not in any way normatively justified and therefore not legitimized from the perspective of society that firms have such property-like positions simply because they have captured these positions of exclusive control over IoT data through their own technological decisions. The non-rivalrous character of data makes it very questionable whether such an exclusive control over data is optimal from an economic perspective.³² Other designs of the bundles of rights on non-personal IoT data might have much more positive welfare-enhancing effects. It is, therefore, the task of society to decide whether and under what conditions such de facto control over data should be accepted or not.³³
- (2) Another implication is that the choice between different technical designs of IoT devices is influenced by the prospects of additional profits from getting control over the IoT data. This can lead to a sub-optimal choice of technology from a social welfare perspective, which, however, is profit-maximizing for the manufacturer due to its additional effect of capturing exclusively this valuable resource. From an economic policy perspective, this implies a market failure due to a misalignment between private incentives of the manufacturers and what is optimal for society (inefficient choice of technologies).³⁴ This raises the question whether also some technological regulation, which limits the "freedom" of manufacturers to decide on the technical design of the IoT devices, might be necessary for avoiding that wrong technological solutions are developed and implemented with negative effects on competition and innovation.
- (3) Methodologically, such technical de facto control positions of firms over data have to be seen as part of the bundle of rights on data, even if these firms have no legal rights. The implications of this conclusion will be discussed in detail in our analyses in Sect. 4.

3.3 The unclear and contradictory approach of the Data Act

The DA understands well that the exclusive de facto control over IoT data by the manufacturers leads to the problems of (1) not enough data access for the users, (2) not enough sharing of this data with potential innovators, (3) not enough meaningful control of the users over the data, and (4) no fair allocation of the value generated

³² The non-rivalrous character of the data, which is the basis of the entire EU data policy, refers to non-rivalry in the use of the data. There is certainly a rivalry with respect to the "capturing" of an exclusive (monopolistic) control over data. These are two very different issues which sometimes have gotten mixed up in the DA discussion.

³³ See Kerber (2022, 176) and Demsetz (2002, 144): "Uses of resources not legitimated by the user's possession of property rights are illegal by definition or are innovative in the sense that existing property rights have not yet been defined to cover these uses."

³⁴ For economic literature about market failures regarding inefficient choice of technology, e.g., with respect to lack of interoperability, see Kerber & Schweitzer (2017, 42–44), and for its application to the example of connected cars, see Kerber (2018, 321).

through this IoT data. The DA, however, does not question the strategy of the manufacturers to capture the data in an exclusive way through the technical design of their IoT devices. Instead, it tries to limit the ensuing negative effects through the following two instruments.

- (1) Introduction of non-waivable user rights (Art. 4 and 5 DA): These imply changes in the bundle of rights on IoT data because additional rights to access, use and share IoT data with third parties are granted to the users of the devices. These new rights will limit the exclusivity of the data holders' position to use, share, and monetize the IoT data in order to allow for more unlocking of data for innovation, and more control over and value from the data for the users of IoT devices. The resulting bundle of rights then consists of a combination of (a) the de facto options of the data holders to use, share and monetize the IoT data and (b) these new data access and sharing rights of the users. All the provisions in the DA about the scope of the covered data,³⁵ the conditions for access and sharing the data as well as obligations for the third parties using them specify these rights in more detail and influence their effects for all parties.
- (2) Introduction of contractual agreements between data holders and users about whether and how the data holders can use the non-personal IoT data (Art. 4(13) and (14) DA): This contract will lead to a far-reaching change of the bundle of rights. This provision implies that the data holders would lose their current factual options to unilaterally use, share, and monetize the IoT data under their control without a contract with the users. It is, however, not sure whether such a contract can help the users to get more control over their data and whether it contributes to the objectives of user empowerment and unlocking data for innovation and competition (see Sect. 4.2 below).

The combination of these two instruments with the strong emphasis in the DA that the manufacturers' incentives for investing in data-generating IoT devices should not be undermined has led to inconsistencies, contradictions, and much controversial discussions about the exact design of the bundle of rights that the DA wants to establish for non-personal IoT data. Whereas the first instrument of new user rights only seems to limit the exclusive de facto position of the data holders, the contract according to Art. 4(13) and (14) DA suggests that the DA grants the bundle of rights on non-personal (raw and pre-processed) IoT data to the users. It is, therefore, not surprising that in the current discussion very different concepts have emerged, often also in a vague and implicit way.

From an economic perspective, the situation is even more complex. To what extent these two instruments are effective with regard to the objectives of unlocking more data for innovation, and of giving users more control over the IoT data requires also additional analyses of the effects of these two instruments. This, in particular, encompasses also the question of the existence and extent of market failures as well as of the costs (including transaction costs) and benefits for using these instruments

³⁵ Since the scope of the data for these user rights is limited to raw and "pre-processed" data, IoT data outside of this scope remains under the exclusive de facto control of the data holders.

by the users and third parties. Such an analysis has not been provided for by the Commission in its DA proposal.

4 Bundles of rights on non-personal IoT data in the DA: three basic concepts

In this section we analyze three different concepts for the design of the bundle of rights on non-personal IoT data. They can be found partly explicitly and partly implicitly in the proposal of the Commission and the final version of the DA and in the academic discussion. Whereas Sect. 4.1 deals with the concept that the manufacturers have an exclusive IP-like position over this data, the concept in Sect. 4.2 would assign the bundle of rights to the users. With the analysis of the concept of co-generated data in Sect. 4.3 we open the perspective that more than one actor might have rights to use IoT data independently from each other. Section 4.4 provides a short outlook on additional concepts.

4.1 Data holder-centric concept: assigning the bundle of rights on non-personal IoT data in an IP-like way to the data holders

In many respects, the DA seems to follow a concept that views the bundle of rights on non-personal IoT data in some analogy to an IP-like protection for the data holders. We already have seen that de facto control over the data gives the manufacturers an exclusive position that enables them to use the data for themselves, share the data with others (via "licensing" contracts) and extract value from them in a similar way "as if" they would have an IP-like exclusive property on this data. The manufacturers also can sell this exclusive technical control position to other firms which are then data holders, i.e., this technically "captured" IoT data can also be seen as tradable.³⁶ While there are certainly differences between the bundle of rights for the owner of an IPR and the bundle of economic options of data holders through their technical control of IoT data,³⁷ we claim that the basic approach of the DA and many concrete provisions in the DA fit very well to such a concept of an IP-like protection of IoT data for the data holders. If the DA can be interpreted as being based upon such an IP-like concept of non-personal IoT data, then it would legally acknowledge and justify this de facto exclusive position of the data holders and their economic options to use and draw value from this data, notwithstanding the explicit statement in the DA that it does not confer any legal rights to the data holders.³⁸ Most important for this justification is that this concept assumes that de facto exclusivity regarding the use and commercial exploitation of the data by the data holders is necessary for the

³⁶ Through the technological control over the IoT device, the manufacturer can usually "capture" the IoT data stream over the entire life-time of the IoT device, i.e. also the future data stream of an IoT device can be tradable.

³⁷ If there are gaps in technical control or data leaks while sharing it with other firms, then the data holder has lost its exclusive control.

³⁸ See DA, recital 5.

incentives of the manufacturers to invest in data generating IoT devices. This closely resembles the economic rationale for IPRs.

The introduction of the new user rights for access to and sharing of IoT data does not contradict such a concept of an IP analogy, because such rights can be understood as limitations of the exclusive position that usually can also exist in IP laws.³⁹ The requirements for a negotiated contract between data holders and third parties also fit to this concept because here it is the data holder who is “licensing” the data to the third parties, even if the users determine the purpose for what the data can be used.⁴⁰ The provision that the data holders should get “reasonable compensation” from third parties if they use the IoT data via the data sharing rights of the users, is also based upon the incentive argument.⁴¹ In addition, the DA introduces a number of provisions that protect the exclusive de facto control position of data holders if these user rights are being used: Data holders can require technical protection measures, use the option to make the IoT data only available “in-situ”, and there are far-reaching remedies against an unauthorized use of shared data by third parties.⁴² Important from an economic point of view is that in this concept the data holders remain free to use monopolistic price-setting if they share the IoT data directly with other firms. In many respects, the provisions in the DA are close to this concept of protecting an IP-like position on non-personal data for the data holders which, however, is based upon technological exclusion instead of legal exclusion.⁴³

Can such an IP-like concept of the bundle of rights on non-personal IoT data that views data holders as the de facto “owners” be defended from an economic perspective? This leads to the key question whether there is a market failure regarding the incentives to invest in data-generating IoT devices in analogy to the market failure with respect to innovation incentives.⁴⁴ The economic rationale of IPRs has always been based upon a balancing between the trade-off for solving an incentive problem (resulting from externalities by copying) and the costs of monopolization through granting exclusive rights.

The DA is very concerned that the manufacturers of IoT devices might not have sufficient incentives for investing in data-generating IoT devices. Therefore, a far-reaching exclusive position to draw value from the IoT data seems to be necessary. However, an economic analysis is missing why such an incentive problem would exist in the case of data-generating IoT devices that are sold to the users. Manufacturers might have high costs in developing and operating data-generating smart IoT devices. However, from an economic perspective, it is entirely unclear why

³⁹ For example, in copyright law a number of limitations of the exclusivity of copyrights exist, through which also the users of copyright-protected works are granted certain rights.

⁴⁰ See Art. 8, 9 and 11 DA.

⁴¹ See DA, recital 46, and, more generally, recital 30.

⁴² See, e.g., Art. 4(11) and 5(5) and the IP-like remedies in Art. 11 DA, and recitals 8 and 22 (“in situ access”, i.e. data holder need not provide a copy of the data to the user or third-party).

⁴³ All these provisions apply to non-personal data, and do not refer only to data that are protected as trade secrets, whose protection has been additionally strengthened in the final version of the DA (see, e.g., recital 31 and Art. 3 (3)(h), and Art.4 (6)–(9)).

⁴⁴ For the following analysis of this incentive problem, see also Kerber (2023a, 128–131).

manufacturers should not be able to include these investment and operating costs into the price of the IoT devices they are selling to the users.⁴⁵ In contrast to other generated data for which such costs can only be recovered by commercially exploiting the value of the data, IoT manufacturers can sell their devices on markets for a price which can cover all costs incurred and, thus, solve this incentive problem.⁴⁶ Therefore, we contend that no unsolved incentive problem exists which would require the manufacturers to have a monopoly for drawing value from this data in order to avoid a systematic under-investment in data-generating IoT devices.⁴⁷ Thus, no market failure can be identified which is comparable to the innovation incentive problem solved by IP rights⁴⁸ and which would justify the de facto exclusive position of the data holders over IoT data in a similar way.

In addition, also the costs and other negative effects of such exclusive control over the non-personal IoT data by the data holders have to be taken into account: Monopolistic price-setting regarding data leads to high data prices, a low quantity of sold data, considerable welfare costs due to dead weight losses, and negative effects on innovation through a systematic under-utilization of this IoT data.⁴⁹ Since this data can be a critical input for other services, like repair and maintenance services on secondary markets, the control over such a data bottleneck can be strategically used by manufacturers for foreclosing other competitors on these secondary markets. Both by the exclusive control over the IoT data and by additional technological decisions (closed systems/lack of interoperability), manufacturers can get gatekeeper positions for entire ecosystems of products and services that can be built upon these IoT devices.⁵⁰ These potentially high costs of exclusive positions of manufacturers on IoT data in combination with the non-existence of a systematic incentive problem lead to the conclusion that an IP-like concept of the bundle of rights on IoT data through de facto exclusive control of the data holders cannot be defended from an economic perspective.

However, the DA itself assumes that the costs of this exclusivity in terms of not making enough data available etc. are larger than its benefits. This is the reason why it tries to limit this exclusivity through its new user data access and sharing rights. These should lead to more unlocking of IoT data for innovation, empower users,

⁴⁵ The costs of operating the devices after their sale can also be covered by subscription fees.

⁴⁶ For the argument that the price of the IoT devices can cover the investment costs and therefore no incentive problem exists, see also Martens (2023), Drexl et al., (2022, para. 72), and Specht-Riemenschneider (2022, 823).

⁴⁷ It certainly can be argued that expected additional revenues from the monopolized monetizing of this IoT data might help financing investments into data-generating IoT devices. But it can be expected that the decision of manufacturers whether to develop or not an IoT device will depend on these additional revenues only in a very limited number of cases. An additional, perhaps more important issue is whether and to what extent additional revenues of the manufacturers from this IoT data might lead to lower prices on the market for IoT devices as this could be expected—at least theoretically—on well-functioning markets. This question would require much more research. See also Kerber (2023a, 128–130).

⁴⁸ It should also be kept in mind that the IoT devices themselves can be protected by IPRs.

⁴⁹ See also Martens (2021, 74).

⁵⁰ The "extended vehicle" concept of the car manufacturers is a well-known example of such a strategy. Similar strategies exist with respect to smart farm machinery, see Kerber (2018) and Atik & Martens (2021).

and enable competition on secondary markets. Does this combination of de facto control by data holders and these user rights lead to a proper balancing of the positive and negative effects with respect to the objectives of the DA? A deeper analysis of the expected effects of the user rights, and especially the data sharing mechanism of Art. 5 DA, comes, however, to the conclusion that this mechanism will be weak and largely ineffective: From an economic perspective, it is not enough that users get rights to access and share IoT data. It also depends on the specific conditions, requirements, and transaction costs, whether such rights lead to an effective instrument for sharing data. The DA, however, entails so many specific conditions and requirements as well as unclear provisions (resulting in high transaction costs), that it will be hard and unattractive for third parties to get IoT data through these new rights of the users. Also the scope of the data (raw and pre-processed data) will often be too small for enabling many services and foster innovation. Therefore, this data sharing mechanism will not lead to much unlocking of IoT data for data-driven innovation, or for new services and competition on secondary markets (e.g., for repair and maintenance services).⁵¹

To sum up, the main problem of the DA is that it seems to follow to a large extent the concept of an IP-like protection of non-personal data for the data holders, although this concept cannot be defended from an economic perspective in the case of data generated by IoT devices that are sold (or leased or rented) to the users. From an economic perspective, applying this concept to IoT data would lead to the introduction of a "de facto property" on non-personal IoT data to the data holders.⁵² It is particularly problematic that such a concept sets large incentives for firms to develop technologies (here the technical designs for IoT devices) that "capture" as much data as possible by bringing them under their exclusive de facto control and excluding others.

4.2 User-centric concept: assigning the bundle of rights on non-personal IoT data to the users

The analogy to an IP-like protection of non-personal data for the data holders, however, does not fit at all to other provisions in the DA (Art. 4(13) and (14)), which suggest on the contrary a very different concept of the bundle of rights on non-personal IoT data. Since according to these provisions the data holders cannot exploit any more their de facto options to use, share and draw value from this non-personal data without the consent of the IoT device users, these provisions can be interpreted

⁵¹ See for a deeper analysis why the DA proposal of the Commission and, especially, why this data sharing mechanism will not be effective and therefore not achieve the objectives of the DA Kerber (2023a, 125–128); see also Krämer (2022), and Podszun & Offergeld (2022). Although the final version of the DA entails a number of changes (some with positive and some with negative effects regarding the data sharing mechanism), it is very doubtful whether the enacted DA will achieve its objectives better than the initial DA proposal of the Commission.

⁵² See Kerber (2023a, 128) and Martens (2023, 2); Metzger & Schweitzer (2023, 54) also acknowledge that "in economic terms, the [DA] proposal may be read as an indirect recognition of the primary data holder's technical, de facto position of 'ownership' ...". But "this indirect recognition does not amount to a legal property right" (ibid).

as assigning the bundle of rights on non-personal IoT data to the users.⁵³ Although such a contract already existed in the proposal of the Commission (Draft DA Art. 4(6) sentence 1), it was one of the most important changes in the final version of the DA to strengthen the position of the users by adding Art. 4(14) DA and explicitly stating in the new recital 26 that only the users should "have the right to share non-personal data with data recipients for commercial and non-commercial purposes".⁵⁴ The basic idea is that only the users should have the right to monetize the IoT data for giving them incentives to share the data in order to "foster the emergence of liquid, fair and efficient markets for non-personal data".⁵⁵ These changes strongly support the interpretation that the DA is assigning the bundle of rights to the users.⁵⁶

Such a user-centric concept that assigns the rights on IoT data exclusively to the users can be based directly on the objective of user empowerment, i.e. to give the users more meaningful control over their non-personal IoT data. It also has direct parallels with the governance of personal IoT data for which the data holders (as data controllers) need the consent of the data subjects for processing and using their personal data. In addition, it can also be derived from the argument that by buying the IoT device the users also acquire the rights of getting the benefits from using this device. From a property rights perspective, we usually assume that acquiring the property of such a physical device also entails the rights to the benefits of using this device (*usus fructus*). If we view the exclusive right on the *usus fructus* of a physical IoT device also as part of the standardized set of rights which are sold to the buyers, then the rights to use, share, and monetize the IoT data would be assigned to the users already through the sale of the IoT device.⁵⁷ If the manufacturer then wants to use this IoT data (for improving its device or sharing it with others etc.), it can conclude a contract with the buyer of this device for allowing it to use this IoT data under certain conditions. The contract about the use and sharing of the non-personal data by the data holders in Art. 4(13) and (14) DA could be interpreted in that way.⁵⁸ In the following, we will analyze the implications of such a concept that starts with the notion that the bundle of rights on the data generated by IoT devices are assigned to the users.⁵⁹

A key question, in that respect, is whether this instrument of a contractual agreement about the use of the data by the data holders can be expected to work effectively for giving users meaningful control over their data or whether it will suffer from market failures. In well-functioning markets with competition between manufacturers and no significant information and behavioral problems, economists

⁵³ See, e.g., Hennemann & Steinrötter (2022, 1483), Specht-Riemenschneider (2022). This is also the main reason why some commentators were very critical to this provision in the Draft DA, see, e.g., Leister & Antoine (2022, 92–95) and Drexel et al., (2022, para. 44–54).

⁵⁴ DA, recital 26; see also recitals 25 and 33.

⁵⁵ DA, recital 26.

⁵⁶ See also Wiebe (2023a, 1570).

⁵⁷ For the concept of standardized sets of rights regarding property, see Merrill & Smith (2000).

⁵⁸ This would also imply that the users are "licensing" the data to the data holders; see Hennemann/Steinrötter (2022, 1483).

⁵⁹ From a legal perspective, see in much more detail Specht-Riemenschneider (2022).

assume that the allocation of rights regarding IoT data can be left to freely negotiated contracts between both market sides. If the users want to have access to the data and/or share the data, manufacturers would have incentives to fulfill these preferences. Since in the DA the required contract about the use of non-personal data by the data holders is left largely to freedom of contract,⁶⁰ the DA seems to assume that these markets work well and that no serious market failures exist. However, in the discussions about the DA large concerns about market failures have been raised, which also emphasize the need to distinguish between B2B and B2C situations.⁶¹

In B2B situations in which, e.g., firms buy smart machines, it can be expected that the allocation of rights regarding the IoT data is part of the negotiations between sellers and buyers, and therefore solved contractually. The contract about the use of the non-personal IoT data by the data holders is then part of a much more comprehensive negotiation between both parties. If buyers are strongly interested in having full control over this IoT data, including rights to share and monetize them (or for enabling them to freely choose repair service providers etc.), then they can make this an important issue in their negotiations. The users might have to pay a higher price if the entire bundle of rights on the IoT data is allocated to them, but this might be an efficient solution based upon their preferences and freedom of contract. Therefore, absent other market failures, users can get full control over the IoT data they are generating. Since in B2B contexts no general market failure problem can be expected regarding this contract,⁶² it can be defended that according to the final version of the DA business users can make contracts with data holders or other third parties in which they waive their user rights for a proportionate compensation.⁶³

In B2C situations, however, this contract between data holder and user can be expected to suffer from the same information and behavioral problems of consumers as in the case of giving “consent” to the use of personal data.⁶⁴ Thus, in B2C situations serious market failures might exist. Due to these market failures, such contracts might not be capable of allocating the rights on IoT data according to the preferences of both parties. Therefore, consumers in particular might not get enough meaningful control over their IoT data nor a fair share of the value from this data. It is, for example, broadly expected that IoT device manufacturers will tie the sale of their devices to a buy-out contract regarding the use of non-personal data by the data holders. Since such a tying strategy implies that the consumers can only buy the device and use it if they agree to such a buy-out contract, they have *de facto* no choice.⁶⁵ This will lead to a very asymmetric allocation of rights to use and draw

⁶⁰ See Staudenmayer (2022, 597). In the DA it is assumed that this contract about the use of the data by the data holders is concluded simultaneously with the sale of the IoT device to the users (DA, recital 25).

⁶¹ See Leistner and Antoine (2022, 80–81); for the following, see also Kerber (2023a, 131–133).

⁶² Also between firms there might be market failure problems through asymmetric bargaining power, but only in a limited number of cases. Here not only the user, but also the manufacturer can be in the position of the weaker party.

⁶³ See DA, recital 25. This is close to a proposal by Metzger & Schweitzer (2023, 56–58) for an exception of the non-waivability of the user rights in B2B situations.

⁶⁴ See Kerber (2023a, 132) and Krämer (2022, 9–10).

⁶⁵ See Specht-Riemenschneider (2022, 820). Similar problems emerge also with respect to the collection and use of personal IoT data, although theoretically EU data protection law provides more protection.

value from the IoT data. Moreover, it does not empower the consumers to decide according to their own preferences whether, to what extent, and for what purposes they want to allow the data holders to use, share, and monetize the non-personal IoT data.⁶⁶ As a consequence, freedom of contract on the market for IoT devices might not lead to a fair and efficient allocation of rights on non-personal IoT data between both parties in B2C contexts. Therefore, this requirement of a contract according to Art. 4(13) and (14) DA, which seems to grant users more meaningful control over their IoT data, might not lead to a significant improvement compared to the status quo because the data holders can contract these rights away.

What are possible solutions for this issue? In data policy, this problem of contracting away rights on IoT data was already discussed with regard to the "data producer right" proposal of the EU Commission in 2017. It implied that the entire bundle of rights on data generated by IoT devices would have been assigned exclusively to the users of IoT devices, who were seen as the "data producers".⁶⁷ One of the main arguments against this exclusive data producer right was that manufacturers can easily contract it away, e.g. in situations with asymmetric negotiation power between the parties or other market failures.⁶⁸

This is the reason why already early in the data policy discussion about IoT data the idea of non-waivable rights on data emerged, e.g. proposals for non-waivable data access rights.⁶⁹ Therefore, the non-waivable access and sharing rights of the users in the DA (Art. 4 and 5 DA) can be seen as an attempt to ensure that the users get at least some minimum rights regarding their generated IoT data which cannot be contracted away by the manufacturers. Although non-waivable (inalienable) rights interfere with the principle of freedom of contract, the existence of market failures can justify the introduction of inalienable rights, even from a pure economic perspective.⁷⁰ However, with regard to the DA proposal, we already have argued that these non-waivable minimum rights of the users can be expected to be weak and largely ineffective due to too many requirements and hurdles for data sharing (see Sect. 4.1). Thus, they do not enable the consumers a meaningful control over their generated IoT data. Therefore, these minimum rights are not a sufficient solution.⁷¹

Another solution would be to strengthen the consumers regarding the contract with the data holders about the use of the IoT data, e.g. by introducing additional rules in analogy to consumer protection. For example, users could have a right to terminate the contract about the use of the data by the data holders (e.g., after two years), without losing the right to the usual functionalities of the IoT device that they

⁶⁶ An additional issue of user empowerment, which we cannot discuss here, is the question whether and to what extent the users can decide which data are generated with their IoT devices.

⁶⁷ See European Commission, 'Building a European data economy' COM (2017) 9 final, 13.

⁶⁸ See for this discussion Kerber (2017) and Drex1 (2018, 4, 132–150).

⁶⁹ See MPI (2017), Drex1 (2018, 18, 154–165).

⁷⁰ From an economic perspective, in cases of market failures inalienable rights can be a solution for achieving a second-best solution if a first-best solution is not achievable (Rose-Ackerman 1986).

⁷¹ One policy option would be to extend and strengthen these rights, e.g. by eliminating many hurdles and thus reducing transaction costs for using them in order to make them more effective. See, e.g. Krämer (2022).

have bought. This would imply that the data holders would get the rights on the non-personal data through this contract only for a limited time and not for the entire lifetime of the IoT device. This would lead to more choice for the users and a limitation of such a (contractual) vendor lock-in regarding the data.⁷² Total buy-out contracts of the rights to use and share the data might also be directly prohibited. Many more regulatory solutions that grant users more granular choices could be introduced.⁷³ Durable IoT devices imply in any case complex long-term contractual relationships, which require sophisticated governance solutions that cannot rely anymore on a simple application of freedom of contract.⁷⁴ The above discussed remedies could give the users to some extent more control over their IoT data.

What are the effects of these user rights on innovation? Firstly, the access of users to their IoT data might enable them under certain conditions to innovate themselves (user innovations). However, this will be possible only to a limited extent.⁷⁵ But, secondly, there also might be a tradeoff between more user empowerment and the objective of unlocking more IoT data for innovation and competition. In the discussion about the DA there is much skepticism about the effectiveness of such an user-initiated data sharing mechanism, especially for building large aggregated data sets for data-driven innovation. The reasons for these serious doubts are seen in a possible lack of incentives of the users (especially consumers) for sharing their IoT data as well as the potentially large transaction costs of collecting them from many users, e.g. by data intermediaries.⁷⁶ Therefore, strengthening the empowerment of users, especially with respect to controlling how others (including the data holders) can use or not use IoT data can also further limit the extent that IoT data are made available to others for innovation and competition.

However, the exclusive assignment of the right to monetize the IoT data to the users in the final version of the DA is justified with the argument that this would give the users the incentives for sharing the data and would lead to the emergence of liquid, fair and efficient markets for non-personal data. With the help of data intermediaries according to the Data Governance Act it would also enable access to aggregated data sets for big data analyses or machine learning.⁷⁷ In order to enable

⁷² The DA contains a transparency requirement about the duration of the contract and arrangement for terminating it (Art. 3(3) (i) DA). It is, however, not clear whether an effective right to termination exists, because this might require that users can continue to use their IoT devices even if they have terminated the contract. To enable competition between service providers it would be particularly helpful if the users could switch the provider of the related service and therefore also the data holder.

⁷³ Of course, such regulatory solutions can also lead to more or less difficult problems, especially from an economic perspective.

⁷⁴ Legally, often national contract law will also be relevant for these contracts.

⁷⁵ This might be easier for business users than consumers. But the broad literature on user innovation shows that also consumers have innovation opportunities (von Hippel 2005, Gambardella et al. 2017, von Hippel 2017) which might be strengthened by these user rights in the DA.

⁷⁶ See, e.g., Leistner & Antoine (2022, 81). Therefore, it was argued that allowing the manufacturers the use and sharing of the IoT data would help promote innovation because they can more easily aggregate them and draw value from them, e.g. through monetization. This led to recommendations of abolishing the need for a contract with the users for allowing the data holders to use the non-personal data. See, e.g., Drexl et al., (2022, para. 44–54).

⁷⁷ See DA, recitals 26 and 33.

data markets, it is now explicitly clarified that users can monetize their non-personal data either directly or via data holders and third parties, and that recipients of data via this user data sharing mechanism are allowed to make this data available also to other third parties, i.e. that also "reselling" the use of the shared data is possible.⁷⁸ From an economic perspective, these changes and clarifications that explicitly allow the emergence of data markets with data from these user rights are very important for fostering innovation, because it cannot be expected that innovating firms can themselves collect the data that they need for their innovations from (often many) users. The explicit integration of the role of data intermediaries is also very important for the emergence of data markets. In that respect, these final changes in the DA remove some important hurdles for making this data available for innovation.⁷⁹

However, this approach in the final version of the DA—to assign IoT data exclusively to the users—raises again a number of critical issues, also with respect to its effects on innovation:

- (1) It is economically not clear why the users of IoT devices should have larger incentives to share and monetize the non-personal data than the manufacturers (or data holders) under the current regime of exclusive *de facto* control.⁸⁰ Why should therefore this change of the bundle of rights lead to more data sharing and more innovation than before?
- (2) Since the DA relies on freedom of contract with respect to the monetization of data through the users, the manufacturers can tie the sale of the IoT device to a contract, in which the users have to grant the data holders the rights to monetize this IoT data to third parties. With such a "contracting away" strategy the right to monetize the data would again end up with the data holders being in a position like in the current situation. Particularly important, however, is that the exclusive assignment of the bundle of rights regarding this IoT data to the users might not change the main problem for innovation, namely that one party might still have exclusive control over this IoT data despite its character as a non-rivalrous resource for data-driven innovation.⁸¹
- (3) Another reason why it remains very doubtful whether this much clearer assignment of this IoT data to the users might not lead to much more innovation is that the many requirements, hurdles, and high transaction costs of the data sharing mechanism still exist in the final version of the DA.⁸² In addition, the DA has gotten much more inconsistent and contradictory because the basic architecture

⁷⁸ See DA, Art. 6(2) (c) and recital 33; however, such further sharing is only possible with the consent of the user.

⁷⁹ See for the key role of enabling markets for the IoT data from these user rights in the DA Kerber (2023a, 125).

⁸⁰ Not only the consumers but also many small- and medium-sized business users might not be very interested in monetizing this data because this might be far away from their business model.

⁸¹ This is to some extent different in B2C cases because the consumers cannot monetize the data exclusively, but these are also the parties which do not have many incentives for making their data available anyhow.

⁸² See fn. 51.

of the DA with its many provisions that protect primarily the interests of the data holders still exist.⁸³

Therefore, with respect to unlocking more data for innovation and competition, both of our first two concepts of assigning the bundle of rights on non-personal IoT data to either data holders or to users are not very helpful. Both solutions have in common that they still start from the notion of exclusivity. In the first concept, it is the exclusive de facto control of the data holders over the data, while in the second case, the users have exclusive rights on this IoT data. In the next section we will start to go beyond such notions of exclusivity.

4.3 Concept of co-generated data: going beyond exclusivity

The concept of co-generated data is a third very influential approach in the recent data policy discussion. It emerged from the insight that in the data economy often more than one actor contributes to the generation of data. Therefore, also each of these actors should have rights on this data and get a share of its value.⁸⁴ As a consequence, the concept of co-generated data mainly intends to offer criteria who should be seen as co-generator to decide to whom rights on data should be assigned to. This is a complex task, especially from an economic perspective. With regard to non-personal IoT data, the DA has explicitly picked up this concept by stating that the generated IoT data are the result of the efforts of both the manufacturers and the users of the device.⁸⁵ Therefore, the new user access and sharing rights in the DA can also be seen as justified by the argument that the users are co-generating the IoT data and should also have a fair share of the value of this data.⁸⁶

Although the concept of co-generated data suggests that all co-generators should have rights on these IoT data, it leaves open the question of the concrete design of this bundle of rights. Should there be joint ownership on this IoT data, or can the co-generating actors use, share, and monetize the non-personal IoT data independently from each other? Many different institutional solutions about the governance of such

⁸³ Assigning exclusive rights to the users is not consistent with the provision that data holders can claim "reasonable compensation" if the users want to share the data with third-parties. From this user-centric concept it also would be a logical conclusion that the users should have the right to decide who the data holders are and also get at least a copy of the data which is not consistent with the option for data holders to grant only in-situ access to the data for making data available.

⁸⁴ This concept has its roots in the ELI-ALI project; see ALI-ELI (2021) and with respect to the DA project Thomas & Wendehorst (2020); see also Schweitzer et al., (2022, 52) and Atik (2022, 416).

⁸⁵ See DA, recital 6. This discussion is closely related to the question who is the "producer" of data. With respect to IoT data, the DA has eschewed this problem by simply assuming that these two actors, manufacturers and users of IoT devices, are always the co-generators of the IoT data.

⁸⁶ However, the DA does not confer legal rights in a symmetrical way to both types of actors. Only the users get rights whereas the manufacturers merely have the option of getting de facto control over IoT data. This can be a problem in the case of powerful buyers vis-a-vis component suppliers, who as manufacturers of IoT devices might not get any access to the IoT data, see, e.g. Martens (2023, 19).

co-generated IoT data are possible, each with different effects on the use, sharing, and monetizing of this data.⁸⁷

In this section, we will focus on one specific variant of this concept of co-generated data, which has emerged prominently in the academic discussion about the DA which has been developed and brought into the DA discussion by Metzger and Schweitzer.⁸⁸ According to this approach, data holders and users should have parallel and independently from each other the same set of rights to use, share, and monetize this co-generated IoT data. An important advantage of this concept as seen by its proponents is that it prevents the monopolization of data and allows competition regarding the provision of data. Thus, it can make more data available for innovators and enable more competition on secondary markets and on data markets. In the following, we will analyze and discuss this concept and its economic implications in more detail.

A consequent implementation of such a concept of parallel and independent sets of rights regarding IoT data would have far-reaching implications. On the one hand, the data holders would not need a contractual agreement with the users about their use of the non-personal data any more, i.e. the provisions of Art. 4(13) and (14) DA would not be needed. On the other hand, however, data holders would lose their exclusive control over the generated IoT data because with such bundles of rights users also can get control over their IoT data, e.g., by getting a copy of the data, which they then can use, share and monetize independently from the data holders. This would allow users to directly share and license the data to third parties by deciding themselves on the conditions and the licensing fees for the data. A bilaterally negotiated licensing contract with “reasonable compensation” between the data holder and a third party with whom the users share their IoT data would not fit any more into such a concept of co-generated IoT data, and thus could be eliminated in the DA.⁸⁹ As a consequence, many of the hurdles and transaction costs for the sharing of IoT data by the users with third parties would cease to exist. This would facilitate the sharing of IoT data by the users considerably. These implications show that

⁸⁷ Additional insights in these questions can be gained from the work done by Ostrom on coproduction and the governance on common pool resources (Ostrom 1996, 2000). However, while co-generation of data by use of IoT devices is in line with Ostrom’s definition of co-production as “(t)he process through which inputs used to provide a good or service are contributed by individuals who are not ‘in’ the same organization” (Ostrom 1996, 1073), it does not imply active collaborative efforts of manufacturers and users for the generation of IoT data.

⁸⁸ See Metzger & Schweitzer (2023, 50–51) and Schweitzer et al., (2022, 213, 216). The basic idea has also been suggested by Leistner & Antoine (2022, 93–94). A similar concept was developed by Martens (2023, 20) with his concept of “mutual exhaustion” of the rights of data holders and users. All of these authors also emphasize that data holders and users have to take into account “legitimate interests” of the other party (e.g., data protection, trade secrets) while using these independent sets of rights.

⁸⁹ In fact, like in the case of the user-centric concept, the entire role of the “data holder” would be very different. It could, in particular, also entail the option that the users can choose who should hold—as a service—the data for them. It would still be possible that the manufacturer might provide the service of operating the IoT device, and collecting and “holding” the data for itself and the user. However, for the user the manufacturer is then only a service provider for “holding” the data who has to be paid for this service by the users (either via the sale price of the device or directly, e.g. through a subscription fee).

also this concept would have far-reaching consequences for the entire architecture of the DA.

What effects can be expected from this concept and what problems might emerge? None of these actors would have a veto position anymore regarding the use, sharing, and monetization of the IoT data, because no exclusive control would exist (with all its negative effects, e.g. through data monopolization). This would enable competition between both types of actors with regard to using, sharing, and extracting value from this data. This can lead to lower prices for this data, and also—perhaps much more important—to less restrictive conditions regarding the use of this data by other firms. This could also foster the thriving of data markets on which the IoT data can be sold, combined with other data to new aggregated data sets, and resold again etc. Therefore, such a concept of co-generated data with parallel and independent rights to both types of actors might be very conducive for data-driven innovation. It would also help to prevent anticompetitive strategies by manufacturers and to protect competition and innovation on secondary markets.⁹⁰ Since the revenues from sharing IoT data with other firms might decline through competition between data holders and users, this concept also implicitly assumes that the IoT device manufacturers can cover their investment costs in IoT devices like in the user-centric concept as discussed in Sect. 4.2. By recovering their costs through their selling price and/or through additional subscription-based prices for services no unsolved incentive problems exist. Nevertheless, the manufacturers might still have considerable competitive advantages compared to users, because they usually can offer more easily and with less costs aggregated data sets than the users who only have rights on their own IoT data (requiring, for example, intermediaries to aggregate the data from many users).

If we see the big advantage of this specific concept of co-generated IoT data in its positive effects on innovation and competition, the question arises, whether these two co-generators (data holders and users) should be allowed to either sell (or exclusively license) their sets of data to each other or to make an agreement to jointly commercialize the data. Both options would eliminate competition between both actors and would lead back to exclusive control over the IoT data and a monopolistic commercialization of the data. If, therefore, the potentially large positive effects of this concept of co-generated IoT data on competition and innovation should be protected, then this would require a prohibition to eliminate competition between both actors through a cartel-like joint commercialization agreement or a "merging" of these two sets of rights through selling (or exclusively licensing them) to each other.⁹¹

The initial DA proposal of the Commission did partly refer to the concept of co-generated data but did not use this approach of two parallel and independent sets of rights for data holders and users. Due to the non-waivability of the user rights (Art. 4 and 5 Draft DA), they could not be sold to the data holders as well as the data holders could not make contracts about whether and how the users are exerting

⁹⁰ However, there might be still other problems, like lacking technical interoperability.

⁹¹ This issue is not explicitly discussed in Metzger and Schweitzer (2023). It also would be relevant in the proposal of Martens (2023, 20) about "mutual exhaustion" of the rights of the data holders and users.

these data access and sharing rights. This implies that in the DA proposal the non-waivability of these user rights would not only have protected a minimum level of empowerment of the users and of a share from the value of the data (Sect. 4.2). It also would have protected—at least to some extent—competition between data holders and users regarding the sharing of their IoT data, and the existence of a second source of IoT data for innovation which is independent from the data holders. In the enacted final version of the DA, this is still the case in B2C situations; in B2B contexts, however, the users now can waive their user rights in a contract with the data holder, i.e. there is no protection any more for an independent second source of this data for competition and innovation.⁹² In Sect. 4.2, we already saw that the final version of the DA sticks very much to the principle of exclusivity.

4.4 Towards more innovation-friendly bundles of rights solutions for non-personal IoT data

In the discussion about the DA, there is a broad consensus about the importance of the objective to unlock more IoT data for innovation. Our analyses about the three stylized concepts regarding the design of the bundle of rights on non-personal data showed that neither of these concepts is very conducive for making much more data available for innovation. In the data holder-centric concept, the reason for this is the much over-rated concern about manufacturers' incentives for investing in IoT devices with the ensuing alleged need for a far-reaching monopolistic commercialization of the data by the data holders. The user-centric concept also includes a tradeoff between the empowerment of IoT device users over their non-personal IoT data and making more IoT data available for innovation. This might lead to the need for more sophisticated solutions like in the much more prominent case of personal data. Even in the third concept of co-generated data, only the very specific variant of assigning parallel and independent sets of rights to the co-generators with additional safeguards against falling back into exclusive solutions might result in more far-reaching positive effects on unlocking data for more innovation and competition.

However, taking the non-rivalrous characteristics of non-personal IoT generated data seriously, there are additional concepts conceivable. Although in this paper we cannot analyze and discuss them in more detail, we want to point briefly to two promising concepts regarding the design of more innovation-friendly bundles of rights on non-personal IoT data.

(1) Direct data access rights: The classical solution for making IoT data available for more innovation and competition is the (already much discussed) direct assignment of rights for third parties to get access and use certain sets of non-personal data (e.g. also aggregated anonymized data sets) without any active involvement of the users. This can be limited to certain groups of firms and/or to certain purposes (e.g., training algorithms). Such a specification and assignment of access rights can also be part of a more comprehensive and targeted sector-specific regulation, which also

⁹² See in the B2B case DA, recital 25; although in B2C contexts the consumers can also monetize their non-personal data via the data holders, they cannot monetize their non-personal data through exclusive contracts with data holders or third parties (Art. 6(2) (h) DA).

might solve additional interoperability problems. Due to the many concerns about the inherent limits of the effectiveness of user-initiated data sharing mechanisms, the need for additional direct access rights has been emphasized repeatedly in the DA discussion.⁹³

(2) Data trustee solutions: Whereas direct access rights still imply the existence of an IoT data holder (like in the DA), an alternative bundle of rights concept would put all (or a significant part) of the non-personal IoT data under the governance of a neutral data trustee. It then would grant access to firms and other entities according to certain principles and conditions in a non-discriminatory way. Here the data trustee itself could be the data holder who has full control over the IoT data. The concrete bundle of rights, especially with regard to who can access and use what kinds of IoT data and for what purposes, can be designed very differently. This would allow for a much better balancing between the interest of making much more data available for innovation and the interests of other stakeholders, as, e.g. users and also manufacturers of IoT devices.⁹⁴

All of these concepts and additional ones, which might be based also on concepts of open data, data as infrastructure, and data commons, go far beyond the approach of the DA.⁹⁵ They may also take into account more directly and explicitly public interests like opening data for scientific research.⁹⁶ Most important, however, is also to enable more differentiation between bundles of rights on IoT data regarding the types of data, B2B vs. B2C situations, and the technological and economic conditions in different IoT contexts. This emphasizes also the inherent limits of horizontal regulations like the DA and the crucial importance of additional sectoral solutions. This also offers the chance to solve better additional and difficult problems like lacking interoperability (e.g. through more standardization).⁹⁷

5 Conclusions

What specific results follow from our economic analysis for the assessment of the provisions about IoT data in the DA?

⁹³ About the limits of the DA for addressing all relevant data access scenarios see Drexl et al., (2022, para.4), Schweitzer et al., (2022, 213), Kerber (2023a, 127).

⁹⁴ For data trustee solutions and possible applications, see Blankertz (2020) and Specht-Riemenschneider (2022).

⁹⁵ From an innovation policy perspective, see, in particular, Potts et al., (2023). Based on ideas developed by the authors like ‘free innovation’ (von Hippel, 2017) and ‘innovation commons’ (Potts, 2018), they discuss in detail welfare gains as well as governance issues related to free access to innovation-related information and data.

⁹⁶ See, e.g., the approach in the EU Proposal for a Regulation on the European Health Data Space COM (2022) 197 final, whose far-reaching opening of health data for secondary use with regard to research differs very much from the approach in the DA.

⁹⁷ The DA also emphasizes the need for additional sectoral regulations (see, e.g., recital 6). For the advantages of sectoral regulation and its relationship to horizontal regulations regarding data access and data governance, see Kerber (2021) and Atik (2022);).

- (1) The DA is not based upon a clear and consistent concept about the governance of non-personal IoT data. On the one hand, its basic architecture and many provisions are dominated much by the data holder-centric concept of an IP-like protection of IoT data through accepting and legitimizing the exclusive *de facto* control over data through data holders. While this suggests that data holders are seen as *de facto* "owners" of data, who also have to be compensated if this data are shared, on the other hand the final version of the DA also emphasizes our second user-centric concept that assigns the bundle of rights on this IoT data to the users. The ensuing inconsistencies and contradictions can be expected to lead to much uncertainty and controversial discussions about the exact design of the bundle of rights in the DA.
- (2) Due to the lack of a comprehensive economic analysis, the DA is also partly based upon wrong assumptions about market failures: (a) There is no general incentive problem regarding the investment in data-generating IoT devices because manufacturers can cover their costs through selling these devices to the users. Therefore, an IP-like exclusive position of data holders is not necessary and hard to defend because it has negative effects on the use and sharing of this data which is non-rivalrous in use. (b) The contract between data holders and users about the use of non-personal data can be expected to suffer from information and behavioral problems (as well as asymmetric bargaining power), especially in B2C contexts. Since the DA does not provide sufficient remedies for this, additional rules in analogy to consumer protection are needed.
- (3) Overall, it can be expected that the DA will not lead to much more unlocking of IoT data for innovation and competition. The main reason is a too large and unnecessary emphasis on the incentives of manufacturers. This has led to a too weak and ineffective data sharing mechanism with too many hurdles, requirements, and high transaction costs due to protecting the interests of data holders. The changes in the final version of the DA for enabling markets for this non-personal data with its emphasis on the role of data intermediaries are an important step into the right direction. However, they are not sufficient for leading to significant improvements with respect to the objective of unlocking much more IoT data for more innovation and competition.⁹⁸
- (4) The main problem with respect to innovation and competition is that the DA still clings to the concept of exclusivity of the control over IoT data, either through exclusive *de facto* control by data holders or through exclusive rights for users, instead of fostering a greater opening of this data to more stakeholders. One option would have been the concept of co-generated data with parallel and independent rights for using and sharing of IoT data for data holders and users or much more far-reaching innovation-friendly bundle of rights, like, e.g. direct access rights for (certain groups) of innovating firms or data trustee solutions.

⁹⁸ For an overall critical view and much skepticism on the DA regarding innovation and competition see also Wiebe (2023a, 1578). For the problem that the DA also entails direct provisions (like non-compete provisions) with negative effects on competition between IoT manufacturers on the primary markets, see Metzger & Schweitzer (2023, 61), Martens (2023, 14) and Kerber (2023b, 33).

- (5) As a consequence, there is a significant danger that the DA might be an important first step on a path (a) towards a further entrenchment and legitimization of the existing pattern of exclusive de facto control of data holders (including the acceptance of the "capturing" of data through technological means), and (b) also towards an explicit introduction of new exclusive legal rights on data with all its negative consequences for innovation, competition, and a thriving data economy.

From a methodological perspective this article has led to several important insights, which are based upon the economic property rights theory and the bundles of rights approach:

- (1) The economic analysis of the effects of legislative proposals for such new data access and sharing rights requires a comprehensive analysis of the effects of the entire bundle of rights on this data, in particular regarding how these rights should be specified and to whom they should be assigned to. Particularly important is the insight that due to the specific non-rivalrous characteristics of data traditional legal concepts of property over physical resources or of IP rights are not suitable for the governance of data. Therefore, new concepts are necessary which so far have not been developed sufficiently.
- (2) If, as often in digital contexts, exclusive de facto control over data through technology plays a significant role, then this factual power over this data and the ensuing economic options for using it have to be taken into account as part of the bundle of rights, even if no formal legal rights exist on this data. It might, additionally, be necessary to go one step further in the analysis, and also ask whether such exclusive de facto control over data is the result of problematic technological strategies for capturing the data and excluding others from accessing and using them. This might then lead to the need for policy measures regarding such technological strategies, if they lead to negative effects on innovation and competition.
- (3) Since rights on data can be reallocated through contracts on markets, the question whether rights on data have to be assigned by the legislator directly to specific actors (and whether such rights should be non-waivable) depends on the results of an analysis of possible market failures. Therefore, appropriate solutions might often entail a combination of the design of the bundles of rights (with the specification and assignment of the rights to different actors) and regulatory rules for the markets, e.g., regarding relevant contracts.

In this article we focused on the question how the DA is changing the bundle of rights on non-personal data generated by the IoT devices of users and how this change can be analyzed regarding its expected effects. Our analysis, however, has limitations, because we have not taken into account additional layers of law which also affect the bundle of rights on non-personal data. Particularly important (and much discussed with respect to the DA) is that non-personal IoT data can also be protected as trade secrets under certain conditions. An economic analysis of the problems of trade secret protection of IoT data, however, was beyond the scope of

this paper. We also have not considered that due to much legal uncertainty about where to draw the line between personal and non-personal data (and how to deal with mixed data sets), also EU data protection law with its far-reaching but not well-enforceable sets of rights on personal data for data subjects can have important implications for the design of the bundle of rights on non-personal IoT data. With regard to the analysis of our three stylized concepts such additional layers of directly applicable or closely related laws and the "legitimate interests" they protect would lead to a further differentiation of these concepts and the ensuing design of the bundle of rights on non-personal data.

From our perspective, the law necessarily has to co-evolve with the technological changes brought about by the digital revolution.⁹⁹ To deal with the effects of such disruptive innovations like smart IoT devices, this not only raises the question about the emergence of new bundles of rights on data but also how these other laws, e.g., trade secret law and data protection law, might have to be better adapted to the specific conditions of the digital economy.

Acknowledgments The authors thank for valuable feedback and discussion Katharina de la Durantaye, Daniel Gill, Moritz Hennemann, Bertin Martens, Juliane Mendelsohn, Axel Metzger, Peter Picht, Roee Sarel, Heike Schweitzer, Louisa Specht-Riemenschneider, Ferenc Szilágyi, Andreas Wiebe, Herbert Zech, two anonymous reviewers as well as the participants of the Annual Conference of the Mannheim Centre for Competition and Innovation (MaCCI), Mannheim, 23–24 March 2023; Hohenheimer Oberseminar (HOS), Weimar, 4–6 May, 2023; Conference “The EU Data Act”, Weizenbaum Institute, Berlin, 23–23 June 2023; Annual Conference of the Academic Society for Competition Law (ASCOLA), Athens, 30 June–1 July 2023; Annual Conference of the German Law and Economics Association (GLEA), Budapest, 6–7 July 2023; Annual Conference of the Society for Institutional & Organizational Economics (SIOE), Frankfurt, 24–26 August 2023; Annual Conference of the European Law and Economics Association (EALE), Berlin, 21–22 September 2023; Annual Conference of the Italian Society of Law and Economics (SIDE-ISLE), Brescia, 13–15 December 2023.

Funding Open Access funding enabled and organized by Projekt DEAL. No funding was received for conducting this study.

Declarations

Conflict of interest Martina Eckardt and Wolfgang Kerber have no conflicts of interest to declare that are relevant to the content of this article.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

⁹⁹ See Eckardt (2001) and Kerber (2023c).

References

- Alchian, A. A., & Demsetz, H. (1973). The property rights paradigm. *Journal of Economic History*, 33, 16–27.
- ALI-ELI (2021). Principles for a data economy: Data transactions and data rights, ELI Final Council Draft. Retrieved February 26, 2023 from <https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/data-economy>
- Anderson, T. L., & Hill, P. J. (1975). The evolution of property rights: A study of the American West. *Journal of Law and Economics*, 18, 163–179.
- Anderson, T. L., & Hill, P. J. (2003). The evolution of property rights. In T. L. Anderson & F. S. McChesney (Eds.), *Property rights: Cooperation, conflict, and law* (pp. 118–141). Princeton University Press.
- Atik, C. (2022). Towards comprehensive agricultural data governance: Moving beyond the “data ownership” debate. *IIC-International Review of Intellectual Property and Competition Law*, 53, 701–742.
- Atik, C., & Martens, B. (2021). Competition problems and governance of non-personal agricultural machine data: Comparing voluntary initiatives in the US and EU. *Journal of Intellectual Property Information Technology and Electronic Commerce Law (JIPITEC)*, 12, 370–396.
- Barzel, Y. (1997). *Economic analysis of property rights* (2nd ed.). Cambridge University Press.
- Barzel, Y. (2015). What are “property rights”, and why do they matter? A comment on Hodgson’s article. *Journal of Institutional Economics*, 11, 719–723.
- Blankertz, A. (2020). Designing data trusts. Why we need to test consumer data trusts now, Stiftung Neue Verantwortung e.V., February 2020. Retrieved February 26, 2023 www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf
- Coase, R. H. (1960). The problem of social cost. *Journal of Law and Economics*, 4, 386–405.
- Cole, D. H., & Grossman, P. Z. (2002). The meaning of property rights: Law versus economics? *Land Economics*, 78, 317–330.
- Demsetz, H. (1967). Towards a theory of property rights. *American Economic Review*, 57, 347–359.
- Demsetz, H. (2002). Property rights. *Palgrave Dictionary of Law and Economics*, 3, 144–155.
- Drexl, J. (2018). Data access and control in the era of connected devices, BEUC (Brussels).
- Drexl, J. (2017). Designing competitive markets for industrial data—Between proprietisation and access. *Journal of Intellectual Property Information Technology and Electronic Commerce Law (JIPITEC)*, 8, 257–292.
- Drexl, J., et al. (2022). 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) (May 25, 2022). Max Planck institute for innovation & competition research paper No. 22–05. Retrieved February 26, 2022 from <https://ssrn.com/abstract=4136484> or <https://doi.org/10.2139/ssrn.4136484>
- Eckardt, M. (2001). *Technischer Wandel und Rechtsevolution*. Mohr Siebeck.
- Eckardt, M. (2011). Legal evolution between stability and change. In P. Zumbansen & G.-P. Calliess (Eds.), *Law, economics, and evolutionary theory* (pp. 202–225). Northampton MA: Edward Elgar.
- Eggertson, Th. (1990). *Economic behavior and institutions*. Cambridge University Press.
- European Commission (2017). Communication from the commission to the European parliament, the council, The European economic and social committee and the committee of the regions, ‘Building a European data economy’, COM(2017) 9 final (10 January 2017).
- European Commission (2020). Communication from the commission to the European parliament, the Council, the European economic and social committee and the committee of the regions, ‘A European strategy of data’ COM(2020) 66 final (19 February 2020).
- European Commission (2022). 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).
- Fia, T. (2021). An alternative to data ownership: Managing access to non-personal data through the commons. *Global Jurist*, 21, 181–210.
- Furubotn, E. G., & Pejovich, S. (1972). Property rights and economic theory: A survey of recent literature. *Journal of Economic Literature*, 10, 1137–1162.
- Gambardella, A., Rasch, C., & von Hippel, E. (2017). The user innovation paradigm: Impacts on markets and welfare. *Management Science*, 63(5), 1450–1468.

- Graef, I., Husovec, M. (2022). Seven things to improve in the data act. <https://doi.org/10.2139/ssrn.4051793>
- Harris, C., et al. (2020). *The origins and consequences of property rights*. Cambridge University Press. <https://doi.org/10.1017/9781108979122>
- Hennemann, M., & Steinrötter, B. (2022). Data Act–Fundament des neuen Datenwirtschaftsrechts? *Neue Juristische Wochenschrift*, 75, 1481–1486.
- Hennemann, M., & Steinrötter, B. (2023). Der Data Act. Neue Instrumente, alte Friktionen, strukturelle Akzentverschiebungen, forthcoming in *Neue Juristische Wochenschrift*.
- Hodgson, G. M. (2015). What humpty dumpty might have said about property rights—and the need to put them back together again: A response to critics. *Journal of Institutional Economics*, 11, 731–747.
- Kerber, W. (2016). A new (intellectual) property for non-personal data? An Economic Analysis, *GRUR International*, 65, 989–998.
- Kerber, W. (2017). Rights on data: The EU communication “Building a European data economy” from an economic perspective. In S. Lohsse, R. Schulze, & D. Staudenmayer (Eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools* (pp. 109–133). Nomos.
- Kerber, W. (2018). Data governance in connected cars: The problem of access to in-vehicle data. *Journal of Intellectual Property Information Technology and Electronic Commerce Law (JIPITEC)*, 9, 310–331.
- Kerber, W. (2019). Data-sharing in IoT ecosystems and competition law: The example of connected cars. *Journal of Competition Law & Economics*, 15, 381–426.
- Kerber, W. (2021). From (horizontal and sectoral) data access solutions towards data governance systems. In J. Drexel (Ed.), *Data access consumer interests and public welfare* (pp. 441–476). Nomos.
- Kerber, W. (2022). Specifying and assigning “bundles of rights” on data: An economic perspective. In Hofmann, F., Raue, B., Zech, H. (Eds.), *Eigentum in der digitalen Gesellschaft* (pp. 151–176). Mohr Siebeck. Retrieved February 26, 2023 from https://www.mohrsiebeck.com/en/book/eigentum-in-der-digitalen-gesellschaft-9783161614927?no_cache=1
- Kerber, W. (2023a). Governance of IoT data: Why the EU Data Act will not fulfill its objectives. *GRUR International*, 72, 120–135.
- Kerber, W. (2023b). Data Act and competition: An ambivalent relationship, *Concurrences* No.1–2023, 30–36.
- Kerber, W. (2023c). Digital revolution, institutional coevolution, and legal innovations. *European Business Law Review*, 34(6), 993–1016.
- Kerber, W., & Schweitzer, H. (2017). Interoperability in the digital economy. *Journal of Intellectual Property Information Technology and Electronic Commerce Law (JIPITEC)*, 8, 39–58.
- Krämer, J. (2022). Improving the economic effectiveness of the B2B and B2C data sharing obligations in the proposed Data Act, CERRE Report (November 2022). Retrieved February 26, 2023 from https://cerre.eu/wp-content/uploads/2022/11/ImproveEffectiveness_DataAct.pdf
- Leistner, M., Antoine, L. (2022). IPR and the use of open data and data sharing initiatives by public and private actors, study commissioned by the european parliament’s policy department for citizens’ rights and constitutional affairs at the request of the committee on legal affairs. Retrieved from <https://doi.org/10.2139/ssrn.4125503>
- Lessig, L. (1999). *Code is law and other laws of cyberspace*. Basic Books.
- Lévy, F., & Ménière, Y. (2004). *The economics of patents and copyright*. The Berkeley Electronic Press.
- Libecap, G. D. (1989). *Contracting for property rights*. Cambridge University Press.
- Martens, B. (2021). Data access, consumer interests and social welfare. In J. Drexel (Ed.), *Data access, consumer interests and public welfare* (pp. 69–102). Baden-Baden: Nomos.
- Martens, B. (2023). Pro- and anticompetitive provisions in the proposed European Union Data Act Working paper 01/2023, Bruegel Retrieved February 26, 2023 from <https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf>
- Mello, M. T. L. (2016). “Property” rights and the ways of protecting entitlements—An interdisciplinary approach. *Revista De Economia Contemporanea*, 20, 430–457.
- Merrill, T. W., & Smith, H. E. (2000). Optimal standardization in the law of property: The *Numerus Clausus* principle. *Yale Law Journal*, 119, 1–70.
- Metzger, A., Schweitzer, H. (2023). Shaping markets: A critical evaluation of the Draft Data Act, *Zeitschrift für Europäisches Privatrecht*, (pp. 42–82).
- MPI (2017). Position statement of the Max Planck institute for innovation and competition of 26 April 2017 on the European Commission’s ‘Public consultation on Building the European Data Economy.

- Retrieved February 26, 2023 from https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf
- Noto La Diega, G. (2023). *The internet of things and the law*. Routledge.
- Ostrom, E. (2000). Private and common property rights. In Bouckaert, B., De Geest, G. (Eds.), *Encyclopedia of law and economics*. Vol. II – Civil Law and Economics. Edward Elgar. Retrieved February 26, 2023 from <http://reference.findlaw.com/lawandeconomics/2000-private-and-common-property-rights.pdf>
- Ostrom, F. (1996). Crossing the great divide: Coproduction, synergy, and development. *World Development*, 24, 1073–1087.
- Podszun, R., Offergeld, P. (2022). The EU Data Act and the access to secondary markets. Study for the Ludwig-Fröhler-Institut für Handwerkswissenschaften. Retrieved from <https://doi.org/10.2139/ssrn.4256882>
- Potts, J. (2018). Governing the innovation commons. *Journal of Institutional Economics*, 14, 1025–1047.
- Potts, J., Harhoff, D., Torrance, A., von Hippel, E. (2023). Profiting from data commons: Theory, evidence, and strategy implications. In: Strategy Science, Published online in Articles in Advance. DOI: <https://doi.org/10.1287/stsc.2021.0080>
- Rose-Ackerman, S. (1986). Efficiency, equity and inalienability. In J.-M. von der Schulenburg & G. Skogh (Eds.), *Law and economics of legal regulation* (pp. 11–39). Kluwer.
- Schlager, E., & Ostrom, E. (1992). Property rights regimes and natural resources: A conceptual analysis. *Land Economics*, 68, 249–262.
- Schweitzer, H. et al. (2022). Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy, a legal, economic and competition policy angle, final report, (8 July 2022). Retrieved February 26, 2023 from https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/20221026-data-access-and-sharing-in-germany-and-in-the-eu.pdf?__blob=publicationFile&v=16
- Specht-Riemenschneider, L. (2019). Diktat der Technik. *Regulierungskonzepte technischer Vertragsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht*. Nomos.
- Specht-Riemenschneider, L. (2022). Der Entwurf des Data Act, *MMR, Zeitschrift für IT-Recht und Recht der Digitalisierung*, pp. 809–826.
- Specht-Riemenschneider, L. (2023). Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO. *ZEuP*, 2023, 638–672.
- Specht-Riemenschneider, L., Kerber, W. (2022). Designing data trustees—A purpose-based approach. Datentreuhänder—Ein problemlösungsorientierter Ansatz, Konrad-Adenauer-Stiftung, Berlin. Retrieved February 16, 2023 from <https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees.pdf/3523489b-2611-a12a-f187-3e770d1a9d94>
- Staudenmayer, D. (2022). Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz. *Europäische Zeitschrift Für Wirtschaftsrecht*, 33, 596–602.
- Szilágyi, F. (2021). The necessity of data allocation: A Plea for a private law (property law) perspective. *European Property Law Journal*, 10, 180–240.
- Thomas, J., & Wendehorst, C. (2020). Response to the public consultation on “A European strategy for data”, COM(2020) 66 final, Wien: European Law Institute. Retrieved February 16, 2023 from https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Data_Economy/ELI_Response_European_Strategy_for_Data.pdf
- Ullrich, H. (2020). Technology protection and competition policy for the information economy—From property rights for competition to competition without proper rights?. In *Penser le droit de la pensée – Mélanges en l’honneur de Michel Vivant*, Dalloz, Paris, (pp. 457–48)
- Umbeck, J. (1981). *A theory of property rights: With application to the california gold rush*. Iowa State University Press.
- von Hippel, E. (2005). *Democratizing innovation*. MIT Press.
- von Hippel, E. (2017). *Free innovation*. MIT Press.
- Wiebe, A. (2023a). Der Data Act—Innovation oder Illusion? *GRUR*, 125, 1569–1578.
- Wiebe, A. (2023b). The Data Act proposal. *Access Rights at the Intersection with Database Rights and Trade Secret Protection*, *GRUR*, 125, 227–238.
- Yandle, B., & Morris, A. P. (2001). The technologies of property rights: Choice among alternative solutions to tragedies. *Ecology Law Quarterly*, 28, 123–168.

Zech, H. (2016). A legal framework for a data economy in the european digital single market: Rights to use data. *Journal of Intellectual Property Law and Practice*, 1, 460–470.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.