ANDRÁSSY UNIVERSITÄT BUDAPEST

ANDRÁSSY WORKING PAPER SERIES IN ECONOMICS AND BUSINESS ADMINISTRATION

Martina Eckardt
Wolfgang Kerber

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

2023

Andrássy Working Paper Series
in Economics and Business Administration
No 51

Martina Eckardt, Wolfgang Kerber
Property rights theory, bundles of rights on IoT data, and the Data Act
Andrássy Working Papers in Economics and Business Administration Nr. 51
2023
ISSN 2560-1458

Published and edited by the the Faculty of Economics and Business Administration of Andrássy University Budapest.
Pollack Mihály tér 3.
H-1088 Budapest
Online at: https://www.andrassyuni.eu/forschung/publikationen/andrassy-working-papers-in-economics-and-business-administration

Managing Editor: Martina Eckardt
Email manuscripts to: martina.eckardt@andrassyuni.hu

Author's address and affiliation:
Martina Eckardt, Andrássy University Budapest (martina.eckardt@andrassyuni.hu)
Wolfgang Kerber, University of Marburg (kerber@wiwi.uni-marburg.de)

_____

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

Martina Eckardt and Wolfgang Kerber*

(first version: 26/02/2023)

Abstract: With the advance of smart IoT devices (Internet of Things) the amount of valuable data will increase dramatically. For much of the thus generated non-personal data no legal rights exist. In its Data Act (DA) draft the EU Commission proposes new data access and sharing rights for the users of IoT devices. Based upon the economic property rights theory, this article analyzes how the DA would 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: Through the technical design of their IoT devices the manufacturers can get exclusive de facto control over IoT data, i.e. they can technologically capture the data, exclude others from accessing and using this data, and draw value from this data as if they have exclusive property rights on them. In a second step, we analyze how the DA would change this de facto bundle of rights in order to unlock more IoT data for innovation, competition, and empowerment of users. Since the DA proposal 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. 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 current DA proposal, which is dominated by the data holder-centric IP-like concept, will not achieve these objectives.

Key words: Internet of Things, data access, data governance, EU Data Act, property rights theory, legal evolution

JEL classification: K11, K24, L86, O33, O34

* Martina Eckardt, Professor of Public Economics and Public Finance, Andrássy University Budapest, martina.eckardt@andrassyuni.hu; Wolfgang Kerber, Professor of Economics, University of Marburg, School of Business & Economics, kerber@wiwi.uni-marburg.de.

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 recent Data Act (DA) proposal of the EU Commission,[3] which intends to introduce new rights for users of IoT devices to access, use, and share IoT data, is an important step in the evolution of a new bundle of rights on non-personal IoT data.

The EU Commission sees 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 proposal of the DA for solving this problem is the introduction of new non-waivable 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). These new user rights for IoT data would be applicable in the same way both in B2C and B2B situations. In addition, the DA stipulates that manufacturers (and, more generally, data holders)[5] are only allowed to use the non-personal IoT data

---

[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, 'Building a European data economy' COM(2017) 9 final; European Commission, 'A European strategy of data' COM(2020) 66 final (19 February 2020).

[3] 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). This article focuses only on those provisions in the DA that are relevant for the governance of IoT data (ch. II and III).

[4] See DA, Explanatory Memorandum, 13, and recital 5.

[5] Data holders have the factual control over non-personal IoT data (Art. 2(6), DA). This position can be held by the manufacturers but also by other actors.

based upon a contractual agreement with the users (Art. 4(6) s.1 DA). So far, manufacturers are free to use the data under their de facto control without the need of such a contract, i.e., without getting explicit consent by the users. With these new user rights the Commission wants to achieve the following objectives:[6] 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 could 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.[7] 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). 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.[8] This 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 confusion and contradictions. In addition, the DA proposal 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 proposal by applying the bundle of rights approach from an economic perspective. This approach enables us to analyze the current status quo of de facto control of data holders over IoT data. We will discuss and compare three alternative stylized concepts for the bundle of rights that can be found (often in a vague and implicit way) both in the text of the DA proposal and in the policy discussions about it: (1) Most prominent is a data holder-centric concept, which views the manufacturer as the de facto "owner" of the non-personal IoT data in some analogy to the owner of an IP right. (2) In another user-centric concept it is the user (as owner of the IoT device) to whom the rights about the IoT data should be assigned to. (3) Much discussed is 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. Such parallel and independent sets of rights might set the stage for even more innovation-centric concepts. We will analyze both the status quo and these three stylized concepts

---

[6] See DA, Explanatory Memorandum, 2-3.

[7] For the discussion about the Data Act proposal, see e.g., Graef/Husovec (2022), Leistner/Antoine (2022), Kerber (2023), Drexl et al (2022), Specht-Riemenschneider (2022), Hennemann/Steinrötter (2022), Metzger/Schweitzer (2023), Schweitzer et al (2022), Podszun/Offergeld (2022), Martens (2023), Krämer (2022).

[8] See, e.g., Leistner/Antoine (2022, 14-16), Kerber (2023), and Krämer (2022).

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 bundle 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 bundle 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.[9]

The structure of the paper is as follows. Section 2 introduces briefly the property rights theory, the bundle 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 proposal for dealing with it. In the main section 4, the above-mentioned three stylized concepts for the bundle of rights on non-personal IoT data are analyzed, assessed, and compared with each other. The final section 5 entails conclusions about the application of the bundle of rights approach on data and an assessment of the DA proposal.

2. Property rights theory, the bundle 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.[10] Whereas the early property rights theory was much dominated by the objective of economic efficiency, 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

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

[10] 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).

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. However, 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.[11]

The bundle of rights approach, which in many variants is also used in legal research,[12] 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 to such a bundle can also be assigned to different actors, or this bundle can be assigned to the state or to a group of individuals, like, e.g., in the complex institutional solutions regarding common pool resources.[13] Intellectual property rights (IPR) (patents, copyrights) that grant exclusive rights on new technological innovations or creative works also fit into the bundle 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 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.[14]

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 IPR rationale emerged with respect to non-personal data.[15] It depends on the specific technology applied whether data can be freely accessed or whether access by others can be excluded partly or totally (e.g. through technical protection measures). Since the costs of generating data as well as the benefits for using it (data-driven innovation) might be very different for different types of data and in different contexts and sectors, a wide range of different bundles of rights might be optimal, defining who should control, access, use, share, and draw value from data.[16] 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 bundle of rights could be

---

[11] See Coase (1960).

[12] 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 bundle of rights discussion in the context of data, see Szilágyi (2021, 216-229).

[13] See, e.g., Schlager/ Ostrom (1992) and Ostrom (2000, 352-379).

[14] For the Law & Economics of IP rights, see e.g., Lévêque/ Ménière (2004).

[15] For a comparison of the application of the bundle of rights approach to physical property, intellectual property, and data, see Kerber (2022, 152-164).

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

assigned exclusively to individual actors implying an exclusive property-like right on data. For many applications, however, the most interesting 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.[17]

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 non-waivable rights for users would 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 Draft, that so far no legal rights exist with respect to non-personal IoT data.[18] 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, using, and sharing it.[19] This exclusive de facto control by the manufacturers has been recognized as a decisive feature of the current status quo both in the 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.[20] 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 bundle of rights approach.

---

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

18 See DA, recital 5 and 19. Under certain conditions non-personal data can be protected as trade secrets, which, however, only protects against misappropriation.

19 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).

20 See also Kerber (2023, 128-131).

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.[21] Such innovations can also lead to the generation of a new valuable resource like non-personal IoT data, which 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.[22] Therefore, also other instruments than legal protection by property rights might be 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.[23] 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 "economic rights").[24] 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. From Barzel's approach, it also follows 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

---

21 For this relationship from an evolutionary economics perspective, see Eckardt (2001, 2011), with respect to the digital revolution, see Kerber (2021a).

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

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

24 See Barzel (1997, 2015).

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.[25] 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 by getting 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.[26] 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 section 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.[27]

What are the implications of the status quo of the governance of IoT data for the assessment?

(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. Other designs of the bundle of rights on non-personal IoT data might have much more positive welfare-enhancing effects. It is, therefore, the task of the society to decide, whether and under what conditions such de facto control over data should be accepted or not.[28]

---

[25] 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.

[26] 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).

[27] 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)

[28] 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 be defined to cover these uses."

(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 the result that from a social welfare perspective not the optimal technology is chosen, but one that is profit-maximizing for the manufacturer due to its additional effect of capturing exclusively this valuable resource. From an economic policy perspective, this results in the market failure of an inefficient choice of technologies due to a misalignment between private incentives of the manufacturers and what is optimal for society.[29] This raises the question whether the "freedom" of manufacturers to decide on the technical design of the IoT devices might have to be limited to some extent 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. This will be important for our analyses in section 4.

3.3 The unclear approach of the Data Act

The DA proposal 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 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 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 the IoT data with third parties are granted to the users of the devices. These new rights might 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, 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(6) s.1 DA): This contractual obligation could lead to a far-reaching change of the bundle of rights. This provision seems to imply that the data holders would lose their current

[29] 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).

factual options to unilaterally use, share, and monetize the IoT data under their control without any agreement 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 section 4.2 below).

The combination of these two instruments with the strong emphasis in the DA proposal that the manufacturers' incentives for investing in data-generating IoT devices should not be undermined has led to contradictions, confusion, and much controversial discussions about the exact design of the bundle of rights that the DA wants to establish for non-personal IoT data.[30] Whereas the first instrument of new user rights only seems to limit the exclusive de facto position of the data holders, the contractual obligation according to Art. 4(6) s.1 DA seems to suggest that the DA grants the entire bundle of rights on non-personal 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 depends also on additional investigations and analyses of the effects of these two instruments. This, in particular, encompasses 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 by the users and third parties. Such an analysis, however, has not been provided by the Commission in its DA proposal.

4. Bundle 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 text of the DA and in the ensuing academic discussion. Whereas section 4.1 deals with the concept that the manufacturers should an exclusive IP-like position over this data, the concept in section 4.2 would assign the bundle of rights to the users. With the analysis of the concept of co-generated data in section 4.3 we open the perspective that several or many actors might have rights to use the IoT data independently from each other, Section 4.4 provides a short outlook on such 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 the de facto control over the data gives the manufacturers

[30] We will not focus on the controversial discussions about the protection of trade secrets and data base protection.

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, who are then the data holders, i.e., this technically "captured" IoT data is also tradable.[31] 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 the IoT data,[32] 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.[33] Most important for this justification is that this concept assumes that this de facto exclusivity regarding the use and commercial exploitation of the data by the data holders is necessary for the 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.[34] Also the requirements for a negotiated contract between data holders and third parties 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.[35] 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.[36] In addition, the DA entails a number of provisions that protect the exclusive de facto control position of data holders if these user rights are being used: Technical protection measures, the option to make the IoT data only available "in-situ", and remedies against an unauthorized use of shared data by third parties.[37] Important from an economic point of view is also that the data holders remain free to use monopolistic price-setting if they share the IoT data directly with other firms. In that respect, the provisions in the DA are close to this concept of protecting an IP-like

---

[31] 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.

[32] 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.

[33] See DA, recital 5.

[34] 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.

[35] See Art. 8, 9 and 11 DA.

[36] See DA, recital 42.

[37] See, e.g., the provisions in DA, Art. 5(4), 11(1 and (2), and recitals 8 and 21 ("in situ").

position on non-personal data for the data holders, which, however, is based upon technological exclusion instead of legal exclusion.[38]

Can such an IP-like concept of the bundle of rights on non-personal IoT data that would view the data holders as the de facto "owners" of this data 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.[39] The economic rationale of IPRs has always been based upon a balancing between the tradeoff for solving an incentive problem (resulting from externalities by copying) and the costs of monopolization through granting exclusive rights.

The DA proposal 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 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.[40] 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.[41] Therefore, we contend that there should be no unsolved incentive problem, 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.[42] Since no market failure can be identified, which is comparable to the innovation incentive problem solved by IP rights [43] and which would justify in a similar way the de facto exclusive position of the data holders over IoT data.

---

[38] All these provisions apply already to the non-personal data themselves, and not only to data that are protected as trade secrets. Therefore, these protections are independent from the protection of trade secrets, which we have excluded from our analysis in this article.

[39] For the following analysis of this incentive problem, see also Kerber (2023, 128-131).

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

[41] 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).

[42] 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 – at least theoretically - be expected on well-functioning markets. This question would require much more research. See also Kerber (2023, 228-230).

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

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.[44] 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.[45] 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 proposal 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, and enable competition on secondary markets. Does this combination of de facto control of 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? Following from a deeper analysis of the user rights, and especially the data sharing mechanism of Art. 5 DA, it can be expected that this mechanism is 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 proposal, 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 from users. It cannot be expected that these user rights lead to a significant limitation of the exclusive positions of the data holders. 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).[46]

---

[44] See also Martens (2021, 74).

[45] 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).

[46] See in much more detail Kerber (2023, 125-128), Krämer (2022), and Podszun/Offergeld (2022).

To sum up, following from our analysis the main problem of the DA proposal is that it is following 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. Here exists no systematic incentive problem which would justify the high welfare costs and large negative effects on competition and innovation resulting from the exclusive control over data whose use is non-rivalrous. 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.[47] All in all, the entire concept of an IP-like protection for non-personal IoT data is deeply flawed and should not be applied to the governance of IoT data. 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 in the last section, however, does not fit to the provision of Art. 4(6) s.1 DA, suggests on the contrary a very different concept of the bundle of rights on non-personal IoT data. Without the consent of the IoT device users the data holders cannot exploit any more their de facto options to use and draw value from this non-personal data. This seems to have some 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. Therefore, Art. 4(6) s.1 DA can be interpreted as assigning the bundle of rights on non-personal IoT data to the users.[48]

Independent from the text of the DA proposal, such a user-centric concept 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. 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 right to the benefits of using this device (usus fructus).[49] If we view the exclusive right on the usus fructus of a physical IoT device also as part of the (standardized) set of the bundle

---

[47] See Kerber (2023, 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).

[48] See, e.g., Hennemann/Steinrötter (2022, 1483), Specht-Riemenschneider (2022). This is also the main reason why some commentators are very critical to this provision: See, e.g., Leistner/Antoine (2022, 92-95) and Drexl et al (2022, para. 44-54).

[49] If a firm A is buying a machine for producing bottles, then these produced bottles are viewed as the property of firm A.

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. If the manufacturer then wants to use this IoT data (for improving its device or sharing it with others etc.), it can make a contractual agreement with the buyer of this device for allowing him or her to use this IoT data under certain conditions. The initial contract about the use of the non-personal data by the data holders in Art. 4(6), s.1 DA could be interpreted in that way.[50] In the following, we will analyze the implications of such a concept that starts with the notion that the users should have control over the data that are generated by their IoT devices.[51]

A key question, in that respect, is whether this initial contract about the use of the data by the data holders can be expected to work effectively or whether it suffers from market failures. In well-functioning markets with competition between manufacturers and no significant information and behavioral problems, economists 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 initial contract about the use of non-personal data by the data holders is left largely to freedom of contract,[52] the DA seems also 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.[53] 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 initial 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 these IoT data, including rights to share and monetize them (or for enabling them to freely choose repair service providers etc.),[54] then they can make this an important issue in their negotiations. In these B2B contexts, it can be expected that the users will even negotiate that they get the exclusive de facto control over the data so that they themselves become the “data holders”. 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

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

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

[52] See Staudenmayer (2022, 597). In the DA it is assumed that this initial contract is concluded simultaneously with the sale of the IoT device to the users.

[53] See Leistner/Antoine (2022, 80-81); for the following, see also Kerber (2023, 131-133).

[54] Business users might want to have full control over the generated IoT data because they deem them as their trade secrets. In the DA discussion, however, the problem of how to protect the trade secrets of the users has been neglected so far.

upon their preferences and freedom of contract.[55] Therefore, absent other market failures, users can get full control over the IoT data they are generating.

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.[56] 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.[57] This will lead to a very asymmetric allocation of rights to use and draw 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.[58] As a consequence, freedom of contract on the market for IoT devices does not lead to a fair and efficient allocation of rights on non-personal IoT data between both parties in B2C contexts.[59] Therefore, this initial contract according to Art. 4(6) s.1 DA, which seems to grant users rights to consent, will not change much compared to the status quo, because the data holders can contract these rights away.

What are possible solutions for this issue? The legislator could directly assign the entire bundle of rights on IoT data to the users like the "data producer right" which had been proposed by the Commission in 2017.[60] It was designed as an explicit exclusive right for the users of IoT devices. However, also such a property-like solution can be easily contracted away in the case of such market failures. This is the reason why already early in the DA discussion the idea of non-waivable rights of users emerged, e.g. proposals for non-waivable data access rights.[61] Therefore, the non-waivable access and sharing rights of the users in the DA proposal (Art. 4 and 5 DA) can be seen

---

[55] Paying a higher price for getting the entire bundle of rights on the IoT data also would solve any incentive problem for the manufacturers and compensate them for not being able to monetize the IoT data themselves.

[56] See Kerber (2023, 132) and Krämer (2022, 9-10).

[57] 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.

[58] 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.

[59] Since the DA does not have provisions regarding the right of the users to terminate this initial contract, this asymmetric allocation of rights would exist for the entire life-time of the IoT device (contractual vendor lock-in).

[60] See European Commission, ‘Building a European data economy’ COM(2017) 9 final.

[61] See MPI (2017).

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.[62] However, with regard to the DA proposal, we already have argued that these minimum rights of the users can be expected to be weak and largely ineffective (see section 4.1). Thus, they do not allow the users a meaningful control over their generated IoT data. Therefore, these minimum rights are not a sufficient solution.[63]

Another solution would be to strengthen the users regarding the initial contract with the data holders, 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 have bought. This would imply that the data holders would get the rights on the non-personal data through this initial contract only for a limited time and not for the entire life-time 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.[64] Total buy-out contracts of these rights might also be directly prohibited. Many more regulatory solutions that grant users more granular choices could be introduced.[65] However, 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.

While the above discussed remedies could at least to some degree give the users more control over their data, there might be, however, 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 a 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.[66] Strengthening the empowerment of users, especially

---

[62] 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).

[63] Another 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).

[64] It might even be possible that such a termination right might also allow the users to switch the firm that is operating the IoT device (if this is technically feasible), and therefore switch the data holders. This would enable an independent operation of the IoT devices under the full control of the users and also allow for competition between firms that provide the service of operating the IoT devices.

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

[66] See, e.g., Leistner/Antoine (2022, 81).

with respect to controlling how others (including the data holders) can use or not use IoT data can further limit the extent that IoT data are made available to others for innovation and competition.

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 should have control over their 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.[67] 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.[68] 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.[69] Therefore, the non-waivable 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.[70]

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? Principally, many different institutional solutions about the governance of such co-generated IoT data are possible, each with very different effects on the use, sharing, and monetizing of this data.

---

67 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).

68 This discussion is closely related to the discussion on 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.

69 See DA, recital 6.

70 Please note that the DA does not confer legal rights in a symmetrical way to both types of actors; only the users get rights, whereas the manufacturer has only the option of getting de facto control over the 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).

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, namely the approach that 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. This approach has been developed and brought into the DA discussion by Metzger/Schweitzer.[71] For them, the important advantage of this concept is that it prevents the monopolization of data and allows competition regarding the provision of data. Thus, it might 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 the IoT data would have far-reaching implications. On the one hand, the data holders would not need any more a contractual agreement with the users about their use of the non-personal data, i.e. the provision of Art. 4(6) s.1 DA is not needed. On the other hand, however, the data holders would lose their exclusive control over the generated IoT data because with such a bundle of rights the 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 entirely independently from the data holders. This would allow the 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.[72] 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 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 anymore (with all its negative effects, e.g. through data monopolization). This would enable

---

[71] 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.

[72] In fact, the entire role of the "data holder" as defined in the DA would be very different. It could, in particular, also entail the option that the users can choose themselves 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).

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.[73] Since the revenues from sharing the 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 the user-centric concept in section 4.2. By recovering their costs through their selling price and/or through additional subscription-based prices for services no unsolved incentive problem exists. 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 the need for, e.g., 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. In the DA proposal such behavior is not possible through the non-waivability of the user rights (Art. 4 and 5 DA). These rights cannot be sold to the data holders as well as the data holders cannot make any contracts about whether and how the users are exerting these data access and sharing rights. This implies that in the DA proposal the non-waivability of these user rights does not only protect a minimum level of empowerment of the users and of a share from the value of the data (section 4.2). It protects - 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 current DA proposal, these positive effects on competition and innovation can be expected to remain small because of the weak and ineffective data sharing mechanism (see section 4.1). However, a consequent implementation of this specific concept of co-generated data with a bundle of rights that assigns two parallel and independent sets of rights to access, use, share, and monetize the non-personal IoT data would lead to much more unlocking of IoT data, and therefore to much more innovation and competition. But this would require a prohibition to eliminate competition between both actors

[73] However, there might be still other problems, like lacking technical interoperability.

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.[74]

4.4 Towards more innovation-friendly bundle 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 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.[75]

---

[74] This issue is not explicitly discussed in Metzger/ 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. However, Metzger/Schweitzer (2023, 56-58) suggest limited exceptions of the non-waivability of the user rights.

[75] 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 (2023, 127).

(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 according to certain principles and conditions in a non-discriminatory way to firms and other entities. 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.[76]

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. They may also take into account more directly and explicitly public interests like opening data for scientific research. 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, which also offer the chance to solve better additional and difficult problems of lacking interoperability (e.g. through more standardization).[77]

5. Conclusions

What specific results follow from our economic analysis for the assessment of the provisions about IoT data in the DA? The DA proposal is not based upon a clear and consistent concept about the governance of IoT data. This leads to different and partly contradictory notions about the design of the bundle of rights in the DA. Due to the lack of a comprehensive economic analysis, the DA is also partly based upon wrong assumptions about market failures, in particular whether a systematic incentive problem exists regarding investing in IoT devices. This leads, on the one hand, to the dominance of the concept of an IP-like protection of non-personal IoT data for the data holders through accepting and legitimizing their exclusive de facto control as the result of the technical design by the manufacturers. This concept with its strong and unjustified emphasis on incentives for manufacturers also leads to the design of a weak and largely ineffective data sharing mechanism via the new user rights. It will therefore not contribute significantly to much more unlocking of IoT data for innovation and competition, to more user empowerment or a fairer allocation of value from the IoT data. Although the DA also entails important elements of our second, user-centric concept

[76] For data trustee solutions and possible applications, see Blankertz (2020) and Specht-Riemenschneider/Kerber (2022).

[77] For the relationship between horizontal and sectoral regulations regarding data access and data governance, see Kerber (2021b) and Atik (2022).

that would like to give the users control over the IoT data through the requirement of an initial contract with the data holders about their use of the data, serious market failure problems can be expected to make such a contract ineffective. At least in B2C contexts, this might require more regulation. From a competition and innovation policy perspective, it would be necessary to implement other bundle of rights solutions to make much more IoT data available. The concept of co-generated data with parallel and independent sets of rights on IoT data for data holders and users might be a helpful step into this direction. However, also other more innovation-friendly concepts of bundle of rights on IoT data are possible and should be systematically explored. All these much more innovation-friendly solutions would require a very different architecture of the DA.

The great problem of the current DA proposal is that due to the dominance of the data holder-centric approach the DA will not only fail to fulfill its objectives of unlocking more IoT data for innovation and achieving more user empowerment. Instead, the DA might be an important first step on a path towards a further entrenchment of the existing exclusive de facto control of data holders which is contrary to its objectives. What is more, the DA proposal might even pave the way for the introduction of exclusive legal rights on non-personal data to data holders because it already acknowledges, legitimizes, and protects exclusive de facto control positions by the data holders over non-personal IoT data. It is not hard to predict that this legal recognition of such exclusive positions can evolve over time into explicit exclusive property rights with all its negative consequences for 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 bundle 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 these 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 neither traditional legal concepts of property over physical resources nor of IP rights are suitable for the governance of data. Therefore, new concepts are necessary which still have to be developed.

(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 of such a bundle of rights and also ask whether such an exclusive de facto control over data is the result of a strategic technological choice for capturing the data and excluding others from accessing and using them. This might then lead to the need for policy measures regarding technological choice.

(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 bundle 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 under certain conditions as trade secrets. An economic analysis of the problems of trade secret protection of IoT data, however, is 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 co-evolves with the technological changes brought about by digitalization. To deal with the effects of such disruptive innovations like smart IoT devices, this then would also raise the question how these other laws, e.g., trade secret law, might have to be better adapted to the specific conditions of the digital economy.

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, https://www.europeanlawinstitute.eu/projects-publications/completed-projects-old/data-economy (last access: 26/02/2023).

Anderson, T.L. / Hill, P.J. (2003): The Evolution of Property Rights, in: Anderson, T.L. / McChesney, F. S. (eds.): Property Rights: Cooperation, Conflict, and Law, Princeton/Woodstock: Princeton University Press, 118-141.

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.

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, New York: Cambridge University Press, 2nd ed.

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, available at: www.stiftung-nv.de/sites/default/files/designing_data_trusts_e.pdf (last access: 26/02/2023).

Coase, R. H. (1960): The Problem of Social Cost, Journal of Law and Economics, 4, 386-405.

Cole, D.H. / P.Z. Grossman (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, in: Palgrave Dictionary of Law and Economics, Vol.3, 144-155.

Drexl, J. (2017): Designing Competitive Markets for Industrial Data – Between Propertisation 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, Available at SSRN: https://ssrn.com/abstract=4136484 or http://dx.doi.org/10.2139/ssrn.4136484 (last access: 26/02/2022)

Eckardt, M. (2001): Technischer Wandel und Rechtsevolution, Tübingen: Mohr Siebeck.

Eckardt, M. (2011): Legal Evolution between Stability and Change, in: Zumbansen. P. / Gralf-Peter C. (eds.), Law, Economics, and Evolutionary Theory, Cheltenham/UK, Northampton, MA: Edward Elgar, 202-225.

Eggertson, Th. (1990): Economic Behavior and Institutions, Principles of Neoinstitutional Economics, New York: 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).

European Parliament / Council (2016): 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 (General Data Protection Regulation), Official Journal of the European Union, L 119, 1-88, 4.5.2016

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, 1137–62.

Graef, I. / Husovec, M. (2022): Seven Things to Improve in the Data Act, DOI: 10.2139/ssrn.4051793

Harris, C. et al (2020): The Origins and Consequences of Property Rights, New York: Cambridge University Press, DOI: 10.1017/9781108979122.

Hennemann, M. / Steinrötter, B. (2022): Data Act – Fundament des neuen Datenwirtschaftsrechts?, Neue Juristische Wochenschrift, 75, 1481-1486.

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. (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. (2021a): Digital Revolution, Institutional Coevolution, and Legal Innovations, DOI: 10.2139/ssrn.3991012 (forthcoming 2023 in: European Business Law Review).

Kerber, W. (2021b): From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems, in: Drexl, J. (ed.): Data Access, Consumer Interests and Public Welfare, Baden-Baden: Nomos, 441-476.

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, Tübingen: Mohr Siebeck, 151-176, available open access at: https://www.mohrsiebeck.com/en/book/eigentum-in-der-digitalen-gesellschaft-9783161614927?no_cache=1 (last access: 26/02/2023).

Kerber, W. (2023): Governance of IoT Data: Why the EU Data Act will not Fulfill its Objectives, in: GRUR International, 72, 120-135, available at: DOI: 10.1093/grurint/ikac107.

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), https://cerre.eu/wp-content/uploads/2022/11/ImproveEffectiveness_DataAct.pdf (last access: 26/02/2023).

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, available at: DOI: 10.2139/ssrn.4125503.

Lessig, L. (1999): Code is Law and Other Laws of Cyberspace, New York: Basic Books.

Lévêque, F. / Ménière, Y. (2004): The Economics of Patents and Copyright, The Berkeley Electronic Press, July 2004.

Libecap, G. D. (1989): Contracting for Property Rights, New York: Cambridge University Press.

Martens, B. (2021), Data access, Consumer Interests and Social Welfare, in: Drexl. J. (ed.), Data Access, Consumer Interests and Public Welfare, Baden-Baden: Nomos, 69-102.

Martens, B. (2023): Pro- and Anticompetitive Provisions in the Proposed European Union Data Act Working Paper 01/2023, Bruegel, https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf (last access: 26/02/2023).

Mello, M.T.L. (2016): "Property" Rights and the Ways of Protecting Entitlements – an Interdisciplinary Approach, Revista de Economia Contemporanea 20, 430-457.

Metzger, A. / Schweitzer, H. (2023): Shaping Markets: A Critical Evaluation of the Draft Data Act, Zeitschrift für Europäisches Privatrecht, 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', https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf (last access: 26/02/2023).

Noto La Diega, G. (2023): The Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies, London and New York: 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. Cheltenham: Edward Elgar, http://reference.findlaw.com/lawandeconomics/2000-private-and-common-property-rights.pdf (last access: 26/02/2023).

Podszun, R. / Offergeld, P. (2022): The EU Data Act and the Access to Secondary Markets. Study for the Ludwig-Fröhler-Institut für Handwerkswissenschaften, available at: DOI: 10.2139/ssrn.4256882.

Rose-Ackerman, S. (1986): Efficiency, Equity and Inalienability, in: von der Schulenburg, J.-M. / Skogh, G. (eds.), Law and Economics of Legal Regulation, Kluwer: Springer Netherlands, 11-39.

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, 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 (last access: 26/02/2023).

Specht-Riemenschneider, L. (2019): Diktat der Technik. Regulierungskonzepte technischer Vertragsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht, Baden-Baden: Nomos.

Specht-Riemenschneider, L. (2022): Der Entwurf des Data Act, MMR, Zeitschrift für IT-Recht und Recht der Digitalisierung, 809-826.

Specht-Riemenschneider, L. / Kerber, W. (2022): Designing Data Trustees – A Purpose-based Approach. Datentreuhänder – Ein problemlösungsorientierter Ansatz, Konrad-Adenauer-Stiftung, Berlin, https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees.pdf/3523489b-2611-a12a-f187-3e770d1a9d94 (last access:16/02/2023).

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, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Data_Economy/ELI_Response_European_Strategy_for_Data.pdf; (last access: 16/02/2023)

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, 457-484.

Umbeck, J. (1981): A Theory of Property Rights: With Application to the California Gold Rush. Ames: Iowa State University Press.

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.

ANDRÁSSY WORKING PAPER SERIES

IN ECONOMICS AND BUSINESS ADMINISTRATION

ISSN 2560-1458

51 Eckardt, Martina, Kerber, Wolfgang. 2023. "Property rights theory, bundles of rights on IoT data, and the Data Act"

50 Bucher. Florian, Eckardt, Martina. 2022. "The EGCT as a Governance form for Cross-Border Cooperation – a Spatial Analysis of its Critical Success Factors"

49 Ade , Adrian. 2022. „The systematic view on literature – a bibliometric analysis of the research front."

48 Alexenko, Alina. 2022. „Geschäftsberichte als ein Forschungsobjekt und die Relevanz von Behavioral Economics für die Unternehmensberichterstattung."

47 Ginter, Tamás. 2022. „Lockdown policies: a review of political effects on restrictive measures."

46 Dötsch. Jörg J. 2021. „Theorizing emergence in framing complexity economics. A Reply."

45 Dötsch. Jörg J. 2021. „Houses, but in what order? Asymmetric recovery in Hungary's residential property market after the crisis."

44 Storch, Rainer. 2020. „Gemeinsamkeiten und Differenzen der Motive von Führungspersonen gewinnrealisierender und dauerdefizitärer Monopolunternehmen"

43 Wontke, Christoph. 2020. „Historische Kapitalanlageperformance deutscher Lebensversicherer im Vergleich zum Kapitalmarkt: Sind die Lebensversicherer besser als ihr Ruf?"

42 Eckardt, Martina. 2019. „Cross-Border Cooperation via the EGTC – A Study on its Main Drivers of Adoption at the Regional Level"

41 Sehic, Jutta. 2019. „Networking and knowledge transfer – Returnee entrepreneurship in the Western Balkans. Research report Bosnia and Herzegovina“

40 Jürgens, Jonas. 2019. „Die Agenda zur besseren Rechtsetzung der Juncker-Kommission: Wirksamer Beitrag zur Stärkung der Union?“

39 Dörstelmann, Felix A. 2019. „Wettbewerb zwischen PEPP und PPP – Zur theoretische Modellierung des potenziellen Wettbewerbs zwischen pan-europäischen und nationalen Altersversorgeprodukten“

38 Sehic, Jutta 2018. „Novelty and links in innovative firms' networks: An analysis of SME in Central and South Eastern Europe“

37 Eckardt, Martina and Stefan, Okruch 2018. „The Legal Innovation of the European Grouping of Territorial Cooperation and its Impact on Systems Competition“

36 Wickström, Bengt-Arne, Templin, Torsten and Gazzola, Michele 2017. „An economics approach to language policy and linguistic justice“

35 Megyeri, Eszter 2016. „Altersarmut und Wohneigentum in der EU – Eine Analyse mit EU-SILC 2014 Daten“

Frühere Ausgaben sind in der Reihe:

ANDRÁSSY WORKING PAPER SERIES / ISSN 1589-603X

erschienen**:**

XXXIV Dötsch, Jörg. 2015. „Building a knowledge economy: is Hungary turning the right screw?“

XXXIII Hornuf, Lars und Lindner, Julia 2014. „The End of Regulatory Competition in European Law?“

XXXII Eckardt, Martina 2014. „The Impact of ICT on Policies, Politics, and Polities – An Evolutionary Economics Approach to Information and Communication Technologies (ICT)“

XXXI Eckardt, Martina 2014. „Legal Form and Internationalization of Small and Medium_Sized Enterprises in the EU“

XXX Dötsch, Jörg 2013. „Ökonomik und Emergenz. Arbeitspapier zum Emergenzbegriff der Heterodoxie"

XXIX Dötsch, Jörg 2013. „Überlegungen zu Prozessen endogener Destabilisierung von Wettbewerbswirtschaften"

XXVIII Eckardt, Martina und Kerber, Wolfgang 2013. „Horizontal and Vertical Regulatory Competition in EU Company Law: The Case of the European Private Company (SPE)"

XXVII Eckardt, Martina. 2012. „The Societas Privata Europaea – Could it Promote the Internatinalization of Small and Medium-Sized Enterprises?"

XXVI Ebert, Werner und Eckardt, Martina. 2011. „Wirtschafts- und finanzpolitische Koordinierung in der EU – Erfahrungen aus einem Jahrzehnt Politikkoordinierung"

XXV Eckardt, Martina und Räthke-Döppner, Solvig. 2008. „The Quality of Insurance Intermedieary Services – Empirical Evidence for Germany"

XXIV Okruch, Stefan und Alexander Mingst. 2008. „Die Kammerorganisation aus evolutorischer Sicht".

XXIII Mingst, Alexander. 2008. „Politische Prozesse und die Rolle von Ideologien: Sinnvolle Geschichten in einer ungewissen Welt".

XXII Mingst, Alexander. 2008. „Evolutionary Political Economy and the Role of Organisations".

XXI Mingst, Alexander. 2008. „The Organizational Underpinnings of Innovation and Change in Health Care".

XX Okruch, Stefan. 2007. "The 'Open Method of Coordination' and its Effects: Policy Learning or Harmonisation?

XIX Okruch, Stefan. 2006. "Die 'Offene Methode der Koordinierung': Gefahr schleichender Harmonisierung oder Chance für Politiklernen?"

XVIII Okruch, Stefan. 2006. "Values and Economic Order: In Search of Legitimacy"

XVII Okruch, Stefan. 2006. „Die EU-Wettbewerbspolitik zwischen Einheitlichkeit und Vielfalt – Anmerkungen aus ordnungsökonomischer Sicht“

XVI Beckmann, Klaus B. 2006. “Tax evaders keep up with the Joneses”

XV Margitay-Becht András 2005 “Inequality and Aid. Simulating the correlation between economic inequality and the effect of financial aid”

XIV Beckmann, Klaus B. 2005. “Tax competition and strategic complementarity”

XIII Meyer, Dietmar – Lackenbauer, Jörg. 2005 „EU Cohesion Policy and the Equity-Efficiency Trade-Off: Adding Dynamics to Martin’s Model”

XII Chiovini, Rita und Zsuzsanna Vetõ. 2004. „Daten und Bemerkungen zu den Disparitäten im Entwicklungsstand ausgewählter Länder”

XI Alfred, Endres. 2004 „Natürliche Ressourcen und nachhaltige Entwicklung”

X Bartscher, Thomas, Ralph Baur and Klaus Beckmann. 2004 „Strategische Probleme des Mittelstands in Niederbayern”

IX Arnold, Volker – Hübner, Marion. 2004. „Repression oder Umverteilung - Welches ist der beste Weg zur Erhaltung der Funktionsfähigkeit marktwirtschaftlicher Systeme? - Ein Beitrag zur Theorie der Einkommensumverteilung.”

VIII Okruch, Stefan. 2003. „Verfassungswahl und Verfassungswandel aus ökonomischer Perspektive - oder: Grenzen der konstitutionenökonomischen Suche nach der guten Verfassung.”

VII Meyer, Dietmar: „Humankapital und EU-Beitritt – Überlegungen anhand eines Duopolmodells.”

VI Okruch, Stefan. 2003. „Evolutorische Ökonomik und Ordnungspolitik – ein neuer Anlauf”.

V Arnold, Volker. 2003. „Kompetitiver vs. kooperativer Föderalismus: Ist ein horizontaler Finanzausgleich aus allokativer Sicht erforderlich?’

IV Balogh, László – Meyer, Dietmar. 2003. „Gerechtes und/ oder effizientes Steuersystem in einer Transformationsökonomie mit wachsendem Einkommen’.

III Beckmann, Klaus B. 2003. „Tax Progression and Evasion: a Simple Graphical Approach".

II Beckmann, Klaus B. 2003. „Evaluation von Lehre und Forschung an Hochschulen: eine institutenökonomische Perspektive".

I Beckmann, Klaus B. and Martin Werding. 2002. „Two Cheers for the Earned Income Tax Credit".

Visit us on the web at http: www.andrassyuni.eu. Please note that we cease to circulate papers if a revised version has been accepted for publication elsewhere.