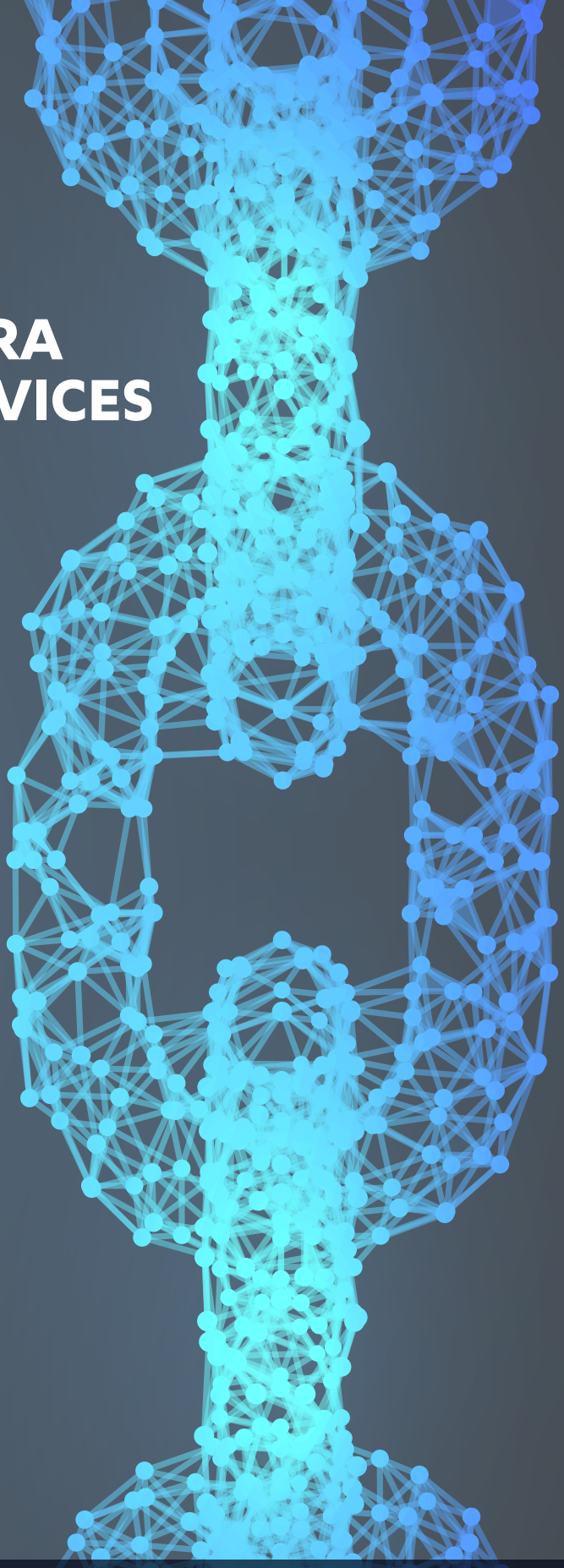
DATA ACCESS AND CONTROL IN THE ERA OF CONNECTED DEVICES



BEUC The European Consumer Organisation

Study on behalf of BEUC
by Prof. Josef Drexl
contact: Agustin Reyna - competition@beuc.eu

Data Access and Control in the Era of Connected Devices

Study on Behalf of the European Consumer Organisation BEUC

Josef Drexl*

This Study was conducted under a contract of the author with BEUC. The contract was concluded on the author's personal behalf. Therefore, the Study only reflects the personal opinion of the author and can neither be attributed to the Max Planck Institute for Innovation and Competition as an institution nor to any other person working at this Institute.

* Professor, Dr iur (Munich), LLM (UC Berkeley), Director of the Max Planck Institute for Innovation and Competition, Munich; Honorary Professor of the University of Munich.

Executive Summary

1 Introduction

(1) This Study aims to contribute to the current debate on the future EU legal framework for the digital economy. Its particular focus is on connected devices, such as connected machines used in different fields of the economy (eg, manufacturing, construction, agriculture) as well as connected devices that are often used by consumers (eg, vehicles, household machines, wearables, meters, mobile telecommunications devices).

(2) Connected devices collect and process large amounts of personal and non-personal data. Therefore, the Study analyses the already existing regime regarding such data and explores its future development. Responding to the policy debate on the EU level, in particular the so-called European Data Economy Communication of the Commission of 11 January 2017, the focus will be on ownership rights in data and the potential need to enhance access to data.

(3) The Study takes particularly account of the interests in the protection and use of personal data as well as the interests of consumers as buyers and users of connected devices. Therefore, the Study puts a particular emphasis on exploring the relevance of the EU data protection rules for the topic and evaluates how EU consumer contract law should be applied and further developed with regard to connected devices.

(4) The Study argues against the adoption of any data ownership regime, including a data producer's right. In contrast, it recommends exploring potential future legislation on data access regimes. Data access regimes should preferable be adopted for specific sectors. Yet the Study recognises the benefits of a generally applicable data access regime. This is why the Study finally identifies key elements of legislation on a general data access regime, which can also be used as guidelines for more targeted sector-specific data access legislation.

2 Basic concepts and issues

(5) For the purpose of this Study, connected devices are understood as all devices that (1) are connected with other things and persons through wireless or wired communication and (2) generate data.

(6) A clear distinction has to be made between 'owning data', based on a property right *in rem*, and mere 'holding of data'. Especially the manufacturers of connected devices will technically be able to control access to data, without having to rely on a property right in data. Manufacturers as 'data holders' can therefore commercialise machine-generated data by entering into licensing contracts with third persons and exclude other persons from access by refusing such licensing. While *de facto* control thus provides factual exclusivity—at least with *inter partes* protection based on contract law—, such factual control of data should not be confused with data ownership. Although legal recognition of licensing contracts does not constitute a neutral allocative choice, attribution of a new data ownership right to another person would also have to face the challenge to overcome *de facto* control exercised by a data holder who is unwilling to grant data access for free. This

shows that remedies providing for data access, whether as part of a data ownership regime or as targeted data access rights, should be placed at the centre of the policy debate.

(7) The discussion on 'who owns the data' runs the risk of ignoring the preliminary question of whether there is a justification for recognising ownership in data. The frequently stated economic value of data does not provide such justification. Quite the contrary, data as information goods are non-rival and, therefore, will not be exhausted by their use. This means that social welfare will in principle be maximised by guaranteeing full access to data. This explains why unrestricted data access should be considered the default rule, while introduction of exclusive rights is in need of a special justification. This analysis is supported by the constitutional principle of freedom of information and the public interest in access to data.

(8) Intellectual property law and trade secrets law present legal instruments for the protection of information. Yet patent law, which provides ownership in technical information, cannot be relied upon as a role model for the recognition of a data ownership right. Patent law is based on the assumption that without protection investment in inventive activity would be suboptimal, while at the current stage of the data economy, it can hardly be argued that there is not enough investment in the production of data. On the contrary, competitive pressure seems to fuel the development of connected devices and the generation of myriads of digital data. In addition, the patent registration system, especially compared with trade secrets protection as an oftentimes imperfect option for inventors, enhances access of the public by both publishing the invention and limiting patent protection in time. Finally, patent law provides for qualitative requirements for an invention to be protected to guarantee a positive innovation trade-off for society. No such qualitative requirements have so far been discussed, even less identified, with regard to data ownership.

(9) Similarly, European copyright law is characterised by an information policy, which is guaranteed by the standard of copyrightability. In principle, copyright law does not protect information as such. By only protecting the creative parts of works, copyright law even provides incentives for investment in business models that are designed to provide information, thereby promoting the free flow of information. Yet the fringes of how far intellectual property protection can go are reached on the EU level with the recognition of a sui generis protection regime for databases. The ongoing critical debate on the appropriateness of this system highlights the risk that any legislation on data ownership would run if legislation only looked at the value of the data without also assessing the negative effects on the economy and society at large.

(10) Strong rights of control over information are provided by the General Data Protection Regulation (GDPR). Yet such protection is limited to personal information and justified by the privacy interest of the data subjects as protected by the EU Charter of Fundamental Rights. The existence of these data protection rules cannot be taken as a justification for transforming these rights into a property rights regime. Although the data subject my make use of her rights in a commercial context, especially by giving consent to the collection and processing of personal data as a means to receive a digital service, the scope of the data protection rules is limited by the underlying privacy interest. This is why the GDPR does not give a right to participate in the income generated by the use of personal data in secondary markets. Hence, the mere character of data as personal data does neither require nor argue in favour of recognising an economic data ownership right in personal data.

(11) Hence, the question remains whether there is a reason for legislative intervention in the first place. The Commission, in its European Data Economy Communication of January 2017, identifies data lock-ins of the owners or long-term users of connected devices as a particular market failure, which could be remedied by a potential data producer's right. Hereby, the

Commission refers to situations where the supplier of a given connected device would require the customer (consumer) to also purchase other connected devices and receive connected data-based services from this same supplier. In contrast, access to the machine-generated data would help to maintain more competitive markets by enabling the owner or long-term users of a connected device to connect the devices of different manufacturers and receive data-based services from third-party service providers.

(12) In principle, it would be for EU competition law to overcome such data lock-ins. Yet the case-law of the CJEU makes it very difficult to argue a refusal to grant access to data as an abuse of market dominance under Article 102 TFEU. To prove market dominance in data-related markets is an extremely difficult undertaking and highly case-specific. Similarly, the very high requirements for an abuse were developed for different situations and may need to be adapted to those related to connected devices. More importantly, only competitors would be able to rely on a right to access data under Article 102 TFEU, which would generally exclude access claims of consumers. Finally, the enforcement system of competition law does not seem effective enough to guarantee competitive markets for the mass phenomenon of data lock-ins caused by connected devices. Hence, the better approach would consist in competition-oriented regulation.

(13) Nor can such data lock-ins effectively be remedied within the realm of European contract law. While data lock-ins can also be understood as a problem of unequal distribution of bargaining power, the Commission has quite rightly identified two obstacles for a contract law solution that are extremely difficult to overcome. First, the scope of application of the Unfair Contract Terms Directive would need to be extended to business-to-business relations. Secondly, for creating a benchmark for the unfairness test, default contract law rules regarding access to machine-generated data would be needed. Addressing both issues on the level of the EU law instead of national law would break with the traditional focus of EU contract law on consumer contracts and, therefore, cause considerable resistance on the part of the EU Member States. More importantly, the person interested in access to the data will not necessarily have concluded a contract with the data holder. Therefore, a contract law solution would not help in all cases where data access is needed.

(14) Still, the idea of the Commission to adopt a data producer's right also raises concerns. On the one hand, as a right *in rem*, it may go too far by creating too much exclusivity. Such a right, with the owner or long-term user of the connected device as the data producer and, hence, holder of the right, would burden the licensing of the aggregated and much larger datasets of the manufacturers with considerable transaction costs caused by the need to clear rights. To force such licensees to take a direct licence from the individual 'data producers' is not an option either, since access to the individual datasets of the data producers will not constitute a viable substitute to access to the aggregated dataset of the manufacturer of the devices—not to mention that licensing by the manufacturer has the transactional benefit of a one-stop shop for potential licensees, liberating them from the need to conclude many more licensing contracts with the individual data producers. On the other hand, recognition of a data producer's right as an intellectual property right does not go far enough because it will not remedy the underlying unequal distribution of bargaining power. Under an intellectual property regime, the more powerful manufacturer can still include a clause in its contracts according to which ownership in the data will be transferred for free to the manufacturer.

(15) The more adequate solution therefore lies in the recognition of non-waivable data access rights. Such rights can specifically target the underlying market failure of data lock-ins, simultaneously avoiding unjustified exclusivity and protecting against a buy-out vis-à-vis the manufacturer of the device who may frequently be in a superior bargaining position. Such rights should be clearly distinguished from any property concept to avoid confusion. A

property right would typically include the freedom to transfer property in the subject-matter of protection, which however needs to be excluded here to remedy the underlying market failure effectively. In addition, apart from specific situations such as in the field of copyright law, intellectual property regimes do not, and do not need to, include a right of access to the subject-matter of protection or copies therefrom.

(16) Preference for data access rights is also supported by an analysis of how connected devices generate and process data. Especially in more complex cases of interconnected and autonomously acting devices, such as in the case of automated or even autonomous driving, data is generated and analysed through sequences of data analyses where the board computer of a motor vehicle will not only rely on data generated by this vehicle but also on data supplied from outside sources. Hence, under such circumstances, data generation and analysis take place in most complex networks of multiple actors who contribute to the generation of economic value. To consider the driver or the holder of the car the data producer owning all the data collected and processed in a vehicle, will neither be justified from a technical nor economic perspective. In addition, such allocation of the right would ignore that a lot of the data in a connected vehicle is, or is based on, external data already owned by other persons. Recognition of a data ownership right *in rem*, also enabling the rightholder to generate income from secondary markets, would create insurmountable obstacles of identifying the rights of many rightholders in such complex networks with several layers of potential rights and rightholders in often 'derivative data' that are generated through many steps of data analysis. In contrast, data access rights, as the much less intrusive form of regulation, avoid such problems. This approach does not require any rights clearing where networks of data generation are set up nor will it have to face the issue of complicated allocation of rights in such networks. The question is only whether a person with a legitimate access interest has a respective claim against the *de facto* holder of the data.

(17) Another argument is that data ownership also has the potential of restricting free flow of information. Advocates of a data producer's right try to avoid this effect by limiting data ownership to 'raw data' on the so-called syntactic level of information. While it is true that such ownership would not relate to the semantic level of information where data conveys meaning, advocates of ownership in raw data overlook that the economic value of the data arises from the semantic level of information and that access to this level will oftentimes require use of the digitally encoded information. Hence, in case where somebody wants to analyse a digital dataset to find valuable information, it has to make use of the raw data in which information is encoded. Hence, information on the semantic level would not be accessible without the clearing of rights in the raw data.

(18) Connected devices will often collect and process personal and non-personal data. To preserve full application of the data protection rules of the GDPR, the Commission discusses a potential data producer's right by limiting it to non-personal data. Yet this overlooks that in the light of the broad definition of personal data in the GDPR, a bright line between non-personal and personal data can no longer be drawn. At the same time, limitation of legislation to non-personal data would considerably reduce the scope and relevance of new legislation. The Commission's idea to anonymise personal data to bring it within the scope of potential legislation on a data producer's right cannot convince either, since data analytics is by now often powerful enough to de-anonymise data. Moreover, this proposal overlooks that the person anonymising the data will typically be the manufacturer who is in *de facto* control of the data. Here, the Commission fails to explain why the owner or the long-term user of the connected device will acquire a data producer's right in anonymised data if the anonymisation is undertaken by a different person. In contrast to the Commission, from a legal point of view, personal data protection does not exclude parallel recognition of a data producer's right in the same data. The underlying conflict could be

solved by giving precedence to the data protection rights of the data subject including the right to erasure. Yet such combination would considerably reduce the effectiveness of legislation on the data producer's rights as an exclusive right encumbered by data protection rights of others. Such problems are avoided by data access rights. The data access and data portability rights of the data subject arising from the GDPR could even serve as a model for legislation on additional data access rights. Data access rights could in principle also be construed with regard to personal data relating to another person. But, in such case, the data access regime should fully preserve the data protection rights of the other person pursuant to the GDPR.

3 Objectives of regulation and relevant interests

(19) For assessing the adequacy of the existing legal framework and for guiding proposals for future reform, the Study relies on a theory of regulation according to which four different objectives and the interaction between them need to be considered. These four objectives are: (1) establishing functioning and competitive market for the data economy; (2) promoting innovation; (3) protecting consumer interests with a particular focus on protecting the privacy of natural persons; and (4) promoting additional public interests.

(20) The commercial interests of those who implement new business models of the digital economy, including their fundamental right of doing business, are considered at the other side of the balancing process. The four objectives are to provide a complete spectrum of the justifications for regualtion in the digital sector. Accordingly, the regulatory theory applied here reflects all public interest grounds and rights of others that are constitutionally recognised. Arguments that cannot be captured by the four objectives, such as mere justice considerations, should therefore be excluded from the analysis.

(21) The starting point of the theory is the first objective. To guarantee functioning and competitive markets is the very purpose of the economic regulation with the contract law system and competition law as its key legal components. Secondly, digitisation and, more specifically, the advent of connected devices, also expresses an enormous innovation. Thirdly, digitisation also comes with increased challenges for society, especially due to the collection of vast amounts of personal data. In this regard, data protection has become the primary concern for consumers. Fourthly, the digital economy is also relevant from the perspective of many other public policy grounds, such as safety of driving, public health and protection of the environment. Most importantly, legislation has to safeguard freedom of information and free flow of information. Since the business models of the digital economy nowadays also influence the distribution of politically relevant information and impact the political opinions of the citizens, safeguarding the democratic process is another public interest to be taken account of.

(22) Against the backdrop of the first objective, adoption of both a new data ownership right and data access rights would be in need of an economic justification in the light of a market failure analysis. Both kinds of rights have to be considered as functional rights that should only be recognised by the legislature if they can be expected to contribute to a better functioning of the markets. In contrast, allocation of new data ownership rights to single stakeholders, such as the owner or long-term user of a connected device, should not merely be based on justice considerations. New ownership rights, the only function of which is to distribute the economic value of of data differently than an unregulated market, would only produce additional transaction costs, thereby reducing economic efficiency to the prejudice of society at large.

(23) Digitisation of the economy also has to be viewed as a major driver of innovation in various regards. As regards connected devices, digitisation brings about product innovations, offering products with more utilities, more safety and more convenience. For firms, smart manufacturing also brings benefits in form of process innovations, above all allowing them to produce at lower costs and to offer various goods, not only connected ones, at lower prices to consumers. Digitisation also brings about organisational innovations, optimising the production processes in the framework of 'smart manufacturing' or 'smart farming' and revolutionising the distribution of goods in the logistics sectors. In this context, also companies that depend on data access for offering data-based services to manufacturers or farmers have to be considered innovators. Finally, digitisation enables marketing innovations in form of new business models including those that make use of consumer data and provide consumers with goods and services without requiring them to pay. With some exceptions such as innovations in the field of mobile telecommunications technologies, these innovations are not primarily driven by incentives created by intellectual property rights, but competitive pressure in an era of a rapid digital transformation.

(24) The privacy concerns arising from the use of personal data has to broaden the regulatory perspective. As a fundamentally non-economic concern, personal data protection is characterised by a very complex relationship with the objectives of both guaranteeing functioning markets and enhancing innovation. On the one hand, data protection rules seem to be in conflict with these two objectives by imposing additional restrictions on companies when they develop innovative business models for the digital sector. This argues for the application of a proportionality principle when adopting data protection rules that need to be respected by businesses active in the digital sector. On the other hand, however, personal data protection can even be regarded a condition for the functioning of markets in the digital sector as well as a driver of innovation. Consumers will be less willing to buy connected devices if the law does not guarantee certain standards of data protection. This is very similar to the situation of industrial customers who would be more hesitant to buy connected machines if the law did not guarantee a certain level of trade secrets protection. Moreover, data protection can be explained as a remedy to a specific market failure. Data protection should be considered a potential competition parameter. But this parameter does not work well in practice due to unequal distribution of information. Consumers cannot monitor whether the data protection commitments offered to them are in fact respected. Finally, data protection rules can also enhance innovation by setting incentives for software programmers to work on innovative technical solutions that help implement the data protection rules.

(25) Personal data protection nowadays has to be considered a most important consumer concern in markets for connected devices. Yet the role of data in the framework of consumer transactions is particularly complex. A consumer making a choice between a connected car and a traditional car will be most interested in, first, protection of the personal data and, secondly, the safety of driving. Yet save automated or even autonomous driving depends on access and use of personal data by the manufacturer. Thereby, the data is collected and processed in the consumer's own interest. From this it can be concluded that, where use of personal data is needed to guarantee the well-functioning of the device in the interest of consumers, provision of personal data should not be defined a counter-performance of the consumer. Furthermore, consumer choice will not be substantially influenced by whether, as purchasers of a connected device, consumers will also be recognised as holders of a data ownership right, including a right to control the commercialisation of their data in secondary markets. In a case of connected devices, the ownership right cannot be expected to provide consumers with additional income, since manufacturers could not only claim the transfer of the data rights under their contracts with consumers, but also vector in the data ownership right of consumers by raising the sales

price for the connected device upfront. This shows that in circumstances where the parties are related by contractual transactions or a chain of such transactions, the income from the commercialisation of data in secondary markets will still be distributed according to the bargaining power of the parties and the competitive conditions in the market, irrespective of how the legislature allocates ownership rights in the data.

(26) As part of the fourth objective, freedom of information and the more general public interest in free flow of information should be considered as the most important public interest concern. Freedom of information and free flow of information is a complementary consideration to the first and second objectives of guaranteeing functioning markets and enhancing innovation. In the absence of a market failure, the default rule of free flow of information should prevail. Access to information as a non-rival good will help society to make maximum use of information to promote the economic well-being of society. At the same time, free flow of information will help disseminate innovation and enable more people and businesses to build on it to generate follow-in innovation. Yet there are also limits. Free flow of information has to be limited where it would otherwise reduce the ability of undertakings to compete. This line is drawn by trade secrets law. Similarly, patent law makes an exception from free flow of information where otherwise the generation of new technical knowledge would be suboptimal. Most importantly, freedom of information has to be balanced against the data protection interests of individuals. Yet freedom of information has yet a separate political dimension. Since digital business models, such as those of social platforms have nowadays also become major intermediaries influencing political discourse and even elections by selecting and distributing politically relevant information and opinions, the law also has to take into account the impact of such business models on democracy. Preserving a functioning democratic society has to be considered a separate public interest concern, since the potentially negative implications of unregulated digital business models for democracy cannot be captured by a purely economic market failure analysis of such markets as part of the first objective or viewed as a particular individual consumer interest in the framework of the third objective.

(27) The regulatory theory applied in this Study can also help assess proposals originating from other sources. Against the backdrop of this theory, two kinds of fallacies can be observed. The first fallacy consists in exclusive reliance on one objective while the other objectives are ignored. For instance, this is the case when authors argue that workable data markets are in need of data ownership. This argument only relies on the first objective, without taking into account the costs caused by restricting free flow of information, on the one hand, and the potentially colliding privacy interests relating to personal data, on the other hand. The second fallacy is characterised by giving full precedence to one objective over the other. An example is presented by the merely justice-based argument that an economic ownership right has to be recognised against the backdrop of the existence of personal data protection, evading a thorough discussion and analysis of the impact of such a right on how data markets would work.

4 The existing and evolving legal framework of the EU for the data economy

(28) While there is no EU or national legislation that specifically deals with property rights in data, several protection systems may be relevant for providing some property or property-like protection.

(29) In particular, the General Data Protection Regulation (GDPR) vests very strong control rights over personal data in the data subject. Yet this does not make the existing data protection

rules of the GDPR the basis of an already existing data ownership right. The fundamental right's basis of the GDPR is the right to data protection and not the property clause of the Charter of Fundamental rights. The data protection rules of the GDPR are not designed as exclusive rights of the data subject, but as a form of personal protection, based on a balancing, *inter alia*, with the fundamental rights of others, most importantly the right to freedom of expression. This fundamental right's perspective translates into a design of the GDPR according to which personal data is not protected as such against the use of third persons, but only against certain forms of data processing that appear as particularly harmful to the data protection interests of natural persons. Although, with the rights to withdraw consent at any time and to claim erasure, the GDPR provides for control rights that go even beyond intellectual property rights, these rights in particular argue against a property right's dimension of the GDPR. These rights are inspired by the goal to preserve the autonomy of the data subject; they thereby run counter to the function of property rights systems to enable the rightholder to maximise economic value of the subject-matter of protection by permanently licensing the use of it to others. The GDPR comes closest to a property rights concept with its data portability right in Article 20 GDPR, which also has the function to protect the economic interest of the data subject in switching suppliers more easily. Yet this does not transform the GDPR in its entirety into property right's legislation. The same holds true for the possibility of the data subject to make economic use of her consent for the purpose of receiving digital services without any monetary consideration. Here, the GDPR only respects the autonomous motivation of the data subject when giving consent to the data processing.

(30) The fact that current EU data protection law does not provide any property right in data would by itself not exclude future legislation of an economic ownership right in personal data as a second pillar of protection. However, two major arguments argue against such legislation. First, the fundamental right to data protection does not require such a right. Quite on the contrary, the GDPR has conclusively spelled out the data protection rules for the EU, balancing all relevant fundamental rights and interests involved. This does not leave any room for arguing that the fundamental right to data protection requires a second prong of economic rights. Hence, such an ownership right would be in need of a completely separate property rights justification in the light of the property clause of the EU Charter of Fundamental Rights. Secondly, a data property regime that is specifically limited to personal data would fail to meet the essential requirement for a workable intellectual property regime. Such property right would not allow, given the difficulties to distinguish personal from non-personal data, to clearly identify the existence of individual rights. Moreover, given the myriads of rights that would exist and would come into existence through multiple steps of data analysis, such rights would not provide a sustainable framework for guaranteeing economic participation of the rightholders in the income generated from the commercialisation of the data. And finally, the right to revoke consent and the right to erasure make it impossible to transfer or license the economic rights to others with a sufficient degree of stability. Quite the contrary, if the legislature would adopt a second prong of ownership in personal data, including the right to permanently license the use of personal data or, even more to transfer the right as such, such legislation would curtail the privacy interests of the data subject as they are currently recognised by the GDPR.

(31) The most obvious legal basis for already existing intellectual property protection in data is the sui generis database right. Yet legal writing so far has mostly argued that such protection will typically not be available in big-data cases. This is explained by the fact that the Database Directive only protects databases, as compared to data as such, as well as the early judgments of the CJEU in the *Fixture Marketing* and *British Horseracing* cases excluding investment in 'creating' data, as opposed to 'obtaining' data, for assessing the essentiality of the investment as the key requirement for the coming into existence of the

sui generis right. However, a more thorough analysis shows that that recent case-law both of the CJEU and on the national level have led to a broad reading of the concepts used by the Directive for the sui generis database protection regime. This includes the concept of a database, the concept of essentiality of the investment and the scope of protection. In particular, national case-law for instance in Germany takes into account investment in observing data for assessing substantiality. This may prove most important for connected devices since, through the sensors embedded in them, these devices often register and collect data coming from outside the device. In sum, recent case-law makes it quite likely that in many instances sui generis data protection may be available in the context of machine-generated data.

(32) Especially from the perspective or the owner or long-term user of a connected device, potential availability of a sui generis database right has to be considered a problem rather than a benefit. As confirmed by the recent evaluation of the working of the Database Directive, sui generis database rights are more likely to be vested in the manufacturer of the device, while the Commission considered adoption of a data producer's right of the owner or long-term user of a connected device as an instrument to unlock data held by the manufacturer. Hence, sui generis database rights relating to machine-generated data will often strengthen the anyhow existing lock-in effects. Moreover, adoption of a data producer's rights would not have the effect of addressing this problem. Such legislation would only create a second layer of rights that would not promote access of the 'data producer' to the data contained in the protected databases of the manufacturer. Rather, such legislation would only create more exclusivity, in particular increasing the barriers to data access for third parties. In the light of these barriers to data access, introduction of a compulsory licensing system as initially proposed by the Commission more than 20 years ago, but finally rejected by the European legislature, is now not only reconsidered as a solution in legal writing, but also as a potential reform in the Final Report on the evaluation of the Directive. Still, the Commission seems to prefer to do nothing. In contrast, this Study recommends the EU legislature addressing the problems created for free flow of data by potential sui generis database rights. As the analysis of the regulation of the data access right under Article 15(4) and the data portability right under Article 20(4) GDPR shows, this task has not even been accomplished for the case in which data subjects seek access to personal data. In contrast to doing nothing or to introducing a compulsory licensing system, as advocated by other scholars, this Study recommends giving precedence to data access regimes over sui generis database rights. Such legislation will not harm any legitimate interests of the manufacturers of connected devices, since the manufacturers would still be able to recoup their investment by charging a respective price when they sell the device.

(33) Other intellectual property systems could give rise to 'data ownership-like' protection in specific situations. This can even be imagined for copyright law, despite its inbuilt features that safeguard free flow of information. As a currently emerging issue, copyright protection for application programming interfaces (APIs), use of which is important for establishing data interoperability, presents considerable potentials of restraining access to data. Emerging practice in the US shows that copyright protection of APIs should also be considered a serious concern in the EU. In addition, patent law could equally restrain access to information if the information generated through the application of process patent, for instance, granted for a diagnostic test, were to be considered a product in the sense of derivative product protection. Against the backdrop of the lack of EU harmonisation in the field, this question is still to be decided under the national laws of the Member States. German patent law practice shows that there are ways to guarantee that the patent laws avoid undue restrictions on free flow of information.

(34) Recognition of data ownership can also be discussed as part of the civil law concept of property. Such recognition is especially important in jurisdictions where tort liability

depends on prejudice caused to absolute rights such as property. Here, the different economics of data as a non-tangible item has to be taken into account. Therefore, it makes perfect sense to provide tort liability to protect the integrity of data against undue interference by others, while rejecting absolute protection against unauthorised use of the data. Data security can be guaranteed by different legal means, including criminal law. Protection of the integrity of data in the private interest of *de facto* data holders pursuant to criminal law does not have to be interpreted as a recognition of civil property in the data. Private and criminal law protection of the data held by the manufacturer as the *de facto* holder of the data is also in the interest of the owner and the long-term user of connected devices, since such protection helps to safeguard the integrity of data to which the latter may seek access.

(35) In contrast to the sui generis database right, EU trade secrets protection has to be considered a useful tool to improve the working of the data economy with regard to data generated by connected devices. The EU Trade Secrets Directive achieves this goal by establishing a more balanced system that allows to take the interests of other market participants, including their interest in access to data, into account. Conceptually, although the regime protects data on the semantic level, the Directive does not protect against any unauthorized use of trade secrets but only against specific forms of illegal conduct which typically requires a breach of confidentiality obligations. On the operational level, excessive protection of data protection is avoided in various regards, namely, as regards the definition of trade secrets, the scope of protection and, finally, the remedies. In particular, the judge is given broad discretion to decide cases flexibly in the light of fairness considerations. Protection of trade secrets against third persons that are not directly bound by confidentiality obligations goes very far, but this is still acceptable in the light of the knowledge requirements for liability.

(36) The EU Trade Secrets Directive creates many legal uncertainties with regard to its application in a digital environment. Yet the Directive can be fruitfully applied also with regard to data collected by connected devices. As the *de facto* data holder, the manufacturer of connected devices is the most obvious candidate for making use of the protection system of the Directive. Trade secrets protection would add a second layer of legal protection to the *de facto* exclusivity already enjoyed by the manufacturer. Still, this protection system can also be used by commercial customers acquiring connected devices. By imposing confidentiality obligations on the manufacturer, commercial customers such as operators of smart factories, can acquire protection against undue communication of trade secrets collected by the devices to third persons. The definition of trade secrets is flexible enough to also cover big datasets whose commercial value only arises from the possibility to discover valuable information through the means of big data analytics. In addition, the Directive can be interpreted broadly as regards the scope of protection to also apply to the use of information that was generated through means of data analytics in secondary markets. Personal data collected by connected device are also capable of constituting trade secrets of the manufacturer. Trade secrets protection of the manufacturer may even serve the personality interests of the data subject by providing additional protection against misappropriation of personal data by third person, which will be enforced by the manufacturer. Yet conflicts may arise where data subjects rely on their rights to access data, erasure or data portability. In this regard, the GDPR and the Trade Secrets Directive have not consistently solved the conflict. In particular, Article 15(4) and 20(4) GDPR should not be read in the sense that protection of personal data as trade secrets of the data processor prevails over the rights of the data subject.

(37) In contrast, the idea of the Commission to introduce defensive rights against misappropriation of raw data as a potential alternative to a data producer's right has to be rejected. At first glance, this idea seems to have the beauty to avoid the exclusivity of the

intellectual property rights in favour of a mere liability approach following the example of trade secrets protection. However, if such protection were granted to the manufacturer of connected devices, the problem would be that such a system would circumvent all the limitations that are implemented in the Trade Secrets Directive that aim to reach a fair balance of interests, without requiring the manufacturer to make any additional efforts to secure protection. The fact that such protection would be limited to raw data would not mitigate the problem since protection of data on the syntactic level can equally create considerable barriers to free flow of information. Yet such protection could in principle also be granted to the owners or long-term users of connected devices as consumers to whom trade secrets protection is not available. But the interests of consumers cannot justify such protection. As regards the use of personal data, the GDPR already sufficiently protects the privacy interests of consumers. Beyond this, consumers cannot rely on the competition-enhancing effect of such protection of either personal or non-personal data collected by connected devices they own or use for conducting their business. In sum, the negative impact of the defensive rights approach arises from both the lack of substantive requirements for the acquisition of such rights and very far-reaching, IP-like remedies at the enforcement level. This shows that such defensive rights would be even more detrimental to the working of the data economy than sui generis database rights.

(38) As regards data generated by connected devices, consumers are currently protected by exclusive property rights only to a limited extent. Where consumers own the device, they may be able to rely on their property in the device to claim national tort law protecting where a third person harms the integrity of the data stored on the device. National tort law may also recognise similar protection for a consumer who only uses a connected device, without being the owner of the device, and a third person deletes data collected by the connected device. Depending on the national tort law system, the latter may require recognition of property of the consumer in the dataset as such.

(39) The data protection rights under the GDPR are the strongest rights consumers can currently rely upon regarding personal data collected and processed by connected devices. From an economic perspective the right to data portability in Article 20 GDPR is particularly important. It is designed to enable the data subject to switch a supplier more easily. The provision should be interpreted broadly, namely, in the sense that 'observed' data that is collected from the user of a connected device should be covered as data 'provided by the data subject'. Still, this provision does not apply to 'inferred' or 'derived' data that is only generated through additional steps of data analyses, which considerably limits the scope of the right regarding data processed by a connected device. In addition, reliance on the right is restricted technically by problems of data interoperability. Article 20 GDPR does not impose any obligation on the data processor to enable data interoperability, nor is any other potential supplier under an obligation to accept the data transfer. Yet the scope of application is very broad in other regards. The right to data portability does not depend on the termination of the contract. Article 20(2) GDPR empowers the data subject to claim direct transmission of the data to another controller. In this vein, the data portability right should also be considered to encompass a right to claim real-time data sharing with another controller.

(40) The specific situation of data generated and processed by connected devices also has to be considered in the current process of a 'digital update' of consumer contract law. The objective of this update is, and should be, to guarantee equal standards of consumer protection with regard to liability for the lack of conformity of the goods and services with the contract as well as the right to be informed and to withdraw from the contract irrespective of whether the contract relates to a connected on non-connected device or a digital service. Thereby, two issues are now debated in particular: the first issue relates to cases where the consumer does not pay with money but provides access to personal data.

Following the Commission's Proposal of for a Digital Content Directive, this debate has mostly been characterised by a theoretical debate on whether the provision of personal data can be considered a 'counter-performance' as formulated by the Commission. It has to be welcomed that the European institutions have now moved away from this notion, which indeed could even limit the scope of the application of the rules of the Directive. Conversely, the proposals of the Commission's proposals fail to take into account that not only digital services as currently defined can be provided without monetary consideration, but also connected devices for which the supply is financed through commercial exploitation of the personal data collected by these devices.

(41) The second issue relates to the treatment of digital content and services embedded in connected devices under future EU consumer contract law. The current proposals of the Commission for the Digital Content Directive would create considerable loopholes in consumer protection by limiting the concepts of digital content and services by only including embedded digital content and services that are not subordinate to guaranteeing the functioning of a physical device. The Consumer Sales Directive and the Proposal for a new Online Sales Directive will not adequately close this gap. The latter Directives only apply to sales contracts, not to lease and rental contracts, and do not cover the above case where the device is supplied without monetary consideration. Most importantly, the latter two Directives only apply to the contract with the trader who is selling the device, while consumers often enter into separate contracts on software updates and the provision of other digital services directly with the manufacturers although the software and the digital services serve the purpose of guaranteeing the functioning of the device. To provide non-discriminatory consumer protection, the definition of digital content and digital services should therefore be broadened to include any embedded digital content and digital service.

(42) The now proposed revisions to the Consumer Rights Directive are designed to align its concepts with those of the upcoming Digital Content Directive. Already in its current version, the right to withdraw from a contract also applies to separate service contracts relating to the provision of embedded digital content and services. Article 16(m) Consumer Rights Directive, which has the purpose to create an exception from the withdrawal right where the provision of the digital content is of a one-off nature, such as in the case of the streaming or download of specific digital content, should not apply where digital content or services are ancillary to the supply of a connected device. This result can be reached by a purpose-oriented interpretation of the provision. The rule according to which the Directive also applies to cases where digital content and digital services are provided only against the provision of personal data by the consumer is to be extended to digital content and services embedded or ancillary to connected devices.

(43) The rules of consumer contract law are in need of being coordinated with the rights of the data subject to withdraw consent and to claim erasure of personal data under the the GDPR. Such need only arises where the processing of data is not already legal without consent, namely, in the case where the processing is necessary for the performance of the contract to which the data subject is a party. Hence, where the digital service, which is ancillary to a connected device, depends on the use of personal data, such as in the case of smart wearables used for remote health care, the consumer cannot terminate the processing of personal data by withdrawing consent in terms of data protection rules. In such case the right to process the data will only end with the termination of the contract following the rules of contract law. In contrast, in a case where a contract also allows for the commercial exploitation of personal data collected through connected devices in secondary markets or where personal data is provided to get access to the use of a connected device without monetary consideration, the rights to withdraw consent and to erasure under the GDPR should be considered to apply. From a contract law perspective, exercise of these rights will also lead to the termination of the contract with the other party unless, following the rules

of applicable contract law, the withdrawal only affects parts of the contract and the rest of the contract can be further applied. To safeguard full effectiveness of the data protection rights, exercise of these rights should not be considered to trigger contractual liability of the data subject.

(44) Another major issue discussed in the context of the on-going digital update of consumer contract law is the question of whether consumers should dispose of data portability rights in case of termination of the contract under the Digital Content Directive that extend to non-personal data. The Commission has in fact proposed such data portability rights in the two cases of termination of a long-term contract and termination of the contract as a remedy to the failure to provide digital content or digital services in compliance with the contract. Yet extension to non-personal data has encountered resistance on the part of both the European Parliament and the Council. This Study recommends maintaining at least extension to non-personal data that represents user-generated content of the consumer. Without a right to retrieve such content, the Directive would not adequately respond to the underlying lock-in effects. As regards connected devices, user-generated content may not be a major concern. Yet to overcome lock-in effects, users of connected devices will often depend on access also to non-personal data more generally. This shows that irrespective of whether and how broadly the Digital Content Directive will finally provide for portability of non-personal data, there remains the need to discuss data access rights to machine-generated data more broadly. Such access rights may not only be needed when the contract on the provision of digital content or services is terminated but also during the time of its execution.

(45) After the Commission seems to haven given up the idea to extend the scope of the Unfair Contract Terms Directive to B2B relations as a means to enhance access do data, the Directive in its current form is still relevant for the digital economy at the interface with data protection rules. Although the GDPR provides for mandatory rules that prevail over the application of national contract law, reliance on protection under the Unfair Contract Terms Directive is especially needed to the extent that Article 6(1)(b) GDPR does not require consent by the data subject to process personal data in the case where the use of personal data is necessary for the performance of the contract. In such cases, consumers may not always be fully aware of the amount and extent of data collected by the other party. Conversely, business may try to present the scope of application of this provision broadly in the terms of contracts with consumers. In this regard, the Unfair Contract Terms Directive should be used to safeguard the data protection rights provided by the GDPR and to maintain transparency as regards the extent of data being processed. Conversely, as part of a two-pronged strategy of mutually supportive application of the GDPR and the Unfair Contract Terms Directive, Article 6(1)(b) GDPR should be interpreted narrowly, excluding use of personal data for the purpose of secondary uses, such as commercial exploitation in secondary markets, as well as the provision of personal data as a counter-performance to the provision of digital content and digital services without monetary consideration. This analysis confirms that the data protection rules of the GDPR have now moved to the centre of the rules protecting consumers in the digital economy.

5 Assessing the potentials of different access regimes

(44) This Study supports the Commission's assessment that the major concern regarding the working of the digital economy relates to access to machine-generated data. For addressing this concern, the Study recommends introduction of targeted data access rights which could either be formulated for individual sectors or be adopted as a generally applicable access regime. The Study rejects the idea of introducing a data producer's right

and highlights the insufficiency of the existing regime for access to personal data under the GDPR.

(47) As regards the assessment of the idea to adopt a data producer's right, before entering into an analysis of its potential design, introduction of such a right is in need of an economic, market failure-based justification. The problem in this regard is that the Commission, in its European Data Economy Communication of 11 January 2017, on the one hand, and the accompanying Staff Working Document (SWD), on the other hand, formulated conflicting positions both with regard to who the rightholder should be and the underlying functions of the rights. The adoption of intellectual property rights is typically explained by the need to create incentives for the rightholder to invest in the production and commercialisation of the subject-matter of protection, to stabilise transactions and to increase legal certainty on the allocation of rights among market participants. The position of the Commission Staff seems to correspond better to this classical approach by allocating the right to the person who has made the major investment in the creation of the right and, thereby, reaches the conclusion that that right should typically be vested in the manufacturer of the device or to both the manufacturer and the commercial owner or long-term of the device as 'co-producers'. Conversely, the Commission in its Communication may well have identified a market failure in form of lock-in effects, and therefore considers attributing the data producer's right to the owner or long-term user of the connected device. The problem with this approach is that this is not a type of market failure that is usually remedied by the adoption of a new intellectual property right *in rem*. Rather, such market failure is at best relied upon to introduce compulsory licensing systems within already existing intellectual property systems as part of the exceptions and limitations of the exclusive right. In this perspective, the Commission seems to have chosen an inappropriate remedy for an existing market failure.

(48) To the extend that the Commission argues in favour of recognising a data producer's right in machine-generated raw data, no traditional market-failure that would typically justify intellectual property protection can be identified. The incentive theory is unconvincing since the raw data are only by-products of the commercialization of connected devices. The development of these devices is driven by intensive competition in the product markets. Nor can property in the raw data stabilise data markets. While it is true that *de facto* control over the data does not provide the data holder with direct claims against third parties, availability of trade secrets protection may already mitigate that problem. Most importantly, a data producer's not would not contribute anything. The data owner would well have claims in case of unauthorised use of the data by third parties but, given the lack of transparencies regarding the use of data by others in a big data world, the rightholder would not be able to monitor the market to find out about such infringements. Finally, a data producer's right would not increase legal certainty by clearer attribution of rights in the market. To the contrary, the creation of a new intellectual property system would only create huge burdens in terms of clearing their rights for those market participants who want to make use of machine-generated data. There might be other market failures, such as the difficulties to assess the economic value of a dataset without knowing the data But such market failures could be remedied more easily by other means than by recognition of a data producer's right.

(49) Beyond the challenge to justify a data producer's right by way of a market failure analysis, to choose raw data for non-personal data as the subject-matter of protection cannot live up to the requirement of attributability of the subject-matter of protection to an individual rightholder. This problem arises both from the fact that data on the mere syntactic (sign) level of information cannot be attributed to an individual person and that it is not possible to draw a clear line between personal and non-personal data. The first problem becomes vital whenever raw data from one dataset is integrated in a larger dataset with aggregated

data. Consisting of a series of bits and bytes, it will no longer be possible to attribute the data to the rightholder. The only way would be to look at the semantic level of information and ask what kind of data is encoded by the raw data. However, even this approach would often only work in case of single source information, where it can be excluded that anther person holds rights in a different sequence of raw data encoding the same information. But this is exactly the situation, where a data producer's right would restrict free movement of information, which limitation of the right to raw data is intended to avoid. The problem of distinguishing between personal and non-personal data does not only arise from the broad definition of the former, but also the technological capabilities of big data analytics to re-anonymize previously anonymised data.

(50) Further problems arise in the context of allocating the data ownership right to the 'data producer'. If the 'data producer' were defined as a factual concept, identification of the rightholder in big data scenarios where frequently multiple persons contribute to the generation of raw data would be extremely difficult and often lead to co-ownership. To only look at the person who has taken the economic risk of exercising the last act that leads to the encoding of data may provide more legal certainty. But this attribution of the right would also be rather arbitrary and will not prevent the market player with superior bargaining power from securing the data producer's right through *ex ante* transfer. The Commission seems to advocate a more interest-based attribution of the right, but there does not even seem to be agreement within in the Commission on the functions of the data producer's right, which also leads to contradictions in identifying the data producer. The Commission Staff seems to follow an incentive-based theory. It therefore wants to attribute the right primarily to the manufacturer who has at least made the investment in developing the connected device. But the Commission Staff fails to convince with the argument that commercial owners and users of the device who paid a price for the device or its use should be considered co-producers. In particular, it is not clear why consumers should be excluded from ownership. In the European Digital Economy Communication, the Commission advances a better theory for choosing the owner or long-term user of the device as a data producer. Yet the justification in the light of existing lock-in effects would argue in favour of choosing these persons as beneficiaries of a compulsory licensing system rather than as holders of an exclusive data ownership right.

(51) Moreover, granting an exclusive property right to the owner or long-term user of the connected device will not produce the expected result of overcoming the problem that the right-holder does not have access to the data under the *de facto* control of the manufacturer. To challenge the manufacturer with injunctive relief is only a theoretical means to get access to the data and to enable the owner or long-term user as the rightholder to license the use of the data to third persons. By making such use of the exclusive right, the rightholder would act against her primary interest in the proper functioning of the device, which typically depends on control and use of the data by the manufacturer. More importantly, the manufacturer will be the person who defines the terms of the contractual relationship with the owner and long-term user of the device and, especially where the manufacturer disposes of superior bargaining power, it can require *ex ante* assignment of the data producer's right. This shows that the exclusivity of the data producer's right cannot substitute a data access regime.

(52) Nor can a data producer's right guarantee allocation of the benefits of the economic exploitation of machine-generated data to the rightholders. This is explained by three reasons: first, unequal distribution of negotiating power would allocate the income differently, namely, typically to the manufacturer. To respond to this problem, the legislature would have to implement mechanisms of price regulation in form of mandatory contract law regarding the relationship between the 'data producer' and the manufacturer. Yet such regulation would necessarily conflict with the formation of prices for the

connected device as such. Secondly, the legislature would have to make sure that the rightholder also participates in the income generated by the exploitation of derivative data that is generated by analysing machine-generated data. How data producer's rights should be best attributed within chains of subsequent data analyses is however a most difficult question. More importantly, concerning the myriads of data producer's rights that may need to be recognised and the legal uncertainties emerging from most complex layers of data producer's rights show that such an intellectual property system will not be capable to fulfil its economic function in practice. Thirdly, introduction of an exception for the use of machine-generated data in secondary markets combined with a system of statutory remuneration for the rightholder would not be an option either. This approach would necessarily require a system of mandatory collective rights management, whereby the collective rights management organisation (CMO) would have to monitor the entire social life of practically all citizens for the only purpose of distributing the income appropriately to the individual members of society as data producers. To implement such a system does not only have to be considered an illusion from a practical perspective, it is also unacceptable for any democratic society.

(53) A final issue regarding the design of a potential data producer's right regards the formulation of exceptions and limitations. Such exceptions and limitations are typically designed to take care of the legitimate interests of other persons to reach a fair balance of interests. Accordingly, the kind of exceptions and limitations depends on the prior attribution of the data producer's right to a specific person. This explains why the Commission, proposing a data producer's right of the owner and long-term user of the connected device, focuses on the access interest of the manufacturer of the device in the framework of discussing necessary exceptions and limitations. In contrast, taking into account the particular access interest of the owner or long-term user of the device, from a traditional intellectual property perspective, it would be more convincing to grant the data producer's right to the manufacturer as the typical *de facto* holder of the data and protect the access interests of the owner or long-term user of the device in the framework of a compulsory licensing system. But such legislation needs to be opposed too for two reasons: first, it would strengthen the already existing *de facto* exclusivity position of the manufacturer, while the legislature may not necessarily be able to foresee all situations for which an exception would be needed. Secondly, as proven by the existence of several sector-specific EU data access regimes, such an approach is based on the wrong assumption that legislation on data access is conditioned by prior recognition of an exclusive intellectual property system. Therefore, this Study recommends concentrating the legislative reform process on the formulation of such self-standing access regimes.

(54) A data access and a data portability right are provided by Article 15 and 20 GDPR. Both rights relate to the personal data of the data subject and, hence, to the semantic level of information. This is explained by the particular interests that these two rights aim to satisfy. Yet this does not mean that data access rights must never relate to whole datasets and the raw data contained in them. Whether a data access regime should relate to information on the semantic or the syntactic level has to be decided based on an analysis of the interests involved. In the case of connected devices, the owners or users of these devices will often be in need of access to all the data, for instance, to connect the devices of different suppliers to enable smart manufacturing, smart farming or smart homing or to receive data-based services from third parties. The data access and data portability rights of the GDPR do not satisfy these interests. Beyond the data portability right of Article 20 GDPR, the owners and users of connected devices will also need to get access to non-personal data and data that is not only observed by the connected device but also derived from such data. Accordingly, the data portability right of Article 20 GDPR can at best be regarded a role model for more

far-reaching access rights to the extent it provides a right to data transfer without requiring prior termination of the contract with the data processor.

(55) The adoption of data access rights has several comparative advantages: data access rights can be more targeted than a data producer's right in responding much specifically to the market failure of a data lock-in. Data access rights can more easily be protected against being contracted away by making them non-waivable. They are also more flexible by being allocated to rightholders in an interest-based approach. They can also be enacted in a positive sense and not just as an exception to a data ownership right. Finally, data access rights can be considered as an expression of fully competition-oriented regulation, that aims at opening up new data-based markets for competition.

(56) The scope of data covered should be defined broadly and in a technology-neutral manner. To exclude circumvention of the data access right by the manufacturer, for instance, through transferring the data processing and storing to the cloud, the data access rights should extend to all data generated or used by the device that is needed to guarantee the functioning of the device or access to which is needed for providing data-based services.

(57) Data access rights should be designed as non-waivable statutory rights. This is the approach that should be preferred over the enactment of such rights as part of mandatory European contract law. The reason is that the person interested in data access will not necessarily be entertaining a contractual relationship with the person controlling the data.

(58) The interest-based approach should define the scope of any access right and the parties between whom the right should be granted. Hence, the right depends on the existence of a legitimate data access interest. The right will therefore be allocated to the person who has a legitimate interest in getting access to data for the purpose of making full use data that is needed for the proper functioning of a connected device and access to which is needed for providing data-related services. This does not necessarily have to be the owner or long-term user of the device. But the legislature can use these persons as examples of persons holding a data access right, preferably in the framework of a rebuttable presumption. In addition, data access rights should not be restricted to consumers, since the problem of data lock-in is equally affecting businesses, especially small and medium-sized enterprises. In most instances, the person being under a duty to grant access should be the manufacturer. Yet, in the data economy, *de facto* data control may often be exercised by other persons or entities, such as the operators of data sharing platforms. Therefore, the person addressed by the right should be defined as the person being in *de facto* or legal control of the relevant data. As non-waivable rights, data access rights should not be transferrable either. This excludes that persons without any legitimate interest can use them for getting access.

(59) Following the example of the data portability right of Article 20(2) GDPR, these access rights should also include the right to have the data transmitted to third persons for the purpose of enabling the entitled person to receive data-based services from third parties, thereby opening up markets for data-based services to competition. The legislature could even go a step further by adopting sector-specific legislation that provides for direct data access rights of third-party data service providers. This would especially be the less burdensome approach for consumers especially as owners and long-term users of devices. Direct entitlement of third-party service providers could even be considered for the abovementioned interest-based test as part of a generally applicable data access regime. However, direct entitlement of third-party service providers should only be accepted on the condition that an otherwise interested person has mandated the third party with providing the service.

(60) Sector-specific access regimes will often constitute the better approach for reaching optimal results. The Study especially supports the approach proposed in the literature to provide for targeted regulation where sector-specific market failures prevent multiple stakeholders of a given sector to create functioning data governance regimes. Yet this does not have to exclude adoption of a generally applicable data access regime. Under such a regime, it would be for the judge to take the interests of the multiple stakeholders and already existing sector-specific regulation into account when deciding whether there is a legitimate interest in access to data. As the more adaptable regulatory tool, such a general data access regime could also be applied in parallel to sector-specific legislation to guarantee that appropriate solutions can also be found against the backdrop of rapid changes in many sectors of the digital economy.

(61) As private rights, data access rights would in principle need to be enforced through private action initiated by the person entitled to data access. This, however, is extremely burdensome especially for consumers. Since data holders could be tempted to consistently refuse to grant access to all holders of the access right, there is a case to consider additional enforcement mechanisms, such as administrative enforcement and collective private actions. The choice of the concrete enforcement mechanism could in principle be left to the national legislature in the framework of harmonising EU legislation on data access rights. Yet the Proposal of the Commission of 11 April 2018 for a Directive on representative actions for the protection of the collective interests of consumers would also apply to legislation of data access regimes where 'the interests of a number of the consumers' would be affected. Therefore, in the ongoing discussion for the adoption of this Directive, the EU legislature should also take into account its relevance for the already existing access and data portability rights of the GDPR as well as potential future access rights of consumers.

(62) Data access rights are in need of being coordinated with other systems of protection. In this regard, the data protection rules of the GDPR should be fully respected. In contrast, data access rights should prevail over sui generis database rights, which would best be implemented by way of an amendment to the Database Directive. Data access rights should also apply where the data to which access is sought are trade secrets of the *de facto* data holder. Yet the data holder should be allowed to impose confidentiality requirements on the person seeking access.

(63) The manufacturer as the data holder may try to restrict exercise of data access rights through contractual arrangements, namely, end-user licensing agreements with the owner of the connected device or vertical agreements with distributors. End-user agreements can legitimately be used by a manufacturer for regulating the details of the exercise of the access right, such as the FRAND-compliant royalty rate to be paid. The EU legislature should make clear that the person entitled to data access is entitled to a licence for the use of the data in compliance with the data access regime, providing the competent courts with the power to control the content of the agreement. Equally, legislation should also declare void any clause in a distribution agreement that would in any way restrict the exercise of the data access right, providing the distributor with the possibility to rely indirectly on the data access regime.

Table of Contents

4.3 Other exclusive rights in data
a) Copyright law
b) Patent law
c) Civil law property

4.4 Trade secrets protection
a) The concept of trade secrets
b) The holder of the trade secret
c) The scope of protection
d) Remedies
e) The interface with data protection
f) Recognition of defensive rights similar to trade secrets protection
g) Comparing sui generis database rights, trade secrets protection and defensive rights against misappropriation in practice
h) Conclusion

4.5 The rights of consumers in relation to data generated by connected devices
a) Property rights
b) Data protection rights, including the data portability right
c) Towards a digital update of consumer contract law
d) Extension of consumer contract law to cases where data is a counter-performance
e) Extension of consumer contract law to embedded software and digital services
f) Overview on the contractual consumer rights regarding the use of data
g) The right to withdraw from a contract
h) Coordination of consumer contract law with data protection law
i) Contractual data portability rights under the Digital Content Directive
j) Control of standard contract terms, especially concerning personal data
k) Conclusion

5 Assessing the potentials of different access regimes

5.1 The potential data producer's right
a) The objectives of a data producer's right
b) Non-personal machine-generated raw data as a subject-matter of protection
c) Identifying the data producer
d) The exclusive right to use the data
e) The right to participate in the economic income from the exploitation of the data
f) Exceptions and limitations
g) Conclusion

5.2 The GDPR as a basis for rights to access machine-generated data
a) Personal data as machine-generated data
b) The right of access to data under Article 15 GDPR and access to machine-generated data
c) The data portability right under Article 20 GDPR and access to machine-generated data
d) Data portability according to Article 20 GDPR as a template for future regulation

5.3 Targeted rights especially of consumers to access machine-generated data
a) The comparative advantages of data access rights
b) Access to what data?
c) Data access rights as non-waivable statutory rights
d) The scope of access rights and between whom these rights should be granted
e) Limitation to consumers?
f) Third-party beneficiaries
g) General or sector-specific regulation?
h) Coordination with other systems of protection
i) Coordination with end-user licence agreements and rules on vertical restrictions
j) Conclusion

1 Introduction

The generation and use of large amounts of data can be considered the cornerstone and major driver of the current digital revolution.[1] The focus of this Study concerns a particular feature of the modern digital economy, namely, connected devices and the—personal and non-personal—data they collect and process.

Connected devices mark a (fourth) industrial revolution and fundamentally change the life of citizens.[2] Connected machines transform the way how goods are produced and distributed. Some connected devices, such as connected cars, household devices, smart meters and smart wearables, directly affect the economic and privacy interests of consumers, users and other natural persons.[3] From a legal perspective, distribution and operation of connected devices build on different business models and require different contractual transactions. Hence, this Study seeks to assess the adequacy of the existing legal framework and explores the need for reform in the light of the advent of connected devices. It thereby contributes to the ongoing European debate on the future legal framework for this part of the digital economy.

At the heart of this debate, there are two seemingly contradictory policy considerations. On the one hand, the fact that commercial exploitation of large amounts of data is key for the success and the commercial value of companies in the digital economy fuels a debate on who owns the data and how ownership rights in data should be distributed among stakeholders.[4] On the other hand, public policy makers advocate a policy in favour of promoting free flow of data to realise the major economic and social benefits for society at large.[5]

On the level of the European Union, this debate has been taken up by the Commission as part of its so-called 'free-flow-of data' initiative, which is one of the 16 key actions of its ongoing priority project to implement a Digital Single Market. By aiming at 'maximising the growth potential of the digital economy'[6], the initiative adopts an industrial policy approach.[7] In 2015, the Commission

[1] See also the Communication of the Commission of 25 April 2018—'Towards a common European data space', COM(2018) 232 final, 2 (describing data as a 'key source of innovation and growth' as well as the 'raw material' of the Digital Single Market') (in the following cited as the 'Common European Data Space Communication').

[2] The importance of the advent of connected devices is generally recognised. See, for instance, Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 989.

[3] The relevance of huge amounts of data, often collected by machines and sensors, for practically all field of life of natural persons is also pointed out in the Common European Data Space Communication (n 1) 2.

[4] See, for instance, Karl-Heinz Fezer, 'Data Property of the People—An Intrinsic Intellectual Property Law Sui Generis Regarding People's Behavior-generated Informational Data' (2017) *Zeitschrift für Geistiges Eigentum* 356, 356-57 ('In the reality of the market, behavior-generated informational data represents a tradable commodity and crucial asset of a booming industry in the digitized world. Being a commodity, informational data requires proprietary shaping in property law.').

[5] OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (Paris: OECD, 2015) 195-98, available at http://www.oecd-ilibrary.org/deliver/9789264229358-en.pdf?itemId=/content/book/9789264229358-en&mimeType=application/pdf (accessed 31 July 2018).

[6] Communication of the Commission of 6 May 2015 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions—A Digital Single Market Strategy for Europe, COM(2015) final, 14-15 (in the following cited as 'Digital Single Market Strategy Communication').

[7] The Commission confirms its industrial policy approach in its Common European Data Space Communication of 2018, calling '[d]ata-driven innovation (...) a key driver of growth and jobs that can significantly boost European competitiveness in the global market'. The Commission also mentions that, according to a European Data Market

announced that, by the end of 2016, it would address both issues of ownership and access to data.[8] With a bit of a delay, in another Communication of 10 January 2017, the Commission finally addressed the issue of ownership in data, but discusses the potential introduction of a new data-producer's right exclusively as a tool to promote free flow of data.[9] However, the following consultation did not produce any support for the introduction for a new intellectual property right in data.[10] This may explain why the Commission has so far refrained from proposing legislation on data ownership.[11]

Rather, shortly after the consultation, the Commission proposed legislation to overcome national data localisation restrictions, which create impediments to cross-border cloud computing services in particular.[12] Then, as part of its most recent 'data package' of 25 April 2018[13], the Commission proposed a review of the Directive on the re-use of public sector information (PSI)[14], updated its

Study of 2017, the European data economy could double by 2020, if the right framework conditions are put in place. See Common European Data Space Communication 2018 (n 1) 1.

[8] Digital Single Market Strategy Communication 2015 (n 5) 15. See also Daria Kim, 'No One's Ownership as the Status Quo and a Possible Way Forward: A Note on the Public Consultation on Building a European Data Economy' (2017) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 697, 699 (criticising that the Commission at that stage did not define what exactly the emerging issue of data ownership is).

[9] Communication from the Commission of 10 January 2017—Building a European Data Economy, COM(2017) 2 final (in the following cited as 'European Data Economy Communication'). See also the accompanying Commission Staff Working Document of 10 January 2017 on the free flow of data and emerging issues of the European data economy, SWD (2017) 2 final (in the following cited as 'European Data Economy SWD'). On the Commission's consideration of a potential data producer's right, see the 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', available at: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf (accessed 30 April 2018). The author of this Study is a co-author of this Position Statement. See also Josef Drexl, 'On the Future Legal Framework for the Digital Economy: A Competition-based Response to the "Ownership and Access" Debate' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 223; Kim (n 8); Herbert Zech, 'Building a European Data Economy—The European Commission's Proposal for a Data Producer's Right' (2017) 9 *Zeitschrift für Geistiges Eigentum* 317.

[10] See Commission, Synopsis Report—Consultation on the 'Building a European Data Economy' Initiative (2017) 5, available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/synopsis_report_-_data_economy_A0EFA8E0-AED3-1E29-C8DE049035581517_46646.pdf (accessed 31 July 2018). Comments were critical both on the idea of vesting a data ownership right in the manufacturers, since this could strengthen the anyhow existing *de facto* exclusivity of manufacturers and make data sharing more difficult, and a data ownership right of the data producers. See, in more detail, Commission, Annex to the Synthesis Report (2017) 23-24, available at: http://ec.europa.eu/information_society/newsroom/image/document/2017-36/annex_to_the_synopsis_report_-_data_economy_A45A375F-ADFF-3778-E8DD2021E5CC883B_46670.pdf (accessed 31 July 2018).

[11] In its 2018 Communication, the Commission clearly states the opposition of stakeholders to the introduction of a 'data ownership type of right'. Stakeholders argued that data sharing 'is not so much about ownership, but how access is organised'. Common European Data Space Communication 2018 (n 1) 9.

[12] Proposal of the Commission of 13 September 2017 for a Regulation of the European Parliament and of the Council on a framework for the free flow of data, COM(2017) 495 final. On this proposal, see also Dominic Broy, 'The European Commission's Proposal for a Framework for the Free Flow of Non-Personal Data in the EU' (2017) 3 *European Data Protection Law Review* 380; Inge Graef, Raphaël Gellert, Nadeszhda Purtova and Martin Husovec, 'Feedback to the Commission's Proposal on a framework for the free flow of non-personal data' (2018), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3106791 (accessed 31 July 2018) (with a critical view on the insufficient coordination with the regime on personal data protection). Data localisation restrictions were previously addressed in Part 2 of the European Data Economy Communication 2017 (n 9), while the issues with which this Study is dealing were addressed in Part 3 of the Communication.

[13] See European Data Space Communication 2018 (n 1) 1.

[14] Proposal of the Commission of 25 April 2018 for a Directive of the European Parliament and of the Council on the re-use of public sector information (recast), COM(2018) 234 final.

Recommendation on access to and preservation of scientific information[15] and provided guidance on sharing private sector data[16]. The Commission also proposed a new Regulation which, *inter alia*, tries to increase transparency about the contractual data access rights of businesses using online intermediaries, such as the operators of search engines and selling platforms, for advertising and selling their products.[17] As a particular consumer-related initiative, the Commission also decided to analyse new issues regarding product safety and liability emerging from data-driven technologies.[18]

As regards rights in data, the focus of the European debate has by now shifted to the assessment of existing forms of protection and their application in the modern data economy. This is most welcome since the question of ownership is a 'key determinant' of any policy that aims to promote access to data.[19] The question of whether and to which extent the 2006 Database Directive[20] still fulfils its objectives in the context of the modern data economy and whether it is in need of a reform have just been broadly examined by the Commission.[21] Moreover, it is unclear to which extent the new Trade Secrets Directive[22] can provide protection with regard to data collected by connected devices. Not to forget the new General Data Protection Regulation (GDPR):[23] This Regulation considerably strengthens the autonomy rights of the data subject. This explains why the GDPR has already given rise to a debate on whether the rights of the data subject already amount to an economic ownership right, or whether the existing data protection regime should be further developed in this direction.[24] What may be more important, however, is to research how new EU

[15] Commission Recommendation of 25 April 2018 on access and preservation of scientific information, C(2018) 2375. See also European Data Space Communication 2018 (n 1) 7-8.

[16] Commission Staff Working Document of 25 April 2018—Guidance on sharing private sector data in the European data economy, SWD(2018) 125 final.

[17] See Art 7 Proposal of the Commission of 24 April 2018 for a Regulation of the European Parliament and the Council on promoting fairness and transparency for business users of online intermediation services, COM(2018) 238 final. This provision also relates to personal consumer data that firms like Google and Amazon would collect, without prejudice to the data protection rules of the GDPR. The provision aims to enhance the ability of online traders to access data to which they are entitled to have access under the contract with the online intermediaries.

[18] See Common European Data Space Communication 2018 Communication (n 1) 4; Commission Staff Working Document of 7 May 2018—Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, SWD(2018) 157 final.

[19] As also argued by Kim (n 8) 698.

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

[21] The results of the assessment of the Database Directive were published on 27 April 2018 in form of a 'Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases, Final Report' (prepared for the European Commission DG Communications Networks, Content & Technology by the Joint Institute for Innovation Policy, the Technopolis Group as well as Lionel Bentley and Estelle Derclaye as External Experts) (in the following: 'Database Directive Final Evaluation Report'). The Final Report is accompanied by an Annex 1 with an 'in depth analysis of the Database Directive, article by article' (in the following: 'Database Directive Final Assessment Report Annex 1') and an Annex 2 with an 'Economic Analysis' (in the following: 'Database Directive Final Assessment Report Annex 2'). The conclusions of the Commission are summarised in the Commission's Common European Data Space Communication (n 1) 6, as well as in the Commission Staff Working Document—Executive Summary of the Evaluation of Directive 96/9/EC on the legal protection of databases, SWD(2018) 146 final.

[22] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, [2016] OJ L175/1.

[23] 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), [2016] OJ L119/1.

[24] See, in particular, Luisa Specht, 'Das Verhältnis möglicher Datenrechte zum Datenschutzrecht' (2017) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 1040; Luisa Specht, 'Property Rights Concerning Personal Data' (2017) *Zeitschrift für Geistiges Eigentum* 411 (arguing against the need of such an extension). See also Christian Berger, 'Property Rights to Personal Data?—An Exploration of Commercial Data Law' (2017) *Zeitschrift für Geistiges*

data protection rules can be better coordinated with the need to make data markets work from an economic perspective, especially because personal data is among the most valuable data.[25]

Meanwhile, the debate on new legislation on data ownership seems to find a continuation on the national level. Scholarship in Germany has influenced, followed and accompanied the discussion on the European level more than scholarship in any other Member State. Some German scholars have argued in favour of introducing a data ownership right for personal as well as non-personal machine data.[26] In August 2017, the debate reached Germany's political level, when the Federal Transports Ministry published a study arguing in favour of a generally applicable data law, which would for instance vest a data ownership right in the holder of a car relating to the personal and non-personal data generated in course of using this car.[27] The idea of 'data ownership' then made it into the coalition agreement of the parties CDU, CSU and SPD as part of the agenda for the new government. There, in the context of fixing the goal of promoting e-medicine services, in addition and beyond personal data protection, the agreement states that any digital data collected in that context constitutes property of the patient.[28] On 21 March 2018, in her speech before the German Parliament explaining the agenda of the new government, Chancellor Angela Merkel even explicitly claimed that Germany should go beyond the European General Data Protection Regulation and build a 'fair system of data ownership' that guarantees participation of the individuals in the returns of the data economy and further promotes data sovereignty.[29] In contrast, a working group appointed by the Conference of Federal States' Ministers of Justice has recently concluded that there is no need to

Eigentum/Intellectual Property Journal 340 (analysing personal data protection rules as a basis of a 'commercial' data law by taking personal data as an economic asset).

[25] The lack of debate on this issue is particularly noted by Maximilian Becker, 'Rights in Data—Industry 4.0 and the IP Rights of the Future' (2017) 9 *Zeitschrift für Geistiges Eigentum* 253, 259.

[26] See, in particular, Fezer (n 4) 356-70; id, 'Dateneigentum—Theorie des immaterialgüterrechtlichen Eigentums an verhaltensgenerierten Personendaten der Nutzer als Datenproduzenten' (2017) *Multi-Media Recht* 3. Fezer's proposal for a data ownership right was taken up in the recommendation of the Consumer Commission of Baden-Württemberg to which Fezer contributed as a co-author; see Andrea Wechsler, Andreas Oehler, Karl-Heinz Fezer and Tobias Brönneke, 'Datensouveränität, -nutzung und Datenverwertung—Forderungen nach einem „update" der Wirtschafts- und Rechtsordnung als Chance für eine selbstbestimmte Datennutzung', Stellungnahme Verbraucherkommission Baden-Württemberg Nr. 45/20017 (1 December 2017) 9-11, available at: http://www.verbraucherkommission.de/pb/,Lde/Startseite/stellungnahmen (accessed 31 July 2018). The first author who discussed such a data producer's right in more detail was Herbert Zech, 'Daten als Wirtschaftsgut—Überlegungen zu einem „Recht des Datenerzeugers"' (2015) *Computer und Recht* 137. However, it is to be noted that Zech has become more cautious about introducing a data ownership right. See Herbert Zech, 'Building a European Data Economy—The European Commission's Proposal for a Data Producer's Right' (2017) 9 *Zeitschrift für Geistiges Eigentum* 317 (explicitly leaving open the question whether there is an economic justification of data ownership and concentrating on the potential legal framing of such a right). Data ownership was discussed in German legal writing even before the advent of big data and the modern data economy. On ownership rights in information goods, see Helmut Redeker, 'Information als eigenständiges Rechtsgut—Zur Rechtnatur der Information und dem daraus resultierenden Schutz' (2011) *Computer und Recht* 634 (with a particular focus on ownership in the digital copies of software). Yet, from an early time on, there have also been voices in German legal writing against recognising ownership in data, see Michael Dorner, 'Big Data und „Dateneigentum"' (2014) *Computer und Recht* 617; Thomas Heymann, 'Rechte an Daten—Warum Daten keiner eignetumsrechtlichen Logik folgen' (2016) *Computer und Recht* 650 (in direct response to Zech).

[27] Bundesministerium für Verkehr und digitale Infrastruktur, '"Eigentumsordnung für Mobilitätsdaten?"—Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive' (2017) available at: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile (accessed 31 July 2018).

[28] 'Ein neuer Aufbruch für Europa—Eine neue Dynamik für Deutschland—Ein neuer Zusammenhalt für unser land', Koalitionsvertrag zwischen CDU, CSU und SPD, 19. Legislaturperiode (12 March 2018) 102, available at: https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1 (accessed 31 July 2018).

[29] Regierungserklärung von Bundeskanzlerin Merkel in Berlin vor dem Deutschen Bundestag (21 March 2018), available at: https://www.bundeskanzlerin.de/Content/DE/Regierungserklaerung/2018/2018-03-22-regierungserklaerung-merkel.html (accessed 31 July 2018).

introduce a data ownership right.[30] Moreover, in April 2018, the Konrad Adenauer Foundation, the policy thinktank of Germany's major governing party CDU published a study authored by Karl-Heinz Fezer, who so far has been the most outspoken academic voice in favour of data ownership of all citizens. This study seems to turn away from data ownership at least as an individual intellectual property right. Rather, Fezer now seems to favour a more regulatory approach based on 'representative data ownership' (*repräsentatives Dateneigentum*) administered by a new agency that would spend the income in the public interest such as for educating citizens to increase digital literacy.[31]

To some extent, the German debate is mirrored in France, where the liberal thinktank Génération Libre, under the catchy slogan '*Mes datas sont à moi*', has published a report in January 2018 that argued in favour of a commercial ownership right in personal data with the particular aim to convince the French Parliament to recognise an economic ownership dimension under ongoing legislation on personal data.[32] The inspiration for claiming recognition of data ownership in personal data seems to be basically the same as in Germany—although the debate in Germany goes much further, also including non-personal data. Génération Libre argues that the citizens should participate in the economic income generated by the exploitation of their personal data not least against the interests of the big platform providers of US origin. Yet the Report only had limited political impact. It was supported by Bruno Bonnell, Member of the *Assemblée Nationale* for the majority Party La Répblique en marche, who brought a respective motion in Parliament to recognise a data ownership right as part of necessary French legislation to enable application of the General Data Protection Regulation (GDPR) in France.[33] Yet this motion was rejected. Opponents argued that such legislation enabling the data subject to sell 'their' data would not be capable of solving the problem of unequal distribution of bargaining power between the data subjects and the platform providers.[34] At the end such legislation could even strengthen the market position the latter by providing them with exclusive property rights they can easily acquire from the data subjects, without any guarantee that the original rightholders would participate in the income generated from the exploitation of their data.

Such debates in major EU Member States show that the discussion on data ownership may not yet be over. The issue deserves continuous attention especially from a European perspective since purely national legislation could not only undermine the functioning of the internal market. Inadequate national legislation in major Member States could easily work as a template for later ownership legislation on the European level.

Against the backdrop of these developments, this Study adopts a both normative and policy-oriented approach. From a normative perspective, it will aim to contribute to a better

[30] See Andreas Christians and Michael Liepin, 'The Consequences of Digitalization for German Civil Law from the National Legislator's point of View' (2017) 9 *Zeitschrift für Geistiges Eigentum* 331, 334-36 (summarising the final report of 2017 as representatives of the Justice Ministry of North Rhine-Westphalia).

[31] Karl-Heinz Fezer, 'Repräsentatives Dateneigentum—Ein zivilgesellschaftliches Bürgerrecht' (St. Augustin: Konrad-Adenauer Stiftung, 2018), also available at: http://www.kas.de/wf/doc/kas_52161-544-1-30.pdf?180424103157 (accessed 31 July 2018). This concept will be discussed further below in the context of the question of whether and how participation of citizens in the economic added value generated by using machine-generated data can be implemented as part of a data producer's right. See at the end of Part 5.1 e) below.

[32] See Génération Libre, 'Mes datas sont à moi—Pour une patrimonialité des données personnelles', Report authored by Isabelle Landreau, Gérard Peliks, Nicolas Binctin, Virginie Pez-Pérard (January 2018), 46-100 (Part 2 of the Report). See also Génération Libre, Comuniqué de presse (25 January 2018), available at: https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-Mes-data-sont-à-moi-.pdf (accessed 31 July 2018).

[33] Projet de loi relatif à la protection des données personnelles, texte adopté n° 113, session ordinaire du 15 may 2018, available at: http://www.assemblee-nationale.fr/15/ta/tap0113.pdf (accessed 31 July 2018).

[34] See Anaïs Cherif, 'Etre propriétaire de ses données personnelles, une dangereuse illusion', La Tribune (29 March 2018), available at: https://www.latribune.fr/technos-medias/internet/etre-proprietaire-de-ses-donnees-personnelles-une-dangereuse-illusion-773398.html (accessed 31 July 2018).

understanding of the current legal situation of data generated by connected devices used by consumers. Policy-wise, it will explore what options are available to clarify and further develop the legal status of such data, in particular with the objective of preventing lock-in effects restricting the ability of consumers to access these data and share them with third parties.

In doing so, this Study is expected to provide answers to the following more concrete questions:

(1) How does the current legal framework (e.g. GDPR and property rights) treat machine-generated data?

(2) What are the rights of consumers in the current EU legal framework in relation to the data generated by the devices he/she is using?

(3) What are the benefits and disadvantages of a 'data producer's right' as suggested by the European Commission in its European Data Economy Communication?

(4) What is the role of the GDPR in this debate?

(5) Can the system of the GDPR based on a right to access data be applied to machine-generated data? What are the benefits of such approach from consumer perspective?

(6) Should additional rights be set up in general legislation, e.g. in consumer law? Can sectoral legislation (e.g. after-sales for car repairs) play a role?

(7) How would a right of access data in the benefit of consumers interact with other contractual relationships between the consumer and the supplier of the device and the embedded software in the device such as end-user license agreements?

(8) What would be the impact on competition and consumer choice of regulating data access rights in EU law? How would such a right interplay with the legislation on vertical restraints concerning restrictions that could be imposed by manufacturers on parties of the downstream market?

(9) If the solution cannot be found in the creation of a new right, what other tools can be proposed to ensure that consumers keep the ability do decide to whom to give access to their non-personal data?

From a methodological point of view, the Study adopts an interdisciplinary approach. Answers to the abovementioned questions cannot be given without taking into account the economics of data markets. Whereas the discussion has so far predominantly been driven by the legal community—both academic and practicing lawyers—, stakeholders and policy makers, more recently also a number of economists[35] have found an interest in the topic and several studies have been published on the emerging data economy.[36] This Study refrains from broadly analysing this very important research, but still strongly builds on it. This is especially the case in Parts 2 and 3 where the Study

[35] See, in particular, the writing of Wolfgang Kerber, 'Digital Markets, Data, and Privacy: Competition Law, Consumer Law and Data Protection' (2016) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 639; id (n 2); id, 'Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective' in Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 109; Wolfgang Kerber and Severin Frank, 'Data Governance Regimes in the Digital Economy: The Example of Connected Cars' (preliminary version, 1 October 2017), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3064794 (accessed 31 July 2018).

[36] See, in particular, the study by the European Commission Joint Research Centre (JRC): Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer, 'The economics of ownership, access and trade in digital data', JRC Digital Economy Working Paper 2017-01 (Seville: European Commission, 2017), available at: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf (accessed 31 July 2018). See also the recent interdisciplinary study by Luisa Specht and Wolfgang Kerber, 'Datenrechte—Eine rechts- und sozialwissenschaftliche Analyse im Vergleich Deutschland-USA', ABIDA – Assessing Big Data (2018), available at: www.abida.de/sites/default/files/ABIDA_Gutachten_Datenrechte.pdf (accessed 31 July 2018).

aims to develop a broader policy framework for answering the questions, whereas in Part 4 and 5, the Study will concentrate on answering the questions from a more legal perspective.

Upfront, this Study will need to clarify the factual, i.e. the technical and economic context. It will do so by exploring this context in the framework of the fundamental concepts that frame this Study (at 2 below). This will be followed by an explanation of the policy framework that is indispensable as a basis for assessing the different options for further legislation (at 3 below). This framework will make it possible to finally answer the questions, whereby the specific consumer interests will also be taken account of (at 4 and 5 below).

2 Basic concepts and issues

In this Part, the Study will explain the concepts concerning access to and control of machine-generated data, which will frame the further analysis of this Study. In doing so, this Part will also help identify the key policy issues.

2.1 Connected devices

This Study uses the term 'connected device' in a broad sense, namely, as all devices that (1) are connected with other things and persons through wireless or wired communication[37] and (2) generate data.

Hence, the term is to be understood in a technology neutral way. Application of sensor technology, such as in cars, farming machines or smart wearables, is just one form of generating data. The concept also includes devices, such as smart meters, that, without necessarily employing sensor technology, are designed to generate data and transmit that data trough wireless or wired communication. Furthermore, connected devices are not limited to those that communicate autonomously through the Internet of Things. Devices used by humans for the purpose of communication, such as PCs, tablets and smartphones, are equally covered, because it is not relevant to which extent data is stored or processed by the device with or without being influenced by the decisions of a natural person. In fact, most data collection through smart devices is influenced to some extent by decisions of the user as a natural person, such as in the case of connected cars or household devices. Whether the user is located through a connected car or a smartphone makes no difference for the purpose of discussing the legal issues surrounding data ownership and access to data. Furthermore, the relevant data generated through smart devices is not limited to data stored in the device. Connected devices are also those that communicate and share dynamic data in larger networks in real time. Connected devices do not only function by using data they autonomously generate; they may also rely on data they receive through wired or non-wired means from other sources, including other connected devices.

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

2.2 Control over data and data ownership

'Data ownership' as a concept is broadly used in the public, political and scholarly debate on the future legal framework of the data economy. Yet it is astonishing that those who rely on it typically refrain from explaining what they mean by 'ownership'. Without a common understanding of 'data ownership' the discussion runs the risk of producing misunderstandings and false conclusions.

a) 'Holding data' is different from 'owning data'

Upfront, a distinction is to be made between 'controlling data' and 'owning data'. In the data economy, a car manufacturer is able to control data collected by a car, simply because the car manufacturer has designed the car and, thereby, will have been able to take all technical steps, in the form of so-called technological protection measures, to exclude others from access to the data. Hence, other persons such as the purchaser or user of a car may not even be fully aware of all data this car collects, nor will such persons automatically be able to access these data. The same holds true for an independent car repairer who will encounter difficulties to circumvent such technical protection measures to access the on-board data necessary for providing the repair service. Yet such *de facto* control does not make the manufacturer of the car, or any other connected device, the owner of the data. Ownership is a legal concept and should not be confused with factual control.[38] Consequently, calling the manufacturer of a car the '*de facto* owner' of the data only based on the fact that the manufacturer is able to control the data and exclude others from access should strictly be avoided.[39] Rather, the term of 'data holder' should be preferred.[40]

Confusion is also caused by the data holders themselves. They often consider and call the data they control 'their' data.[41] But the use of property language alone does not change the legal situation.[42] In a contract law context, ownership terminology creates confusion by falsely implying that private parties have the legal authority to create new intellectual property rights.[43]

What is true, however, is that *de facto* control enables the data holder to enter into contracts on access and use of the data. From an economic perspective, *de facto* control suffices to charge a price to others who seek access to the data. Conversely, contract terms used by the data holder, including terms used in the contracts with consumers on the sale of connected devices in which the

[38] This distinction is important with regard to any—tangible or intangible—object. As regards tangible objects, 'possession' as physical control over an object is to be distinguished from (legal) ownership. See also Kim (n 8) 700 (pointing out in footnote 70 that this distinction should also be made against the backdrop of the Common Law tradition).

[39] The concept of a '*de facto* owner' is nevertheless used by the Commission. See the European Data Economy Communication 2017 (n 9), 10 ('In some cases manufacturers or service providers may become the *de facto* "owners" of the data that their machines or processes generate, even if those machines are owned by the user…'). Notably, the Commission puts the term 'owners' in quotation marks, indicating that the term is not used in a legal sense. With the same understanding, Kim (n 8) 700.

[40] This term is also generally used by the Commission. See the European Data Economy Communication 2017 (n 9) 13 ('A framework potentially based on certain key principles, such as fair, reasonable and non-discriminatory (FRAND) terms, could be developed for data holders, such as manufacturers, service providers or other parties, to provide access to the data they hold against remuneration after anonymisation.')

[41] See, for instance, the sample contract from the UK in the Annex to Osborne Clarke LLP, Legal study on Ownership and Access to Data, Final Report (prepared for the European Commission) (2016) 148-55, available at: https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1/language-en (accessed 31 July 2018) (where clause 8.1 describes clinical test data as the 'exclusive property of the Client').

[42] See also Osborne Clarke LLP, Legal study on Ownership and Access to Data (n 41) 6-7 (criticising the 'mistaken assumption that data is property').

[43] See also Kim (n 8) 700.

data holder claims 'ownership' in the data cannot result in ownership rights as rights *in rem*. As a matter of privacy of contract, such stipulation can only produce (*inter partes*) effects among the contracting parties and, hence, cannot be relied upon by the manufacturer vis-à-vis third parties.[44]

Proponents of a data ownership right seem to be concerned about accepting mere *de facto* control over data as a basis for allocating economic exploitation to an individual person. Indeed, it is true that legal recognition of licensing contracts offered by *de facto* data holders does not constitute a neutral allocative choice.[45] Yet recognition of a data ownership right for another party does not automatically remedy factual data control. Any new legal instrument that seeks to promote data access, including a regime recognising data ownership for another person, will have to include remedies to overcome such *de facto* control. Accordingly, addressing the issue of data access has to be at the centre of interest of this Study, even where it discusses the introduction of a new data ownership right.

b) On the mistaken question of who owns the data

Another misunderstanding underlies the discussion on 'who owns the data'. This discussion creates the perception that the only, yet imminent, task of the legislature consists in making a choice on who the data owner is, while the preliminary and much more important question is whether 'data ownership' should be recognised in the first place. This fallacy seems particularly influenced by the observation of the increasing economic value of data.[46] Yet there are many 'goods' that have considerable societal value without being owned by anybody, such as the air we breathe or the water of the ocean. Such 'public' or 'common goods' are excluded as objects of property because of the very value of these goods for everybody. In the case of such goods, ownership would allow the owner to exclude others from the enjoyment of these goods in clear conflict with the public interest in guaranteeing access to them for everybody.

This is extremely important to note, since data is not so different from other public goods.[47] On the semantic level, data conveys information. As a matter of the fundamental right and constitutional principle of freedom of information[48], information should in principle not be owned by anybody.

The economic reasons for this are equally clear: information as a public good can be used by everybody without exhausting the information as a resource. Accordingly, full access to information enhances public welfare. The more valuable a particular kind of information is, the more important

---

[44] See also Rolf H Weber and Florant Thouvenin, 'Dateneigentum und Datenzugangsrechte—Bausteine der Informationsgesellschaft' (2018) I *Zeitschrift für Schweizerisches Recht* 43, 51; Herbert Zech, 'Daten als Wirtschaftsgut—Überlegungen zu einem „Recht des Datenerzeugers"' (2015) *Computer und Recht* 137, 140.

[45] Francesco Mezzanotte, 'Access to Data: The Role of Consent and the Licensing Scheme' in: Sebastian Lohsse, Reiner Schulze and Dirk Staudenmeyer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 159, 167.

[46] In this regard, it is important to note that the value of 'data' does not arise from the syntactic level, namely, the encoding in digital data, but from the information data conveys on the semantic level. See, also, Zech (n 44) 138 (who nevertheless argues in favour of a data producer's right on the syntactic level of raw data).

[47] On the international level, the interest in access to public goods is a major aspect of the globalisation debate in the light of the objective of sustainable development. See the publication of staff members of the UN Development Program (UNDP): Inge Kaul, Pedro Conceição, Katell Le Goulven and Ronald U Mendoza (eds), *Providing Global Public Goods* (New York and Oxford: OUP, 2003). One of these public goods covered by this publication, which is closely linked to data, is knowledge. Property rights as exclusive rights of use directly conflict with the goal of maintaining and enhancing access of everybody to public goods. This explains why especially intellectual property scholars got interested in the debate on public goods. See the contributions in Keith E Maskus and Jerome H Reichman (eds), *International Public Goods and Transfer of Technology—Under a Globalized Intellectual Property Regime* (Cambridge, UK: Cambridge University Press 2005).

[48] See, in particular, Art 11(1) of the EU Charter of Fundamental Rights.

it is that it is freely available and not owned by anybody. The more people can access and use such information the greater the public benefit.

As a matter of principle, this also means that the high social value of information as such cannot argue in favour of recognising property in that information. Quite on the contrary, the default rule is that unrestricted access should be guaranteed.

c) On cases when ownership in information is justified

This default rule of unrestricted access to information does not come without exception. It does not exclude that under certain circumstances ownership in information is and should be granted.

For instance, such exceptional protection is recognised under patent law, which creates ownership in specific technical information. The reason is that without protection nobody would invest in the necessary inventive activity. Hence, patent law works as an incentive for the production of information for which the level of production would otherwise be sub-optimal. Similarly, the law on trade secrets protection is based on the assumption that keeping certain commercial information secret is important for promoting competitive behaviour among firms.[49]

A comparison of patent and trade secrets protection shows that patent law even encompasses two in-build traits that promote access: first, patent protection is only granted for a limited period of time. Twenty years after the patent filing, the invention falls into the public domain and everybody is allowed to use it, whereas trade secrets, if kept secret, can in principle be protected for ever. Secondly, the patent system overcomes factual control of the information by making knowledge about the invention publicly available through publication. Without patent protection, inventors would only be able to maintain control over their inventions by keeping them secret, which would have the specific shortcoming for inventors of not providing protection against parallel inventions and the specific shortcoming for society of not guaranteeing access of the public to the invention enabling them to freely implement the invention after the expiry of the term of protection

This may raise the question whether the patent logic could also be applied by analogy to data generated by connected devices. Yet, for answering this question, fundamental differences need to be noted. On the one hand, it does not seem that there is and will be sub-optimal production of such data.[50] Quite on the contrary, competitive pressure already provides the necessary incentives for firms to invest in the development of connected devices that collect data.[51] Even traditional manufacturers and service providers of many different sectors are today heavily investing in the digital transition, based on the belief that they would otherwise soon have to leave the market. Secondly, patent law does not protect all technical information. Rather, inventions need to fulfil certain standards, most importantly of novelty and inventive step, to merit protection. In contrast, data collected by connected devices can relate to any information;[52] and establishing an agency that

[49] See Recital 1 of the Trade Secrets Directive 2016/943 (n 22).

[50] This observation seems to be shared by both proponents and critics of the idea of recognising a new data ownership right. See Dorner (n 26) 626; Zech (n 44) 144-45.

[51] See also Josef Drexl, 'Designing Competitive Markets for Industrial Data—Between Propertisation and Access' (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce* (JIPITEC) 257, paras 74-80. The absence of an incentive problem is also confirmed by economists. See Wolfgang Kerber, 'Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective, in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 109, 117. The incentive theory as a basis for the recognition of a data producer's right is also rejected by Zech (n 44) 144-45 (still arguing in favour of such a right). See also Spindler (n 69) 401.

[52] This is also stressed by P Bernt Hugenholtz, 'Data Property in the System of Intellectual Property Law' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 75, 77.

would be appointed to 'grant' data ownership rights based on qualitative standards—whatever those standards might be—has to be considered unfeasible for practical reasons, given the myriads of data that are and will constantly be produced by connected devices.

The bottom line remains that creation of any data ownership, as an exception to the principle of unrestricted access to information, is in need of a positive justification[53], which explains why markets would otherwise work sub-optimally and takes into account the social costs to be paid in form of a limitation of freedom of information.

d) The need to keep information in the public domain in copyright law

Hence, quick analogies to other intellectual property rights should generally be avoided. This holds especially true for copyright law. Copyright law only protects the creative expression of ideas, but not ideas as such (often termed as the 'idea-expression dichotomy').[54] Thereby, copyright law does not only avoid protecting information as such, it even serves the public interest in promoting free flow of information by protecting the business models of industries that are essential for an information society, such as the newspaper and broadcasting industry as well as scientific publishing.[55] Information as such fails to qualify as protected subject-matter protected under copyright law. Rather, by a decision of the legislature, information is delegated to the public domain for the very purpose of promoting free flow of information.[56]

These principles are also expressed in EU copyright legislation for 'digital works' under the Computer Programs Directive.[57] Its Article 1(2) provides that the Directive (only) protects the 'expression in any form' of a computer program, while 'ideas and principles which underlie any element of a computer program, including those which underlie its interfaces, are not protected by copyright under this Directive'.

Yet the fringes of what should legitimately be protected are reached by the Database Directive.[58] Its adoption and especially later application and evaluation were accompanied by an intensive discussion on whether it strikes an appropriate balance of interest as regards both the freedom of information and the need to guarantee access to data. On the one hand, to safeguard these

[53] With the same claim, see Dorner (n 26) 625.

[54] See in this regard the frequently cited provision of Sec 102(b) US Copyright Act, which reads as follows: 'In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.'

[55] Yet there have been rare instances where copyright law resulted in the protection of information. The most important case in this regard is the *Magill* case, where UK and Irish copyright law prevented third parties from reprinting the mere listings of TV programs, thereby enabling the TV broadcasting companies in the Republic of Ireland and Northern Ireland to monopolise the downstream market for printed TV guides. In the 1990s, the Commission and the European Courts could only address this issue within the competition law framework by holding that the refusal to license the copyright would amount to an abuse of dominance. See Joined Cases C-241/91 P and 242/91 P *RTE and ITP v Commission* ('*Magill*') [1995] ECR I-743 = ECLI:EU:C:1995:98. Today, such a case could no longer arise as a matter of harmonised copyright law. According to the case-law of the CJEU on the concept of a copyrightable work, which requires that there is room for making free and creative choices and that the creator has indeed made such choices, the mere listings of TV programs, which are defined by the programming schedule, could no longer be considered as protected by copyright. See, for instance, Joined Cases C-403/08 and C-428/08 *Football Association Premier League and Murphy* [2011] ECR I-9083 = ECLI:EU:C:2011:631, paras 96-98 (holding that football matches are not protected by copyright); Case C-145/10 *Painer* ECLI:EU:C:138, paras 90-92 (on copyright protection for photographs).

[56] This 'information policy' embedded in copyright law is generally supported by modern copyright scholarship. See also Hugenholtz (n 52) 94.

[57] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (codified version), [2009] OJ L111/16.

[58] Database Directive 96/9/EC (n 20).

interests, the Directive limits the subject-matter of protection and provides for specific exceptions and limitations. In particular, Article 1(1) defines a database as a 'collection of ... data'. This should in principle guarantee that the Directive will not protect the individual data. On the other hand, in its First Evaluation Report, also the Commission concluded that especially the sui generis database right, despite 'the long-standing principle that copyright should not be extended to cover basic information or "raw" data ... comes precariously close to protecting basic information'.[59] This shows how important it is to explore whether and to which extent the Database Directive already provides protection for the modern data economy (see at 4.2 below). Still, by highlighting the problematic character of the sui generis right, the First Evaluation Report informs that, for more than 10 years, the Commission has been aware of the risk of undermining the principle of freedom of information by granting too extensive intellectual property protection in the digital environment.

e) Why personal data protection is different

Within the realm of data protection rules, legal control over the use of data—as an exception to the principle of freedom of information—is nevertheless justified by the conflicting fundamental right of privacy.[60]

The discussion, however, on whether data protection rules can be seen as a basis or starting point of data ownership tends to distract from the real issues that need to be discussed. While it is true that the GDPR vests rights in the data subject that can be qualified as control rights directed against any third person, and although the data subject may also make economic use of these rights—maybe even by supplying personal data as a 'counter-performance'[61]—, it is also to be noted that the GDPR only protects 'personal' data and that the scope of this protection is defined by the specific interests of the data subject without giving rise to a general economic right, including in particular a right that would enable the data subject to participate in the economic benefits generated through the economic exploitation of the use of personal data in downstream markets.

Hence, as regards the debate on making personal data protection a point of departure for the recognition of more extensive data ownership rights of the data subject, the key question remains whether there is a justification for the recognition of such rights as such and for the particular design of the ownership right, by also taking into account the definition of the subject-matter of protection, the right-holder and the scope of protection, including the exceptions and limitations.

So far, those who argue for such an extension, irrespective of whether they are in favour of extending personal data protection to participation in the economic income generated in downstream or neighbouring markets or whether they advocate protection beyond personal data to include non-personal data generated through the use of a connected device—calling the user of such a device a 'data producer'—, have only justified such extension by reference to justice considerations.[62] This, however, fails to take into account two important concerns: first, justice arguments cannot put aside a sound economic analysis of the issues. Creation of property rights that build on justice in terms of participation in income of others risks reducing general welfare, not least by producing high transaction costs and, thereby, can obstruct optimal use of data in the interest of society at large. Secondly, this approach cannot replace a full analysis of the interests of

[59] DG Internal Market and Services Working Paper—First Evaluation of Directive 96/9/EC on the legal protection of databases (12 December 2004) 24, available at http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf (accessed 30 April 2018).

[60] See, in particular, Art 8 of the EU Charter of Fundamental Rights.

[61] See Art 3(1) of the Proposal of 9 December 2015 for a Directive on certain aspects concerning the supply of digital content, COM(2015) 634 final, which stipulates that the Directive shall also apply where a 'consumer actively provides counter-performance other than money in the form of personal data or any other data'.

[62] See, in particular, Fezer (n 4).

all stakeholders, including the economic interests of the purchasers and users of connected devices and the public interest in free flow of information against the backdrop of the constitutional principle of freedom of information.

2.3 Data access rights as a means to address lock-in effects

The preceding analysis has put the general focus on the concept of ownership as such and, thereby, has highlighted the potential negative effects of data ownership based on the exclusionary nature of property on third parties. In contrast, in its European Data Economy Communication of 10 January 2017, the Commission addresses the possibility of a 'data producer's right' as a means to promote access to data. More concretely, the Commission argues that such a right could 'contribute to unlocking machine-generated data' to enable the 'owner or long-term user' of a device to make use of that device.[63]

With this latter perspective, the Commission clearly adopts a functional approach. Future legislation is discussed as a means to react to a particular market failure. This coincides with the analysis of this Study (at 2.2 above), according to which introduction of new ownership rights is always in need of a justification, most importantly to address existing market failures. By linking the introduction of a data-producer's right with the general objective of promoting free-flow of information, such 'data ownership' seems to avoid colliding with the principle of freedom of information.

In the following, the Study will first delve into problems of potential lock-in of data to the disadvantage of the owner/user of connected devices as a potential cause for such market failure justifying data ownership (at a) below) and then discuss whether there is a need to respond to such lock-in effects by recognising a data-producer's right (at b) below).

a) Data lock-in in case of connected devices

Lock-in effects in the context of connected devices will occur when the owner/user has an (economic) interest in access to the data, while the manufacturer as the data holder has an economic incentive to deny such access. Such situations may not only arise in the case of the use of consumer goods. Rather, this is a problem which arises in markets for any connected device.

The reasons are two-fold: first, 'connected' devices are no longer discrete products. In the era of the Internet of Things (IoT), such devices often need to be connected with other similar devices or have to come with particular 'data-related' services. If the manufacturer of a connected device also offers other devices which need to be connected in a particular situation, the manufacturer will be tempted to refuse access to the data in order to bundle the sale of several connected devices. In the industrial field, machines are nowadays equipped with sensors to control the functioning of the machine primarily for the purpose of predictive maintenance. Yet the operator of the factory will also be in need of access to the data for running an integrated 'smart factory' where all machines need to be connected and where the machines may be supplied by different manufacturers. Without a duty to provide access to the information, the supplier of a connected machine, in which sensors are embedded, could try to bundle the sale of different machines and the sale of the machine with maintenance services. Similarly, in order to preserve competition against tying strategies, a consumer buying a kitchen computer that connects different devices should not be forced to purchase all different devices used in the kitchen from the same supplier. Without the possibility of connecting the devices of different manufacturers, consumers could be technically locked in by their decision to buy a kitchen computer from a given device producer. Whenever one

[63] European Data Economy Communication 2017 (n 9) 13.

of the kitchen devices breaks down, the consumer would only be able to buy from the same supplier again. Therefore, markets for connected devices often demonstrate the features of aftermarkets, where the purchase of one product forces the customer to constantly buy other 'connected' products or services from the same manufacturer or supplier.[64]

The second feature is that the contract regarding a connected device can no longer be regarded as a simple sales contract that is directed at the transfer of property. Rather, for many connected devices, the contract will establish a permanent legal relationship between the supplier and the user regarding services surrounding the use of the device. In some instances, such services are key for the use of the device and can hardly be disconnected from the sale of the device.

This applies, for instance, to connected cars in the era of automated and autonomous driving. In this case, the manufacturer is not only selling the car and transferring the property in the car. The manufacturer turns into a provider of a service for safe driving. Yet not all services will be intrinsically linked to the operation of the connected device. Repair and maintenance services, especially for cars, may also be provided by independent repairers. There is no need that the supplier of a kitchen computer is also the one who decides on who will deliver the milk, whenever the refrigerator identifies the need to order milk. Hence, in the digital economy, the suppliers of connected devices tend to become also providers of data services.

Another highly relevant sector is health care. Devices carried by patients can detect side effects of potentially hazardous drugs long before the patient feels any problem. Drugs may even be swallowed with a sensor attached to it for the purpose of checking the behaviour of unreliable patients.[65] Such information will typically be communicated to the drug producer, transforming this company as a mere provider of pharmaceuticals, prescribed by a medical doctor, into a healthcare provider who takes over monitoring and health care tasks from doctors and hospitals.[66] Still the patient's doctor should not be reduced to a competitor for healthcare services, who may gradually be replaced by the pharmaceutical companies. Rather, centralised access to all the health data, whatever the source is, will be key for optimal health care. This central point of data collection, and the system used for it, should be defined by health policies, taking into account the patient's autonomy and data protection rights, without being undermined by the special economic interests of pharmaceutical companies.

Finally, many start-ups are currently developing data analyses tools for IoT applications without producing connected devices. Examples would be digital management tools for the administration of farms. Such a 'digital' start-up will need to rely on access to all the data collected by the machines working on the fields of a given farmer. As regards consumers, similar data analysis services for smart homes need to connect not just the kitchen devices but also have to control the consumption of energy and water as well as provide security. Of course, such services could equally be provided by the supplier of kitchen devices, the energy or water suppliers or, last not least, independent service providers that do not sell or provide any other goods or other services to the holder of the household.

---

[64] Typical examples are the markets for razors and the razor blades, for printers and the printer cartridges or cars and spare parts.

[65] For the first time ever, in November 2017, the US Food and Drug Administration has granted market authorisation to a drug that is swallowed with a digestible sensor. The sensor has the function of informing the pharmaceutical company that the patient has drug taken the drug for the treatment of schizophrenia. See FDA New Release, 'FDA approves pill with sensor that digitally tracks if patients have ingested their medication' (13 November 2017), available at: https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm584933.htm (accessed 31 July 2018).

[66] Such new technologies are just one way of how digitisation revolutionises health care. The Commission considers the digital revolution of health care more broadly—taking into account telemedicine, personalised medicine, early detection of outbreaks of infectious diseases and accelerated development of pharmaceuticals and medical devices—in its Communication of 25 April 2018 on enabling the digital transformation of health and care in the Digital Single Market empowering citizens and building a healthier society, COM(2018) 233 final.

This is where the focus of the Commission's analysis lies. The Commission's idea to address data lock-in by a data producer's right is very much inspired by the objective of guaranteeing competition in the market, openness of markets for new market entrants and free choice for customers, including consumers, where conflicting interests of the stakeholders could easily hamper the development of markets for connected devices and for the data services attached to them.

The question remains how these concerns can be best addressed. Recognising a data producer's right is by far not the only option. Indeed, the Commission also discusses several options, including contract law legislation in particular.[67]

b) Why competition law does not offer a sufficient solution

The baseline for addressing data lock-ins in the EU is competition law. Within the competition law framework, a refusal to grant access to data would need to be regarded as a case on refusal to deal as a sub-category of an abuse of dominance under Article 102 TFEU. The respective case-law goes back to the *Magill* judgment of 1995 where the CJEU confirmed an abuse of market dominance of TV stations that, controlling access to the listings of TV programs based on Irish and British copyright law, prevented an independent publisher from entering the market by offering comprehensive TV guides including the programs of all TV stations.[68] In this case, the CJEU justified competition law intervention by the fact that the TV stations prevented the emergence of a new product to the prejudice of consumers. This new product rule was later interpreted as an additional requirement in the case of a refusal to license an intellectual property right as compared to other refusal to deal cases.[69] However, application and enforcement of this rule creates considerable challenges.[70]

First, an abuse can only be argued if the data holder is dominant. In the data economy market definition and the assessment of dominance can be particularly difficult, even more so in the relevant cases of aftermarkets where the initial decision to buy a connected device from an individual supplier may well take place in a competitive environment. In addition, it is not necessarily so that the purchaser of a connected device, especially if this is a large industrial customer, suffers from an inferior bargaining position.[71]

Secondly, the refusal to deal has to constitute an abuse. The leading case of the Court of Justice of the EU (CJEU) in this regard is the *Bronner* case, dealing with access to a nationwide home delivery

[67] European Data Economy Communication 2017 (n 9) 12.

[68] Joined Cases C-241/91 P and C-242/91 P *RTE and ITP v Commission* [1995] ECR I-743 = ECLI:EU:C:1995:98.

[69] Explicitly in this sense the General Court in Case T-201/04 *Microsoft v Commission* [2007] ECR II-3601 = ECLI:EU:T:289, para 334. The fact that arguing an abuse would be more difficult in the case where intellectual property are at stake is also indicated by Gerald Spindler, 'Data and Property Rights' (2017) 9 *Zeitschrift für Geistiges Eigentum* 399, 404.

[70] On this see also the author's more extensive analysis: Drexl (n 51) paras 123-42. See also Sebastian Telle, 'Kartellrechtlicher Zugangsanspruch zu Daten nach der essential facility doctrine' in: Moritz Hennemann and Andreas Sattler (eds), Immaterialgüterrecht und Digitalisierung (Baden-Baden: Nomos, 2017) 73.

[71] Here, the Study does not address the issue of whether national competition law rules on the control of superior supplier power based on economic dependence below the benchmark of market dominance could be applied in the relevant cases. For instance, such a rule can be found in Sec 20(1) of the German Act Against Restraints of Competition, which, in practice, is often used in a setting of private enforcement, since it is easier for courts to assess (relative) economic dependence than market dominance, which would typically require a fully-fledged definition of the relevant market and an assessment of the market power of the firm in that market. The reason for not discussing such a rule in this Study is that this is an option that could be considered on the national level, while European law has not developed any competition law tradition in extending enforcement in unilateral conduct cases below the threshold of market dominance.

system for daily newspapers.[72] Under European law, such an abuse requires a refusal to supply an indispensable input, thereby preventing the petitioner from competing in a downstream market. The latter requirement already precludes consumers from relying on this provision, since they cannot be considered 'undertakings' in the sense of EU competition law. But other manufacturers of connected devices or service providers could in principle rely on Article 102 TFEU to argue an abusive refusal to deal. Yet the difficult question remains whether data collected by connected devices can constitute such an indispensable input. The individual data as information will often be publicly accessible and can simultaneously be collected by others, such as the registration of the weather conditions in a particular area by a connected car. Yet the question is whether the fact that collecting and storing the information in a digital format, which makes the information retrievable and treatable, including for the purposes of big data analysis, should not make the digital dataset of the data holder a different and 'indispensable' product. Even if this question were answered in the affirmative,[73] challenges would arise from the relatively restrictive interpretation of the indispensability test in *Bronner*. According to this test, an input will not be considered indispensable if there are no 'technical, legal or even economic obstacles capable of making it impossible, or even unreasonably difficult' to duplicate the resource.[74] In this context, the benchmark for economic obstacles is very high. According to the CJEU, the question is whether duplication would be possible if the petitioner created the resource on a commercial scale comparable to that of the dominant firm.[75] Hence, the mere fact that the petitioner is a considerably smaller firm, such as a start-up, that does not have the economic potential to make the same investment in also entering the market for connected device, would not suffice to explain an abuse. Yet in the *Bronner* case, the CJEU did not take into account the particular features of connected devices.[76]

Competition law may also fail to provide sufficient relief in the field of restrictive agreements in the framework of Article 101 TFEU. Manufacturers of connecting devices may also impose restrictions on distributors that make it more difficult for the final users to get access to the machine-generated data. It would be difficult to argue a violation of Article 101(1) TFEU in a case in which manufacturers could unilaterally deny access in the framework of Article 102 TFEU.[77]

These challenges as well as the difficulty to enforce competition law in each and every case, while these problems are now becoming widespread features of digital markets, strongly argue in favour of taking additional legislative action outside the realm of competition law. Yet such legislation should be competition-oriented.

c) Promoting access through contract law?

An alternative to competition law could be contract law. In this regard, the Commission refers to the working of the Unfair Contract Terms Directive.[78] At first glance, refusal to grant access to data collected by connected devices may indeed be considered an issue of unequal distribution of

[72] Case C-7/97 *Bronner* [1998] ECR I-7791 = ECLI:EU:C:1998:569.

[73] In this sense Drexl (n 51) para 133.

[74] *Bronner* (n 72) para 44.

[75] Ibid, paras 45-6.

[76] See also Drexl (n 51) para 135 (arguing that an abuse could possibly be argued by taking into account the network effects arising from the control of big data, which make it more difficult for newcomers to enter the market).

[77] On restrictions in distribution agreements see at 5.3 i) below.

[78] European Data Economy Communication 2017 (n 9), 12. See Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, [1993] OJ L95/29.

bargaining power, which brings the cases of data lock-in within the realm of the application of the Unfair Contract Terms Directive.

However, this approach also has several shortcomings. First, from the Commission's perspective too, such control would also be needed in B2B relations since especially smaller businesses such as start-ups are as much affected as consumers.[79] Therefore, the Commission considers extending control of unfair contract terms also to businesses.[80] Secondly, there exists no legal benchmark for what can be considered as fair. Hence, the Commission argues that therefore, for extending the fairness control, default contract rules would need to be adopted.[81]

Both challenges show that this solution would not be possible without major legislative actions in the field of contract law, which, as regards the extension of the unfairness control to B2B contract, would certainly produce long and heated debates on the appropriateness of such a major shift in the fundamental fabric of European contract law.

Moreover, two other shortcomings need to be mentioned that cannot be overcome by a reform of the Unfair Contract Terms Directive or an overhaul of EU contract law in general. First, the Directive only applies to contract terms that have not been individually negotiated. Secondly, and more importantly, this contract law solution only works where the person interested in access and the data holder enter into a direct contractual relationship. However, such direct relationship does not always exist. Problems already start where connected devices are resold as used goods to third persons. The third person may not have a contractual claim against the data holder if the claim is not transferred with the property. Even more importantly, the user of a connected device will not always be the owner of the device. Cars may be used based on a lease contract with an intermediary. Smart meters and smoke detectors are frequently leased from service providers. Especially smaller farmers outsource working their fields with particular machines to independent service providers, but still it is the farmer and not the service provider who is in need of access to the data collected by the machines. While mandatory contract law can solve the first problem, it cannot address the second shortcoming. Where connected devices are purchased or used through intermediaries, recognizing direct statutory rights of access to data against the data holder, which hence do not require an existing contractual relationship between the person interested in access to the data and the data holder, would be more likely to produce adequate results.[82]

d) Promoting access through a data producer's right?

The question therefore is whether a data producer's right in data generated by connected devices can appropriately remedy the problem of the data lock-in. The data producer's right as conceived by the Commission raises two fundamental concerns arising from. On the one hand, it risks creating more exclusivity than needed and, thereby, could result in unnecessary transaction costs and impediments to the free flow of data. On the other hand, the data producer's right may not go far enough to effectively protect against data lock-in.[83]

---

[79] According to the Commission, there were 254,850 data companies across the EU in 2016, producing data-related products, services and technologies. See Common European Data Space Communication 2018 (n 1) 3.

[80] European Data Economy Communication 2017 (n 9) 12.

[81] Ibid.

[82] In this sense, the proposal made in the Position Statement of the Max Planck Institute for Innovation and Competition of 26 April 2017 (n 9).

[83] Both shortcomings have already been explained in the Position Statement of the Max Planck Institute of 26 April 2017 (n 9), paras 17-19. See also Drexl (n 9) 235-36.

As regards the—first—problem of exclusivity, it is to be noted that the Commission conceives the 'potential' data producer's right as a right *in rem* that grants exclusive control over the use of data.[84] This is why the Commission wants to take care of the interest in access of other persons than the user of a connected devise (the data producer), including the state seeking access to machine-generated data for the purpose traffic management or environmental reasons, in the framework of exceptions and limitations. This, however, will not suffice. Many commercial users will have an interest in access to the larger—aggregated—datasets of the manufacturer, for instance, of farming machines. The manufacturer's datasets will demonstrate very different utilities than the individual dataset of a single farmer. However, if the datasets of the manufacturer are encumbered by ownership rights in the data of often innumerable data producers (the farmers in the example), the petitioner for access will face considerable problems of rights-clearing.[85] Conversely, the manufacturer will equally have problems to prove its right to sub-license aggregated data where the origin of the underlying raw-data and the identity of the right-holder is practically no longer discernible. In sum, the data producer's right would run the risk of creating excessive, sometimes even prohibitive, transaction costs for the commercialisation of the datasets of the manufacturers and, thereby, undermine the legislative goal of promoting access.

As regards the—second—problem of insufficient guarantee of protection of the interest of the data producer, it is to be noted that the data lock-in problem needs to be understood as one of unequal bargaining power of the user of the connected device, on the one hand, and its manufacturer, on the other. This problem, however, cannot be overcome by the creation of property, since the owner will always enjoy the 'freedom' of assigning his or her property to third persons. Hence, where the manufacturer has an incentive to lock in the user of a connected device, it will include a stipulation in its contracts according to which the ownership in the data collected and produced by the connected device will be assigned to the manufacturer. As pointed out in the introductory part of this Study, this second problem was decisive for the French legislature to reject the motion for the introduction of a data ownership right in personal data, when it implemented data protection rules for the purpose of making the GDPR applicable in France.[86]

In sum, if both arguments are taken together, the better approach to unlocking data, as claimed by the Commission, will consist in recognising non-waivable statutory access rights.[87]

Whether such access rights can also be termed as 'non-alienable data ownership' is very much a matter of taste. If one accepts that the concepts of property is not predefined and that, especially in the field of intangible property and intellectual property in particular, there is a need to clearly define the scope of protection, the use of the term 'ownership' would be not excluded as such.[88] Yet such ownership would not go beyond a mere access right, and, hence, use of the term of 'access right' has the advantage of greater precision. Furthermore, it should be noted that 'access' is not something that specifically characterises ownership. In intellectual property, such access makes no sense in the first place since the intangible and hence non-rivalrous character of the subject-matter

[84] On the concept of a right *in rem* the Commission is using here, see also the analysis by Kim (n 8) 702.

[85] See also Weber and Thouvenin (n 44) 53-54 (arguing that introduction data on ownership would increase rather than reduce search costs). See also Spindler (n 69) 402 (stressing the need for clear indicators for the existence of rights and rejecting the idea of introducing a system of registered data ownership rights). It is to be noted that, even without introduction of a new data ownership right, undertaking a process of rights clearing in the case of big data business models is to be recommended already today to avoid any infringement of database rights or data protection rules. See Dorner (n 26) 627-28. On the relevance of the sui generis database right, see the extensive analysis at 4.2 below.

[86] See at n 34 above.

[87] In this sense, see also the Position Statement of the Max Planck Institute (n 9) paras 20-25. Data access rights as an alternative to a data producer's right is also supported by Rolf H Weber, 'Improvement of Data Economy Through Compulsory Licences?' in: Sebastian Lohsse, Reiner Schulte and Dirk Staudenmeyer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 137, 145.

[88] Indeed, Zech (n 44) 139 includes access to data within the scope of his data ownership concept.

of property, apart from very specific situations, will not prevent the rightholder from using the subject-matter.[89] To equate a right to data access with a property right is more convincing in analogy to tangible property where the owner can claim the tangible object from any third person who, without being entitled to it, is in possession of the item. Yet even this analogy is flawed since the locked-in user of a connected device is not in need of 'de-possessing' the manufacturer of the data. For satisfying the particular interest of the user, it will typically suffice to limit the data access right to a right to 'sharing the data'. In sum, for the purpose of legal certainty, it is better to distinguish between data ownership and data access rights.[90] The latter indeed may also require conclusion of an additional licence to specify the concrete terms of use, especially in the case where the data access regime relies on an obligation to license at fair, reasonable and non-discriminatory (FRAND) terms. In such cases, it is appropriate to characterise the data access regime as a claim for a compulsory licence on the use of data rather than a data ownership right.[91] Hereby, the term 'licence' does not relate to any intellectual property right—since the licensor will often only be a *de facto* data holder. 'Licence' has to be understood as a permission to analyse and make issue of the digital data, including the information it contains, as supplied by the data holder.[92]

2.4 The concept of data and how data are used in the data economy

For discussing the future legal framework for the data economy, including the legal regime for data collected through connected devices both as regards data ownership and access, it is important how the concept of 'data' has to be defined in legal terms.

In general, two issues need to be distinguished. On the one hand, the question is whether legal rules should refer to data as information or only to a set of so-called 'raw data'. On the other hand, the question is whether legal rules should apply only to personal or non-personal data or to both. While it is clear that, depending on the context, the legislature can differentiate as regards the scope and subject-matter of regulation, for discussing both issues, it is important to have a clear understanding of how connected devices, especially those in which sensors are embedded, collect and treat data.

---

[89] Exceptional cases can arise in a copyright context, especially in the field of the visual arts. If the painter sells the painting, she will no longer be able to commercially exploit the work in different forms, such as through the sale of posters, if she is not allowed to access the painting to take a photograph (unless she has made the photograph before selling the painting). Copyright laws therefore grant a right to access the original or other copies of a work. See, for instance, German Copyright Act, Sec 25(1), which provides: 'Der Urheber kann vom Besitzer des Originals oder eines Vervielfältigungsstückes seines Werkes verlangen, dass er ihm das Original oder das Vervielfältigungsstück zugänglich macht, soweit dies zur Herstellung von Vervielfältigungsstücken oder Bearbeitungen des Werkes erforderlich ist und nicht berechtigte Interessen des Besitzers entgegenstehen.' In English (translation by the German Ministry of Justice): 'The author may require that the owner of the original or of a copy of his work make the original or copy thereof available to him insofar as this is necessary for the production of copies or adaptations of the work and does not conflict with the legitimate interests of the owner.' In patent laws, the inventor, based on the right to the patent, can claim the transfer of the patent application or patent from any third persons who has applied for a patent or has been granted a patent for that invention.

[90] Against use of the term 'data ownership' with respect to data access rights, see also Herbert Zech, 'Building a European Data Economy—The European Commission's Proposal for a Data Producer's Right' (2017) 9 *Zeitschrift für Geistiges Eigentum* 317, 320.

[91] See also Weber (n 87) 145 (arguing that in all cases where the data holder refuses access, access will need to be enforced through the grant of a compulsory licence). In a similar sense Mezzanotte (n 45) 175-86 discusses 'non-consensual access regimes'. In contrast to Weber, it has to be noted that even gratuitous and voluntary grant of data access requires the recognition of a contract. This issue is more closely explored by Ruth Janal, 'Fishing for an Agreement: Data Access and the Notion of Contract' in: Sebastian Lohsse, Reiner Schulze and Dirk Staudenmeyer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2017) 271.

[92] Ibid.

a) How data are collected and processed in the context of connected devices

In the discussion on data ownership in the new digital economy, the argument is often made that data can nowadays be traded as any other commodity.[93] While it is true that there are instances where holders of data sell and transfer whole datasets to other parties, use of such a paradigm as a basis for designing the future legal framework would fail to meet the particular circumstances and needs of the digital economy linked to connected devices. In particular, as has already been pointed out further above, the users of connected devices are primarily interested in the getting access to the data. This access will typically be needed for connecting several devices or for enabling data services by a third service provider. Such access will oftentimes not require the complete transfer of the data. What users often need is access to data as real-time data on a permanent basis. Yet transfer of data, namely, in form of data portability, will be required when a user (consumer) wants to switch to a different supplier or service provider.

But what kind of data is collected and processed by connected devices? The very nature of the data will depend on the particular function of the connected device. This function can be limited to collecting, treating and transmitting very specific data, such as in the case of smart meters or a smoke detector. In the case of more complex devices, such as connected cars, the function of collecting and treating data goes much further. It serves the very purpose of operating the car and controlling the functioning of the car in an autonomous manner. Such 'autonomous' or 'smart' devices will often make use of data analytics, machine-learning and artificial intelligence. They treat and analyse data for the purpose of making 'autonomous' decisions in lieu of the user of the device. Thereby, the device will not necessarily only take account of data that is collected by the sensors embedded in the device, but also make use of data that it receives through the Internet from other connected devices. A typical example would be autonomous driving, which critically depends on communication of data among cars and other devices, such as traffic lights and signs.

For discussing the question of 'who should own the data' in the case of on-board data of a car, it is essential to look closer at the way a car collects and processes data. Take the following example: on a winter day, a car enters an icy road. The wheels are equipped with sensors that register the functioning of the wheels. Such sensors register how the wheels turn. Whether this is 'abnormal' will already be a conclusion to be drawn by a computer program that takes account of additional data, for instance, the speed of the car. However, for the car to react to the ice on the street, the auto-pilot also has to make an assessment of the reasons for the abnormality. In particular, the board computer has to distinguish between potential external causes (weather conditions) and international causes (a technical defect of the car). For such an assessment, the auto-pilot will take additional information into account, such as the outside temperature registered by yet other sensors of the same car, or external data, such as the weather forecast for the relevant time and location. Even more, if other connected cars experience an identical problem, data-sharing among these cars would make the analysis of the situation more robust; the cars will almost engage in collective decision making that results in slowing down when car enters this road and alerting other cars to avoid this road.

This example produces the following insights: the sensors of a more complex connected device do not just generate raw data. What interests most is the information that can be drawn from the raw data collected by the sensors. However, the direct information gained from the sensor will typically be very limited. It needs to be further refined by taking account of additional information that can come from various sources, including other connected devices owned by other persons and supplied by other manufacturers. The latter is what characterised not only smart (autonomous)

[93] See, in particular, Herbert Zech, 'Information as a Tradable Commodity' in: Alberto De Franceschi (ed.), European Contract Law and the Digital Single Market (Cambridge, UK: Intersentia, 2016) 51.

driving, but also smart manufacturing, smart homing or smart farming. Data treatment thereby occurs through (big) data analytics, which relies on correlations between different pieces of information whose relevance is assessed based on probabilities. This process of data analysis will often go through different stages where series of new information is produced and further analysed. This shows that the key input in the use of smart devices is not the raw data as bits and bytes as collected by the car, but the information that can be retrieved and gained through further steps of data analyses.[94] Every information that is generated during the process of data analysis may be stored again as raw data. If the legislature wants to reward the major technical contribution to the generation of economic wealth, the data processing and analysis would be a much better candidate as the act giving rise to ownership than the initial encoding of machine-generated data by a device. Still also this value generation would not have been possible without making use of the original machine-generated data. In sum, the issues of data ownership and data access need to take into account this technical context.[95]

In its 2017 European Data Economy Communication, the Commission considers the 'user' of a smart device the 'data producer'.[96] But who is actually producing the on-board data of a car, if the process of production of the concrete data goes through so many different stages? In fact, the question of who produces the data in such circumstances can hardly be answered from a factual perspective. In the relevant moment, the driver as the user of the car at best only decides what road to take—not to mention that such decision is already now oftentimes taken by the navigation system of the car, and the driver does not do so for the purpose of producing specific information about the functioning of the wheels which could then be exchanged with other cars. Compared to others, such as the software programmers, the computer scientists who trained an AI-based program implemented in the car, the providers of data for training AI-applications for cars[97], the providers of external data on which an autonomous car relies during its use and last but not least the manufacturer of the relevant car who technically designed and continuously controls the operation of the car, the driver's contribution appears most minimal and negligible. Hence, only vesting ownership in the user of a connected car amounts to a choice that needs to be justified on normative grounds. In contrast, calling the user of the car a 'data producer', against the backdrop of what is going on technically, even appears as a misnomer. As the person owning the car that finally 'produced' valuable information, the holder of the car may be a better candidate than the person driving the car. As can be observed here, the process of data analysis occurs in a much larger network and is constantly controlled, monitored and even improved by software updates maid by the car manufacturer. To conclude on the question of who produces data in such circumstances, the answer can only be that data production occurs in networks of multiple connected systems and devices to which many actors contribute in various ways.[98] The problem of identifying a 'data producer' with sufficient legal certainty, if the rule should rely be that the right is vested in the

[94] As also stressed by Michael Denga, 'Gemengenlage privaten Datenrechts' (2018) *Neue Juristische Wochenschrift* 1371, 1373.

[95] Whether those who invest in and enable value generation in data analytics should acquire data ownership is rarely considered. For an exception, see Rolf Weber, 'Data Portability and Big Data Analytics—New Competition Policy Challenges' (2016) 23 *Concorrenza e mercato* 59 (highlighting the enormous welfare effects that are generated through data analytics; ibid, 62).

[96] European Data Economy Communication 2017 (n 9) 13.

[97] The Commission also notes that availability of data for training AI applications is a major challenge in Europe. See Common European Data Space Communication 2018 (n 1) 10.

[98] This is now also confirmed by the Commission, stating that contractual agreements should recognise that, 'where data is generated as a by-product of using a product or service, several parties have contributed to creating the data'. Accordingly, the Commission considers 'shared value creation' a 'key principle' to be respected in contractual agreements on non-personal machine-generated data. See Common European Data Space Communication 2018 (n 1) 10.

person who has actually 'produced' the data, may already be seen as an argument against the recognition of a data producer's right.

Apart from difficulties to identify the data producer, the above example also shows that it is not so easy to decide what the subject-matter of protection should be. There are multiple layers of information that is constantly produced, digitally stored and/or re-analysed in almost real time. While ownership is argued to be necessary when data is 'traded', recognition of data ownership for the data holder would oblige to analyse for each and every piece of data and information by whom and how it was generated. Even in the above case general allocation of ownership in the on-board data of a car to a single person—the driver or holder of the car, or alternatively the manufacturer who is in control of access to the data—would not solve the problem that such data will often be generated by making use of data originating from outside the car in which third persons would hold pre-existing data ownership rights. Hence, for the purpose of designing data ownership legislation, the fact that data analyses can go through several analytical steps raises the difficult question of how the rights of multiple layers of data ownership rights of different data producers relate to each other. Should data that are generated through data analytics be considered 'derivative data'—similar to a translated novel—in which separate rights of the owner of the original data and the later data producer coexist? Indeed, the argument according to which data owners should participate in the income generated from the commercial exploitation of data in downstream markets would exactly argue for such a solution. But in network situations as described above, such rights allocation would create a nightmare of overlapping rights of a multitude of rightholders. In such a situation, the question is not only whether a holder of a car—as a potential 'data producer'—can prohibit the commercialisation by others—including the manufacturer of the device in particular—for the purpose of participating in the revenue collected from secondary markets. The question would also arise whether the holder of the car also has to take a payable licence for the use of external data when using the car.

Beyond this legal challenge, use of existing data ownership rights for the production of 'derivative' data creates factual problems. Use of systems based on deep-learning and artificial intelligence (AI) algorithms de-personalise the process of data production and processing. In such a technical environment it will typically be impossible to identify which data was used by an artificial intelligence program to reach a particular result. In the case in which connected cars of different manufacturers collectively slow down when entering an icy road, it may well become impossible to identify which data owned by whom was used to reach such a result. This explains that it is will be practically impossible to monitor the use of other persons' data in such complex network scenarios.

In contrast to data ownership, pure and simply reliance on *de facto* data holding and data access rights will avoid these problems. The reason is that the latter approach does not interfere with, and obstruct, the technological development and emergence of new business models upfront by recognising property rights that lead to transaction costs as well as problems of rights clearing and monitoring. This approach avoids the design of a complex ownership rights system that has to build on general definitions of the rightholder, the subject-matter of protection and the scope of protection. Rather, the recognition of access rights builds on existing interests. The data holder is in principle free do develop new business models linked to the use of data, including those relating to connected devices, but will have to grant access to data where identifiable interests of third parties justify such access rights. As regards the entitlement to access, the question is not who produced the data or even who uses a connected device, but who has a legitimate interest in access to the data collected by a connected device. Hence, this interest relates to the concrete data collected and, therefore, does not necessarily have to be linked to the use of a device. For instance, if data of the soil of a farmer is collected by a sowing machine that is operated by an independent company to whom the farmer has outsourced the sowing activity, the data access right against the manufacturer of the sowing machine who holds the data should be directly vested in the farmer and not the holder (user) of the sowing machine. The argument is that the farmer has a legitimate interest in access to the data collected from his land.

Compared to data ownership, data access rights therefore constitute the less interventionist form of regulation. Cases where data holders will anyhow have strong incentives to share data with other data holders, such as the different car manufacturers to increase the safety of driving, will not be burdened with additional legal uncertainty and the need of rights clearing. Data access rights, which can also be designed in more targeted ways for particular scenarios and sectors,[99] only become relevant where otherwise the data holder would refuse to voluntarily grant access to data and where, based on a balancing of all interests involved, the data holder should not be allowed to refuse access to the data.

b) Raw data or information?

As explained further above, recognising data ownership may distort free flow of information. However, the discussion on whether data ownership rights should be recognised does not relate to ownership in information, but to the raw data from which information could be extracted.[100] The raises the question of whether limiting data ownership to raw data can avoid undue restrictions on the free flow of information.

This question must be answered in the negative.[101] The reason is that the raw data is not an asset that can be completely separated from the information it contains. In this regard, it is important to look at data markets from the perspective of semiotics. According to semiotics, at least three levels of information need to be distinguished: (1) the structural, (2) the syntactic, and (3) the semantic level.[102] These levels relate to (1) the physical career of information (for instance, a book), (2) the signs in which the information is encoded (for instance, the letters in which an information is encoded) and (3) the meaning that can be taken from the data (for instance, by reading a book).

General ownership rights in information on the semantic level should strictly be avoided, since such ownership would clearly undermine the inbuilt limitations of the intellectual property system.[103] In particular, recognition of ownership rights in any information on the semantic level would amount to intellectual property protection without the requirement nor the guarantee that such information promotes innovation.[104]

---

[99] In favour of sector-specific legislation on data access rights, Position Statement of the Max Planck Institute (n 9) para 23. On the question of whether a sector-specific approach is to be preferred, see also at 5.3 g) below.

[100] This also seems to be the position of the Commission when it discusses property in 'raw machine-generated data'. See European Data Economy Communication 2017 (n 9) 10. Here, as the European Data Economy SWD 2017 (n 9) 34, shows, the Commission takes inspiration from the proposal of Zech (n 93) 74 (claiming that a data producer's right should be limited to the syntactic level of information).

[101] This opinion is shared by other scholars. See, in particular, Hugenholtz (n 52) 91-92 (showing that data ownership even if limited to the syntactic level could particularly be used against the copying of a copyrighted work encoded in data with a disruptive impact on the possibilities of a copyright holder who could no longer exploit its works without consent by the data owner).

[102] Sometimes, an additional—'pragmatic'—level is mentioned. On this level, information conveys knowledge, which can be used for achieving a particular effect, or the information serves a particular function. See, for instance, Weber and Thouvenin (n 44) 46-47; Andreas Wiebe, 'Protection of industrial data—a new property right for the digital economy?' (2016) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 877, 881 (distinguishing between the syntactic, the semantic and the pragmatic level). Wiebe, ibid, 881-82 argues that intellectual property rights can be located either on the semantic or the pragmatic level (with patents and trade marks allocated to the pragmatic level). He further argues that also any data ownership right should therefore focus at least on the semantic level. Ibid.

[103] In this sense, see also Heymann (n 26) 650-51. In this context, Wiebe (n 102) 881 warns against a paradigm shift in intellectual property law.

[104] See also Dorner (n 26) 625; Kim (n 8) 705. Data ownership on the semantic level is also rejected by Zech, who was the first author to promote the idea of data ownership in raw data on the semantic level. Zech (n 90) 322.

This does not mean that ownership rights on the structural and syntactic level cannot result in any barriers to free flow of information on the semantic level.[105] If, for instance, certain information is only contained in an ancient book or manuscript for which only one copy exists, the owner of this book and manuscript will also be in control over access to this information by denying access to the book. This is even a problem today. Although copyrights in old writing has expired, there are many archives and libraries that control access to text documents that belong to the world's cultural heritage. Not only to preserve these documents, but also to provide access of the public to these documents and the information they contain, such memory institutions nowadays work on digitising these documents.

Ownership in raw data seems to refer to the syntactic level, since information can be encoded in bits and bytes.[106] Barriers to access to information can also result from exclusivity on this sign level. As explained above (at 2.2 d)), copyright takes precautions to avoid such barriers by only protecting the creative expression of the information, while the letters and individual words used for expressing information are not protected.[107] Thereby, copyright law even promotes free flow of information, since it creates incentives for publishing writings—which is most important for the press and academic publishing—by prohibiting direct copying. But the same information (on the semantic level) may still be communicated by others by using different wording.

In case of ownership in raw data, the situation is more complex. Raw data is not just a sequence of binary digits in which the information is encoded. Ownership in raw data would relate to the concrete encoding of information as part of a given dataset. It is true that the same information could independently be encoded in another dataset—for instance, if two cars enter an icy road and, after running through several analytical steps finally produce raw data from which the information can be taken that there is ice on the road.[108] Hence, data ownership in separate raw data could co-exist although they contain the same information. None of the two data owners will—strictly speaking—own the information on the syntactic level.

Still, this form of ownership would also obstruct free flow of information. Problems for free flow of information arise, first, from the *erga omnes* effect of such data ownership and, second, from the fact that third parties' interests do not specifically relate to the binary code, but the semantic information (meaning) that can be taken from the raw data. If data holder A grants access to its datasets to B for allowing B to analyse this dataset, this is done so because B hopes to find valuable information in this dataset. Yet, if the law recognised data ownership right in the raw data and the analysis constituted use of the data ownership right, B would run the risk of infringing third parties' rights in some of the data contained in A's dataset. Or to put it differently, also ownership in raw data burdens transactions, whose purpose it is to provide access to information, with additional transaction costs and the need for rights clearing. This is exactly the situation in which a third party would find itself who seeks access to the datasets of the manufacturer of connected devices. If the

[105] See also Heymann (n 26) 653 (arguing that ownership in 'structural' or 'syntactic information' will have an impact on 'semantic information', since the former carry or encode the latter); Wiebe (n 102) 882 (arguing that protection of raw data on the syntactic level would indirectly affect access to information on the semantic and pragmatic level and, thereby, produce a chilling effect on access to the use of information); see also Andreas Wiebe, 'A New European Data Producer's Right for the Digital Economy?' (2017) 9 *Zeitschrift für Geistiges Eigentum* 394, 396. Doubts on whether such limitation of protection to encoded, ie syntactic, information is possible at all and whether it can avoid monopolisation of information are also expressed by Kerber (n 2) 992 and 997.

[106] This is especially the approach advocated by Zech. See Zech (n 90) 322 ('data may be defined as information coded to be machine readable').

[107] In *Infopaq*, the judgment in which the CJEU started to develop a European concept of a work, the question was whether a sequence of 11 words can already be considered a person's own intellectual creation. See Case C-5/08 *Infopaq* [2009] ECR I-6569 = ECLI:EU:C:2009:465, para 45, holding that '[i]t is only through the choice, sequence and combinations of those words that the author may express his creativity in an original manner and achieve a result which is an intellectual creation.'

[108] See also Weber and Thouvenin (n 44) 47.

law recognised ownership rights of the users of such devices in the data they generate, the manufacturer who wants to commercialise the aggregated data would have to show that it is indeed authorised to do so either after a transfer of the ownership in the data by all the original rightsholders ('data producers') or after a grant of respective licences.

In sum, ownership rights in raw-data (on the syntactic level of information), with all its third-party effects, would exercise a gatekeeper role as regards use of data on the semantic level.[109] This shows that the negative effects of data ownership rights cannot be avoided from shifting protection from the semantic to the syntactic level of information. Ownership in raw-data should therefore meet the same concerns of undermining the inbuilt limitations of the intellectual property system as ownership in data on the semantic level of information.

c) Personal and non-personal data

In its free-flow-of-data initiative, the Commission acknowledges that machine-generated data can be personal or non-personal.[110] This is particularly true in the case of data generated by connected devices that are used by humans, such as cars or household devices. Both kinds of data will therefore regularly be found in the datasets of manufacturers of such devices.[111]

The capturing and processing of personal data falls within the scope of application of the General Data Protection Regulation (GDPR). Hence, any future legislative action has to take into account the applicability of the GDPR to parts of the data that are collected by collected devices.

The GDPR is highly relevant for the debate on access and control of data collected by connected devices, since it contains a series of statutory rights that relate—in a broad sense—to access and control. In particular, Article 15 provides for a right of access of the data subject against the data controller, which includes a right to obtain a copy of the personal data the controller is processing.[112] Most powerful is the right of the data subject to erasure especially after withdrawal of the consent to the processing of personal data.[113] And finally, the data portability right of Article 20 GDPR can be considered a most important right that is not only designed as a right enhancing the autonomy of the data subject, but also a pro-competitive means addressing economic data lock-ins where the data is processed based on a contract with the data subject.[114]

For the future legal framework for data generated by connected devices, these rights are important in two different ways. On the one hand, they may be considered as a template for general legislation

[109] This analysis confirms the claim that intellectual property rights should be limited to the semantic and pragmatic level of information. See Wiebe (n 102) 882 (more based on the analysis of existing intellectual property rights).

[110] European Data Economy Communication 2017 (n 9) 9.

[111] Ibid.

[112] Art 13(3) GDPR.

[113] Art 17(1)(b) GDPR.

[114] See Recital 66 of the GDPR. See also Inge Graef, Jeroen Verschakelen and Peggy Valcke, 'Putting the right to data portability into a competition law perspective' (2014), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416537 (accessed 31 July 2018). Use of Article 102 TFEU as a means to enforce data portability is analysed by Aysem Diker Vanberg and Mehmet B Ünver, 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' (2017) 8(1) *European Journal of Law and Technology* at 8-11, available at: http://ejlt.org/article/view/546 (accessed 31 July 2018); and Barbara Van der Auwermeulen, 'How to attribute the right to data portability in Europe: A comparative analysis of legislations' (2017) 33 *Computer Law & Security Review* 57, 61-63.

of rights of access to data, including non-personal data.[115] This is especially true for the data portability right. On the other hand, if new data ownership rights were recognised, whether vested in the data subject or, even more so, another person, such new rights would need to be coordinated with the data protection rights under the GDPR to exclude any conflict or friction.

The Commission also seems to acknowledge the risk of conflicts between property rights in machine-generated data and personal data protection. These concerns become most obvious when the Commission explicitly restricts the discussion of a potential data producer's right to non-personal data.[116] Indeed, the Commission thereby tries to avoid any conflict between a new data producer's right and the data subject to withdraw her consent regarding personal data at any time.[117] Such limitation will necessarily make it difficult to distinguish between the two kind of data in practice.[118] Given the fact that both personal and non-personal data will regularly be found in the same dataset, limitation of data property to non-personal data would also considerably limit the relevance of legislation on a data producer's right. The only way out of the problem is found by the Commission arguing that personal data can still be anonymised to become the subject-matter of a data producer's right the use of which can be licensed to others.[119]

From a legal perspective, however, personal data protection does not necessarily have to exclude a parallel data producer's right vested in another person or where the data subject as the original data producer has assigned the right to another person. If the data subject withdraws consent and asks for erasure of the data according to Article 17(1)(b) GDPR, this would destroy the subject-matter of the data producer's right in the raw data that encodes the personal data and thereby negate the data producer's right of the other person. But this is not unusual in the intellectual property realm, especially when intellectual property rights conflict with real property. In particular, the holder of an intellectual property can claim destruction of an infringing good owned by another person.[120] In other words, if an additional data producer's right would be recognised also for personal data, the legislature would have to decide, in case of conflict, which right prevails over the other. Hence, a generally applicable data producer's right could also be introduced that, in the very moment of coming into its existence, will be encumbered with the data protection rights, thereby fully respecting the rules of the GDPR.

If the legislature decided to introduce a data producer's right at all, this solution should be preferred to a limitation of a data producer's right to non-personal data for two reasons: first, the Commission's approach to find a solution in anonymisation collides with the idea to vest the data producer's right in the 'owner or long-term user'[121] of the connected device. A right of this person presupposes that the right comes into existence through the use of the device as the act of producing the data. The later anonymisation will typically be undertaken by another person,

[115] For instance, in its Common European Data Space Communication, the Commission now argues that also companies offering a product or service that generates (non-personal) data as a by-product should allow and enable data portability as much as possible. Common European Data Space Communication 2018 (n 1) 10.

[116] European Data Economy Communication 2017 (n 9) 10.

[117] Ibid. This is obviously overlooked by Zech (n 90) 323, criticizing the limitation of data ownership to raw data encoding non-personal data as 'unnecessary' since raw data would only be protected on the syntactic level. Here, Zech ignores the restrictive effect of exclusive rights in information on the syntactic level for access to information on the semantic level. As the GDPR proves, although it protects personal data on the semantic level, its data protection rights, for being effective, also extend to the syntactic level like in the case of the right to erasure.

[118] This is an argument for Weber (n 87) 143-44 to argue that a data ownership right cannot be limited to non-personal data.

[119] Ibid. The Commission states: 'Personal data would need to be rendered anonymous in such a manner that the individual is not or no longer identifiable, before its further use may be authorised by the other party.'

[120] See Art 10(1)(c) Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, [2004] OJ L157/45.

[121] See European Data Economy Communication (n 9) 13.

namely, the manufacturer as the *de facto* data holder. Accordingly, if the act of anonymisation is the relevant act of creating (anonymised) raw data as the object of the data producer's right, the right in this regard would need to go to the manufacturer. This would however run counter to the legislative goal of using the data producer's right as a means to unlock data in the interest of the user. Furthermore, if one recognised a data producer's right of the manufacturer in the anonymised data, different pieces of raw data that are included in the same dataset—original non-personal data, on the one hand, and anonymised data, on the other—would be owned by different persons, while it would be extremely difficult, if not practically excluded, to distinguish between the two kinds of data.

The second argument stems from the very concept of personal data. Personal data falling within the scope of the GDPR is not only information relating to an identified natural person, but also data relating to an identifiable person.[122] According to the GDPR, data that can be 'attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person'.[123] Such additional information that is needed to make the natural person identifiable does not have to be part of the same digital dataset. Given the potentials of big data analytics, which allows to draw probability conclusions from correlations between different pieces of information, it is no longer possible to neatly distinguish between non-personal and personal data.[124] Even more, re-identification technics as part of big data analytics can be used to retrieve the person behind anonymised data.[125]

Yet the concerns that lead the Commission to argue against a data producer's right in machine-generated raw data that contains personal data underline a major dilemma. On the one hand, legislation on a data producer's right concerning data generated through the use of connected devices has to take into account the technical and economic reality that the resulting dataset will often, and to a large extent, contain personal data, and that therefore legislation should not be limited to non-personal data. On the other hand, it is to be accepted that the rules of the GDPR will need to be applied and take precedence over the economic rights of the data producer.

This dilemma seems to argue in favour of allocating the data producer's right to the 'data subject' in the sense of the GDPR. But even this is no viable solution. It is not necessarily so that connected devices will only collect data about one person. Personal data can relate to several persons at the same time, for instance, it the data conveys information about the interaction and relationship among two or more persons. Such multi-personal data can also be collected by connected devices. The most obvious example is a smartphone that registers with whom its users communicates.

In sum, a data producer's right that also applies to personal data and, simultaneously, is encumbered with data protection rights of third persons, has to raise doubts about its suitability as a key component of the legal framework of the modern data economy.

In contrast, recognition of access rights to persons who have a legitimate interest also offers a superior solution as regards the relationship with data protection rules. Those rights would be directed against the data holder who will only be able and allowed to grant access in the framework of the rules on data protection. With regard to data protection, data access rights do not add any additional legal complexity. If the data holder wants to grant access of third persons to its datasets, it will only be allowed to do so within the framework of the data protection rules. This mechanism is also expressed in Articles 15(4) and 20(4) GDPR, providing that the right to data access and the

[122] Art 4 No 1 GDPR. On this notion of an 'identifiable person', see also Manon Oostveen, 'Identifiability and the applicability of data protection to big data' (2016) 6 *International Data Privacy Law* 299, 305-306.

[123] Recital 26 of the GDPR.

[124] On these difficulties, see also Oostveen (n 122) 306, who point out that identifiability is always context-specific and probability-based.

[125] Weber (n 87) 144.

right to data portability 'shall not adversely affect the rights and freedoms of other'. These provisions also cover the case where data access and data portability would affect the data protection rights of another natural person.[126] In line with this rule, data access rights could be recognised in full respect of the data protection rules.

3 Objectives of regulation and relevant interests

This study seeks to assess and make policy recommendations on the future legal framework for connected devices by taking into account the specific perspective of consumers. However, consumers are just one group of relevant stakeholders. In the following part, the Study will therefore locate consumer interests in a broader regulatory framework, which takes account of all relevant regulatory objectives and interests as well as the interactions between them. This enterprise is especially designed to create transparency about the value judgments and the necessary balancing of interests that will guide the analyse in the subsequent parts of this Study.

3.1 Toward a regulatory theory for the data economy

This Study builds on a regulatory theory the seeks to analyse legislation on the data economy against the backdrop of four key objectives that need to be considered simultaneously. These four objectives are: (1) establishing functioning and competitive market for the data economy; (2) promoting innovation; (3) protecting consumer interests with a particular focus on protecting the privacy of natural persons; and (4) promoting additional public interests.

Apart from consumer interests and privacy concerns, these goals do not explicitly mention any other stakeholder interests. In particular, these objectives do not specifically mention the interests of the firms operating in the digital sector. The reason is that the business models of the firms are to be considered the object of regulation. Therefore, their interests, including their fundamental right of conducting a business[127], will primarily be taken into account as part of a classical fundamental rights analysis by balancing them with the public interest and the rights of others on which the state relies as a basis for regulation. Yet, as will be explained in more detail further below, the public interest dimension of guaranteeing the freedom of firms to conduct a business is also captured by the first objective of guaranteeing functioning and competitive markets.

Yet the focus here will be put on the four key objectives since the interaction between them is highly complex in itself; and it appears as highly important to identify and coordinate all relevant objectives that legislation should aim to achieve in designing the future legal regime for connected devices and the digital economy in general.

The four objectives should also primarily be understood from a public interest perspective. This is also the case as regards consumer interests, since all citizens of society will constantly and

[126] See Recital 68, sentence 8, GDPR: 'Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation.' The underlying data protection and intellectual property concerns arising from the data portability right are described by Van der Auwermeulen (n 114) 60. In this regard, it is even argued that the data portability right would be excluded in the case of a picture uploaded on Facebook that does not only show the data subject, but also other persons. See Diker Vanberg and Ünver (n 114) 3. This, however, appears rather doubtful since, in the framework of Art 20(1) GDPR, it must have been the data subject who has uploaded the picture. Hence, it does not seem that data portability for the purpose of migrating with the picture to another social platform would interfere with the data protection interests of others more than the posting of the picture on Facebook in the first place.

[127] Art 16 EU Charter of Fundamental Rights.

practically everywhere be exposed to the digital sector, including the operation of connected devices.

The starting point of the theory is the first objective. To guarantee functioning and competitive markets is the very purpose of the economic regulation with the contract law system and competition law as its key legal instruments. For many sectors, focusing on this particular objective may already suffice. Secondly, digitisation and, more specifically, the advent of connected devices, also expresses an enormous innovation. Society has a general interest in generating the societal benefits linked to digital innovation. Thirdly, digitisation also comes with increased challenges for society, especially due to the collection of vast amounts of personal data. The digital sector therefore requires a broadening of the regulatory market theory that integrates personal data protection as an additional and integrated element. Fourthly, although already the first three objectives have to be regarded as public interests, the digital economy is also relevant from the perspective of many other public policy grounds. Even the state itself will often have a vital interest in getting access to the vast amount of data that is now collected through the digital economy, for instance for the purpose of guaranteeing safety in driving, helping the State in urban planning, enhancing protection of the environment or public health.[128] Digital business models, especially those of social platforms, allowing the sharing of political news and opinions among individuals, can have a tremendous impact on the democratic process by shaping political convictions of citizens. As an overarching concern in the digital economy, the interest in guaranteeing freedom of information, not least as a key component of a democratic society, also has to be attributed to these further public interests.

These four objectives reflect the constitutional framework of fundamental rights in its entirety. Guaranteeing functioning and competitive markets does not only constitute a public interest goal. It also expresses, and is supported, by the fundamental rights of the market participants, namely, the freedom to conduct a business[129] and the constitutional protection of property[130]. Personal data protection in the EU is constitutionally closely linked with the protection of private life.[131] Public interest grounds also express fundamental freedoms and social rights of citizens.[132] This shows that the four-objectives regulatory theory also provides a comprehensive theory for assessing regulation of the economic economy from a justice perspective. This has very important implications. Recommendations that are based on pure justice arguments without being capable of being explained against the backdrop of this regulatory theory should in principle be considered as unfounded.

The four objectives are characterised by intensive interactions. On the one hand, they are not inherently in conflict with each other, but to a large extend, mutually supportive. For instance, competition can enhance innovation[133], and innovation and competitive markets are expected to

[128] In its 'data package' of 25 April 2018, the Commission therefore complements a reform of the PSI Directive with an examination of how access of the public sector to private sector data can be enhanced through preferential treatment of re-use. See Common European Data Space Communication 2018 (n 1) 12-14.

[129] Art 16 EU Charter of Fundamental Rights.

[130] Art 17 EU Charter of Fundamental Rights.

[131] Art 8 EU Charter of Fundamental Rights (right to personal data protection); Art 7 EU Charter of Fundamental Rights (right to respect for private and family life).

[132] For instance, Art 2(1) (right to life); Art 11 (freedom of expression and information); Art 34 (social security and social assistance); Art 35 (rights to access to health); Art 37 EU Charter of Fundamental Rights (right to environmental protection).

[133] This is nowadays accepted in modern competition policy. Even intellectual property rights are no longer considered to be inherently in conflict with the principle of competition (so-called 'inherency theory'). Rather, intellectual property and competition law are considered to pursue complementary goals by creating incentives for firms to invest in new and improved products and processes and by maintaining competitive pressure on undertakings to innovate. See

serve consumers better. But, of course, there are also tensions. In the following, the analysis will therefore turn to explore these interactions more thoroughly and thereby put an emphasis on the consumer perspective.

3.2 The four objectives and their interactions

a) Guaranteeing functioning and competitive markets

It is in principle presumed that, based on freedom of contract, free markets will work best and produce efficient results. A fundamental condition for this is that markets are characterised by competition. Therefore, competition law complements contract law to prevent undertakings from anti-competitive conduct.

In a market economy, additional interventions may be needed to respond to market failures. Instruments adopted by the legislature to remedy such market failures include intellectual property and consumer protection laws. At least to some extent, they deviate from the principles of competition—intellectual property does so by excluding competition by imitation—and freedom of contract.

Accordingly, new ownership rights, from a market regulatory perspective, are also in need of an economic justification. This identifies intellectual property rights as 'functional' property. They are introduced by the legislature to improve the market results. To reach such results, the legislature however makes use of the private interests of economic actors by recognising private property rights as a decentralized form of regulation. Thereby, the legislature expects that markets will work better through private ordering. Yet this also means that the legislature should refrain from recognising 'dysfunctional' intellectual property rights that hamper the working of markets instead of enhancing their well-functioning. In addition, the legislature should take precautions against strategic use of intellectual property rights understood as use of rights in conflict with the goals pursued by the intellectual property legislation.

Accordingly, as a matter of principle, mere justice considerations, without being supported by a sound market-failure analysis, cannot justify the adoption of new intellectual property rights. This also applies to the introduction of potential data ownership rights.[134] In particular, the mere fact that data generated by connected devices has economic value and can also be commercialised in secondary markets cannot explain that economic rights of exploitation shall be attributed to the owner or user of a connected device. Without a market failure such legislation would risk creating harmful transactions costs and, therefore, distort the working of data markets rather than improving them.

Yet the recognition of access rights is equally dependent on a market-failure analysis. In principle, from a purely market-regulatory perspective, data holders should not be obliged to grant access to data without evidence of such market failure. Typically, a competition law analysis would provide the legal standard for intervention. However, as already argued further above[135], *inter alia*, the difficulties to enforce competition law as well as the fact that refusal to grant access to data may now become a mass phenomenon, can argue for data access rights. Market failure analysis in this context can also argue in favour of more targeted sector-specific approaches that take into account the specific circumstances of the relevant markets.

Guidelines of the Commission of 28 March 2014 on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements, [2014] OJ 89/3, para 7.

[134] On the analysis of potential market failures as a basis of data ownership see Drexl (n 51) paras 73-102.

[135] See at 2.3 b) above.

b) Enhancing innovation

Digitisation can and should be viewed as a major driver of innovation. According to the OECD Oslo Manual, four different kinds of innovation can be distinguished: (1) product innovation; (2) process innovation; (3) organisational innovation; and (4) marketing innovation.[136] All of these kinds of innovation require implementation.[137] This means that new developments can only be termed as innovations if they reach the market and thereby create benefits for society. In contrast, new technological developments that are retained by the developer and never get implemented are irrelevant from an innovation policy perspective. In addition, a distinction has to be made between innovation, on the one hand, and 'innovation activity', on the other hand. According to the Oslo Manual, 'innovation activities are all scientific, technological, organisational, financial and commercial steps which actually, or are intended to, lead to the implementation of innovations.'[138] Hence, innovation activities are part of the innovation process. Patent law, for instance, may set incentives for innovation activities. But neither the invention nor the patent granted for the invention can be considered an innovation, or protecting an innovation, as long as the invention is not implemented.

In the digital sector, all four kinds of innovations can be identified. Connected devices constitute above all *product innovation*, namely, in form of the 'introduction of a good or service that is new or significantly improved with respect to its characteristics or intended uses'.[139] Connected devices bring major benefits for the users of consumers, for instance, in form of new utilities, safety or user convenience.

Connected devices, especially employed in manufacturing, can also lead to *process innovation*. A machine, in which sensors are embedded for the purpose of predictive maintenance, will help the manufacturer avoid unforeseen downtimes. By reducing costs, such process innovation will also enable the manufacturer's ability to compete on price, and indirectly serve markets better with more and cheaper goods. Sensors that control the quality of the goods during the manufacturing process constitute process innovations for the manufacturer, but product innovations for consumers. Process innovation can also relate to delivery methods.[140] The digitisation of content and the distribution of digital copies of works without a physical carrier (music, films, videogames, news, literature, computer programs) through the Internet has to be considered as process innovation. The same can be said about digital tracking systems for goods in the logistics sector.[141]

To a large extent, the digital environment is characterized by organisational and marketing innovations. Connecting the different machines and devices in a factory as part of a digital quality management[142] can be considered a form of *organisational innovation* as the implementation of a new organisation method in a firm's workplace.[143] This also means that not only providers of connected devices should be considered innovators. Companies seeking access to the data held by the suppliers of connected devices to digital management services to factories, farms or

[136] OECD, Oslo Manual—Guidelines for Collecting and Interpreting Innovation Data (Paris: OECD, 3rd edn 2005) paras 31 and 155-84.

[137] Ibid, paras 146-47 and 150.

[138] Ibid, para 149.

[139] Ibid, para 156.

[140] Ibid, para 163-64.

[141] Ibid, para 166.

[142] Ibid, para 180 (explicitly mentioning quality-management systems).

[143] Ibid, para 177 (on the notion of organisational innovation).

households should also be considered innovators. Hence, data access rights can also promote innovation.

Marketing innovations can particularly be observed in the Internet economy. Generally referring to new marketing methods,[144] these innovations also include the new business models of the sharing economy (e.g., Uber, AirBnB) or of the Internet platform economy that offer digital services exclusivity financed through advertising, and without any monetary consideration by the users (e.g., social platforms and search engine operators).[145] For consumers, these business models provide them with services they like without having to make any financial investment.

From a regulatory perspective, the most important feature of all these innovations is that they seem to be much more driven by competition than intellectual property. Yet digitisation of products also involves inventions and their protection by patents. Development and standardisation of mobile telecommunications technologies strongly patent protection plays a crucial role. Computer programs used for big data analysis are protected by copyright. Yet the most important driver of the digital economy is competition. Firms invest in digitising their factories, their products and their distribution based on the assumption that they would run the risk of otherwise soon having to leave the market. Participating in the digital revolution also for many manufacturers of connected devices has become a 'competitive must'. For the economic success of the big Internet firms, which are today among the most prosperous and capitalised firms of the world, intellectual property has not played any significant role.[146] This shows in general that data economy markets develop particularly without the need of additional state intervention as regards the goal of innovation.

c) Consumer protection, and data protection in particular

Especially the concern about personal data protection distinguishes digital markets from other markets. This concern requires a broader regulatory perspective.

Although they create individual rights of control—a feature shared with property rights—data protection rules impact markets very differently. They are not adopted to optimise the functioning of the market, but to protect the privacy interest of the data subject.[147] They therefore risk colliding with the economic goals of both guaranteeing optimally functioning markets and enhancing innovation. Indeed, there is a risk that the requirements of the GDPR put too much of a burden on

[144] Ibid, para 169.

[145] Here, the question is whether granting access to personal data on the part of the user can be considered a counter-performance. Economists consider such platform markets as 'attention markets'. According to this idea, users pay with 'attention', expressed by the economic value of the time they spend on such platforms. See David S Evans, 'The Economics of Attention Markets' (1 November 2017), available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3044858 (accessed 31 July 2018) (according to Evans, in 2016, US American adults spent 437 trillion hours on ad-supported media websites, amounting to a value of US$2.8 trillion based on average after-tax minimum wage rate).

[146] In fact, the most valuable assets for firms such a Google and Facebook are the algorithm they use and the customer data they control. The latter is protected by technical protection measures (on trade secrets protection see at 4.4 below). Computer programs are protected at least through copyright law. However, even the computer program as such may prove to be of little value to a competitor, if the latter does not have access to the data.

[147] The difference of objectives is also observed as a starting point of the analysis of the relationship between data protection and competition law by Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection Between Data Protection and Competition in EU Law' (2017) *Common Market Law Review* 11, 12. In line with the approach taken in this study, the authors advocate a holistic approach, based on the understanding that both fields of the law are part of EU law that share the objectives of market integration and wellbeing of citizens. On the data protection and competition law interface, see also Weber (n 95) 63-66.

firms and that high standards of data protection in the EU could reduce international competitiveness of the European data economy as compared to the US and China in particular.[148]

Still this perception appears too one-sided. Data protection can also be considered a condition for developing digital markets and even a driver of innovation, since the goods and services of the data economy will only be accepted by consumers and other customers if their privacy and confidentiality concerns will be respected.[149] This holds true both for natural persons and firms. A manufacturer will only accept data collection through the sensors of a machine in its factory for the purpose of predictive maintenance, if the supplier of the machine refrains from making the data collected by the machine accessible to competitors of the manufacturer. Such data will often constitute trade secrets of this manufacturer.[150] Consumers will be less likely to put smart kitchen devices in their homes, if they don't know, and cannot control, which data on their living habits is collected and to whom such data is made accessible.

Moreover, from an economics perspective, data protection can be conceived as a legal instrument to respond to a particular market failure. Where data treatment is related to connected devices and the provision of services, the transaction is characterised by an information asymmetry. Without legal intervention the suppliers of connected devices and providers of digital services could freely decide on what and how much data they collect from the customers and how they process them. Of course, potential customers could refuse to buy products and services from firms that do not commit to the level of confidentiality they prefer. Yet a customer will not be able to monitor whether the other party fulfils the confidentiality obligations of the contract. Sufficient protection of personal data and trade secrets, combined with effective remedies, is therefore a condition for data markets to work. Against this backdrop, data protection also has to be considered as a key element and an integral part of modern consumer protection law in the digital sector.

It is often believed that individuals today care less about privacy than in the past. Certainly not all citizens value data protection the same way; and technical tools to reduce the collection of data through connected devices, for instance by turning off the geolocation function of a smartphone, although they may be available and easy to handle, are not or only rarely used. But this does not argue against the existence of a market failure in form of an information asymmetry. Even more, the concrete behaviour especially of persons using the services offered by social platforms and search engines that collect vast amounts of personal data does not prove that these persons do not value privacy anymore. Rather, an explanation could also be found in a data protection paradox. People still value data protection highly but have at the same time already largely given in to the fact that they can no longer control who knows what about them. Hence, mindless use of the Internet may also largely be caused by the omnipresence of the collection of data in the daily life of everybody, which influences and shapes our behaviour. As regards the question of how the legislature should react to this phenomenon, the answer should not be to simply accept that attitudes have changed

[148] For instance, it is argued that especially Article 20(1) GDPR granting a data portability right against all data producers without the competition law safeguard of Article 102 TFEU, requiring market dominance, would unduly restrict the business opportunities of small and medium-sized enterprises as well as start-ups. See Diker Vanberg and Ünver (n 114) 4; Graef, Verschakelen and Valcke (n 114) 9; Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 *Maryland Law Review* 335, 349-50; Weber (n 95) 67-68.

[149] Hence, privacy should be recognised as a potential competition parameter. See also Weber (n 95) 63.

[150] An example would be a machine for the production of steel in which sensors are embedded that guarantee that the steel maintains a constant temperature during the production process. Deviations from that temperature are an indicator for the mal-functioning of the machine and should therefore cause the supplier of the machine to intervene before the malfunction produces cost-intensive downtimes in the factory. At the same time the optimal temperature will be a trade secret for the operator of the factory. This example shows that data can have very different functions based on the specific interest of the person who is seeking access.

and that individuals do not value personal data protection anymore, but, quite on the contrary, to enhance data protection in the digital sector.

However, modern data protection should also take account of what firms as data controllers can possibly do to respect data protection rules. Hence, there needs to be a balance between protecting the privacy concerns of individuals, including those using connected devices, on the one hand, and the economic and technical possibilities to fulfil data protection requirements imposed on firms, on the other hand.[151]

Moreover, data protection rules can also enhance innovation. Similar to the case of environmental law, data protection rules can create incentives for computer scientists and developers to develop new technical means to control the use of data. For instance, there is an emerging debate on using blockchain technology as a tool for individuals to get back control over the use of their data in the digital economy.[152]

As regards data access and control from the perspective of consumers, it is clear that the focus should be put on access and not on data ownership. Beyond privacy concerns consumers already today benefit from data access rights that help unlock data in their economic interest. European law provides for a right of independent car repairers to get access to the on-board data of cars.[153] Similarly, the Payment Services Directive 2 (PSD2) for a right of payment services providers to get access to the bank account of their costumers and thereby enables these providers of new and innovative digital payment systems to enter the market against the resistance of the banks.[154]

In addition, Article 20 GDPR now also provides for a general right to data portability as regards personal data, which is not just a right to strengthen the data subject's autonomy, but has been conceived from the very beginning as a tool to 'support the free flow of personal data in the EU and foster competition between controllers'.[155] However, this right is limited to personal data. The more consumers use connected devices, the more they will also need to connect devices of different suppliers, for instance in their households, whether the data shared among those devices is personal or non-personal data.

In contrast, consumers will not have a primary interest in 'owning' the data connected devices produce for the purpose of generating additional income from authorising the use of data in secondary markets. Consumers who nowadays choose between acquiring a traditional and a new 'connected' car will make this choice based on two principle considerations: respect of their privacy concerns, on the one hand, and safety of the driving, on the other. Both considerations are

[151] In fact, also the GDPR, recital 4, points out that the right to data protection is not an absolute right and that it is in need of being balanced with other fundamental rights and has to respect the principle of proportionality.

[152] Shraddha Kulhari, *Building-Blocks of a Data Protection Revolution* (Baden-Baden: Nomos 2018). The reverse discussion relates to the question whether other blockchain applications are compliant with the GDPR. For a rather positive view see Christopher Kuner, Fred Cate, Orla Lynskey, Christopher Millard, Nora Ni Loideain and Dan Svantesson, 'Blockchain versus data protection' (2018) 8 *International Data Privacy Law* 103.

[153] See Arts 6 and 7 Regulation (EC) No. 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and 6) and on access to vehicle repair and maintenance information, [2007] OJ L171/1, as well as Art 13 Regulation (EC) No 692/2008 of the European Parliament and of the Council of 18 July 2008 implementing and amending Regulation No 715/2007, [2008] OJ L199/1.

[154] See Art 36 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment service in the internal market, amending Directive 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L337/35.

[155] Article 29 Data Protection Working Party, Guidelines on the Right to data portability (13 December 2016; revised 5 April 2017) 3. On the objectives of Art 20 GDPR see also Paul De Hert, Vagelis Papakonstatinou, Gianclaudio Malgierei, Laurent Beslay and Ignacio Sanchez, 'The right to data portability in the GDPR: Towards user-centric interoperability of digital services' (2018)34 *Computer Law and Security Review* 193, 194-96; Ruth Janal, 'Data Portability—A Tale of Two Concepts' (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce* 59, para 4.

intrinsically intertwined. The collection of data, including personal data, is the very condition of automated and autonomous driving. Safety of driving in the new digital era depends on the use of data. This shows that data collected by a car should not be regarded as a mere counter-performance under the sales contract for a car. Rather, it is a condition for the service of enabling safe driving, which the car manufacturer will permanently provide to the consumer. Thus, the consumer has a vital interest in the manufacturer making best use of data to increase safety.

These key consumer interests need to be taken into account in the context of the discussion of new ownership rights in data. At first glance, it seems that participation in such income does not constitute a primary consumer interest, but still may be a welcome add-on for consumers. But it is also to be noted that the consumer will buy a connected car, directly or indirectly, from the manufacturer who controls the data as a data holder. If the legislature introduced a data ownership right of the purchaser of a connected car, the manufacturer could not only request this purchaser to transfer or license the data ownership rights. More importantly, the data ownership right would most likely fail to generate any additional income for the purchaser of the car since the manufacturer would immediately vector in the prospective payments made for the commercialisation of the data in the sales price for the car. Hence, the creation of ownership rights between two parties where the creation of the subject-matter of protection depends on a prior contract to be concluded between these parties, without further state intervention, cannot be expected to produce any additional income for the rightholder. The principle of freedom of contract will allocate the economic value of using the subject-matter exclusively according to the distribution of the bargaining power between the parties.[156]

d) Public interest grounds, and freedom of information in particular

The most important public interest ground that needs to be taken into account is freedom of information. This principle is directly opposed to the idea of creating ownerships rights in information. As explained further above[157], control over the use of data depends on a specific justification that, from a fundamental rights perspective, can explain the exception to the principle of freedom of information. In the case of data protection, this justification is to be found in the constitutional right to data protection as an emanation of the general right to privacy of the data subject. Data protection law even expresses the result of the legislature's balancing of the right to data protection with other fundamental rights, such as the freedom of expression and information in particular.[158] In the case of trade secrets protection, the justification relates to the pro-competitive effect of such protection. As compared to data protection, trade secrets are protected less strongly. Protection depends on the secrecy of the information and, hence, ends when the information becomes publicly known. In contrast, the idea of introducing data ownership rights, which would result in exclusive control by the data owner without any additional substantive

[156] This phenomenon is well known from copyright law. The standard example relates to translations. Depending on the jurisdiction, the translation will give rise to original copyright either of the translator—as under the Continental *droit d'auteur* tradition—or of the publisher as under the so-called work-made-for-hire doctrine of US law. Irrespective of who the original copyright owner is, the translator is expected to receive the same remuneration in both systems, namely, a market price for the service of providing the translation. This is so, because also under the continental European tradition, the translator depends on a mandate from the publisher and it will be the publisher who typically takes the licence for the translation and its commercial exploitation from the holder of the copyright in the original work. In continental Europe, the contract between the publisher and the translator has to take account of the copyright situation. Typically, without further regulation, this can easily be implemented by declaring part of the overall market price paid to the translator a royalty payment for the use of the copyright. If the legislature wants to guarantee that the translator will get additional remuneration for the copyrighted work, additional price regulation—for instance, as part of copyright contract law guaranteeing fair remuneration—will be required.

[157] At 2.2. c) through e) above.

[158] As explicitly pointed out in Recital 4 GDPR.

requirement for protection and without the requirement of secrecy, would run the risk of violating the principle of freedom of information.

Freedom of information is also compliant with the interest in guaranteeing the functioning of markets and in promoting innovation. The economics of information is very different from the economics of tangible goods. Information is non-rival, and publicly available information is non-excludable. The more people are using such information the higher the social benefit. Ownership in information, such as under patent law, is only justified if otherwise markets would not produce such information. Since, however, there is no indication that there is general underproduction of raw data, there is no case for a general ownership right in such data. In addition, information often works as an incentive for innovation, such as in the case of transfer of technology. The more people know about new technology, the more likely it is that implementers will come up with follow-on innovation. Therefore, from an innovation policy perspective, free flow of innovation has to be considered a most important public interest in a knowledge and innovation-based society.

The need to recognise freedom of information and free flow of information as a key principle of the market economy also argues against the Commission's idea expressed in European Data Economy Communication of 2017 to take care of the interest in access to data in the framework of the exceptions and limitations of a data producer's right.[159] Such legislation would turn upside down the principle and the limitation. Property rights in information should not be made the default rule but should rather remain the exception to the principle of freedom of information, which is in need of a specific justification.

Although freedom of information can be regarded as a key principle of a policy guaranteeing the functioning of markets and enhancing innovation, this principle is not limited to these goals. Freedom of information has, just like privacy, major non-economic implications for society. Democracies have to rely on two principles to work: on the one hand, citizens have to know what others, including the state, knows about them to act as autonomous persons. On the other hand, free flow of information and free speech have to be guaranteed as the basis for democratic debate. Given the obvious tension between the two principles, a balancing is needed in the framework of designing the data protection rules.

Attribution of freedom of information to the fourth objective of public interests for the purpose on which this Study relies is indeed motivated by the fundamental importance of freedom of information for democracy. This helps justify additional regulation of the distribution of news and opinions through social platforms with political implications.[160] The fact that the algorithms of social platforms create efficient markets in terms of economic theory[161] and provide individual users with the kind of news and opinions they prefer[162], is hence not sufficient to argue against its regulation.

As explained before, multiple public interest grounds also create an interest of the state to get access to data held by private businesses. However, such access is limited by fundamental rights. Public security, including the fight against terrorism, finds its limits in the data protection rights of

[159] European Data Economy Communication 2017 (n 9) 13.

[160] On the need to regulate the distribution of news through social platforms see Josef Drexl, 'Economic Efficiency Versus Democracy—On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics (2016), available at: https://ssrn.com/abstact=2833165 (accessed 31 July 2018).

[161] This is the conclusion of authors who conceive social platforms in relation to its users as attention markets. See Evans (n 145). This literature does not take into account the negative effects of the distribution of news on democracy.

[162] The fact that an increasing number of citizens nowadays consume information about politics mainly through social media by only communicating with others who share their political views can hardly be termed as irrational behaviour from the perspective of the individual consumer. Therefore, the negative implications of distribution of news for democracy cannot easily be captured within the classical consumer protection framework. On this see also Josef Drexl, 'Bedrohung der Meinungsvielfalt durch Algorithmen—Wie weit reichen die Mittel der Medienregulierung?' (2017) *Zeitschrift für Urheber- und Medienrecht* 529, 533-35 (also discussing insights from social psychology).

the citizens. As regards non-personal or anonymised data of companies, to which the state seeks access, for instance, to protect the environment or public health, businesses can at least rely on their right to conduct a business[163] to claim respect for their trade secrets and to receive at least fair compensation. Therefore, to protect businesses against excessive claims of the state to get access to data, there is no need to recognise data ownership rights of private data holders.

3.3 On the fallacy of not taking account of all objectives

The regulatory theory developed above does not only have the function of proactively guiding the development of the legal framework for the data economy. It can also help identify errors or shortcomings in proposals submitted for relevant legislation. The following parts of the Study will often have to assess whether the proposals of other sources should be followed or not. In this regard, especially proposals on the introduction of data ownership rights often suffer from the fallacy of not taking account of all objectives explained above. In turn, this fallacy appears in two variations, namely, first, exclusive concentration on one objective, thereby not taking account of other, especially conflicting objectives, and, secondly, domination of one objective over others, thereby failing to adequately balance the different objectives.

Typical examples of the first case would be claims to 'digitise the civil code', who identify data as a valuable economic asset that needs to be owned by somebody. By quickly trying to extend the concept of ownership in tangible movable items to data they do not only risk overlooking the different economics of data as compared to tangible items, but also the particular interest in maintaining freedom of information. This fallacy can also be detected in the study mandated by the German Transport Ministry of August 2017, which recommends introducing a data producer's right of the user of connected devices without giving any regard to the public interest in safeguarding freedom of information.[164] Another example is the resistance of experts of data protection law to acknowledge that personal data is nowadays also used for economic purposes. Conversely, the most modern economics literature on social platforms argues that the markets in which social platforms operate can be conceived as efficient attention markets as regards the users.[165] Yet this literature fails to distinguish that the welfare effects in terms of economic efficiency and further political implications may well differ considerably depending on whether social platforms, using the identical algorithm and the same rational of profit maximisation, distribute commercial or political information.

Conscious domination of one objective over the other, without engaging in the necessary balancing, can be observed with regard to claims that personal data protection has to result in the recognition of a data ownership right of the data subject.[166] The respective literature does not necessarily ignore the potential economic costs and impediments additional exclusivity rights may cause for the well-functioning of data markets. But the market and economics-based analysis is put aside by mostly relying on justice considerations. Thereby such literature ignores that, from a constitutional rights and public interest perspective, the fundamental right to data protection, which necessarily needs to be balanced with the public interest in free flow of information, cannot be used to argue ownership rights falling within the scope of protection of a very different fundamental right. Another example concerns claims according to which data protection should be

[163] Art 18 Charter of Fundamental Rights.

[164] Bundesministerium für Verkehr und digitale Infrastruktur (n 27). This study claims to also take an economic perspective, but no economist or economics research centre was included in preparing the study. More importantly, the fundamental rights perspective, including the particular right of freedom to information was ignored despite participation of the Lorenz von Stein Institute for Public Law at the University of Kiel.

[165] See Evans (n 145).

[166] See further discussion at 4.1 c) below.

put aside since such data protection would hamper the competitiveness of the EU, especially as compared to the United States and China, and harm innovation. Such 'economic' absolutism is not even convincing from an economic standpoint, since strong data protection rights will also create incentives for developing technological tools for data protection as a form of innovation building on the computer sciences; and it is not at all clear which jurisdiction and society will prosper more at a long-run, those that value data protection highly or those that tend to ignore it.

4 The existing and evolving legal framework of the EU for the data economy

In the following, the Study will analyse the existing legal rules relevant for the data economy. An earlier study mandated by the European Commission has already analysed very broadly the EU acquis and the legal situation in some national jurisdictions, namely, England and Wales, France, Germany and Spain, affecting access to and ownership of data.[167] This study looked at several issues, including exiting ownership rights in data, the role of competition law, what aspects are not covered and whether contractual arrangements provide an efficient legal framework. As regards ownership, the study observed considerable legal uncertainty, but also noted that neither EU law nor national laws provide a comprehensive ownership regime for data and that freedom of contract basically governs the use and licensing of data.[168] Legal uncertainty specifically arises from the fact that there are many laws that are relevant for the data economy.[169] None of these laws specifically regulates machine-generated data. In addition, many sector-specific laws oblige data-holders to disclose information.

In the following, this Study will not replicate such previous studies. Rather, it will focus on some core issues that deserve particular attention from the consumer perspective and with regard to connected devices. The Study will first concentrate on the relevance of the GDPR (at 4.1 below), the Database Directive (at 4.2 below), legislation on other intellectual property rights (at 4.3 below) and the Trade Secretes Directive (at 4.4 below). Finally, it will identify the rights of consumers concerning data generated by devices that a consumer is using (at 4.5 below). In doing so, this Part 4 of the Study provides answers to Questions (1) and (2) in the introduction (at 1 above). Beyond analysing the existing legal regime, this part will also take into account on-going discussions on reforming the law, especially with respect to the Database Directive and European contract law.

4.1 The General Data Protection Directive (GDPR)

The objective of the GDPR is to give natural persons 'control of their own personal data'.[170] Although data protection is inspired by the privacy interests of the data subject, the right to data protection as a 'control right' resembles property rights, which are in a similar way designed to give the owner 'control' over the use of the subject-matter of protection. In the following, against the backdrop of the GDPR, the right to data protection will be analysed in three regards: first, the analysis will identify the subject-matter of data protection and seek to answer the question of whether data protection

[167] Osborne Clarke LLP, Legal study on Ownership and Access to Data (n 41).

[168] Ibid, 7.

[169] Here, the study mentions rules on trade secrets protection, intellectual property rights, data protection and consumer contract law. Ibid, 8.

[170] Recital 7 GDPR.

can be perceived as property in data (at a) below). Secondly, the concrete control rights of the data subject will be identified and compared with those that property rights usually attribute to the owner (at b) below). Finally, in a more prospective way, the question will be asked whether data protection rights should be extended to data ownership rights (at c) below).

The following analysis—as well as other parts of this Study concerning personal data protection—do not take specific account of the Proposal for a new ePrivacy Regulation,[171] although this Proposal is strongly influenced by the advent of new business models of the digital economy. The proposed ePrivacy Regulation aims to 'particularise and complement' those of the GDPR by laying down specific rules for electronic communications services.[172] Yet the fundamental concepts and scope of application of the ePrivacy Regulation differ in several regards from the ones of the GDPR. Since the ePrivacy Regulation is not supposed to protect personal data interests as such, but more specifically the confidentiality of electronic communication, the scope of application also extends to non-personal data and data related to legal persons.[173] In addition, the ePrivacy Regulation would extend application of European ePrivacy rules to functionally equivalent electronic communication services[174] which are substitutable to traditional services, but so far do not have to comply with the same rules.[175] These so-called 'Over-The-Top' communications services (OTTs) include Voice-over-IP, instant messaging and web-based e-mail services.[176] Since the concept of connected devices as used in this Study also covers smartphones, tablets and PCs that are used for communication of 'electronic communications contents', including text, voice, videos, images, and sound, through such OTTs, the ePrivacy Regulation would in principle also have relevance for the Study. To the extent that personal data falls within the scope of application of the ePrivacy Regulation, the latter would constitute *lex specialis* in relation to the GDPR.[177] Still, to the extent that the ePrivacy Reguation does not depart from the GDPR, the latter is and remains part of the European ePrivacy regime. As will be seen further below, the most important substantive data protection rule for the analysis in this Study will be Article 20 GDPR on the data portability right. On this right, the proposed ePrivcy Regulation does not contain any specific rules. Hence, Article 20 GDPR is also applicable with regard to OTT communications service providers. This justifies concentrating the following analysis on the rules of the GDPR.

a) The object of data protection as a basis for data ownership

Article 4(1) GDPR defines 'personal data' as 'information relating to an identified or identifiable natural person'. For the purpose of answering whether 'personal data' as the object of protection can be considered subject-matter of a property right under the GDPR, the term 'information' in this definition is most important. This term shows that data protection relates only to the semantic level

[171] Proposal of the Commission of 10 January 2017 for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final. On this Proposal, see, among others, Giovanni Buttarelli, 'The Commission Proposal for a Regulation on ePrivacy: Why Do We Need a Regulation to ePrivacy in the European Union?' (2017) 3 European Data Protection Law Review 155.

[172] Recital 5 and Art 1(3) Proposed Regulation.

[173] Commission Proposal (n 171), Explanatory Memorandum, at 3.1. See also Butarelli (n 171) 156.

[174] Ibid, Explanatory Memorandum, at 3.4.

[175] Recital 6 Proposed Regulation.

[176] Commission Proposal (n 171), Explanatory Memorandum, at 1.1. For instance, the ePrivacy Regulation would also cover the services of Gmail, Skype, Facebook Messenger and WhatsApp.

[177] Butarelli (n 171) 157. Those rules are especially important with regard to the electronic communications metadata as a particular kind of personal data. See Art 6(2) Proposed Regulation. Such data includes machine-generated data, such as the websites visited, geographical location, the time, date and duration when an individual made a call. See Recital 2 Proposed Regulation.

of data, where data conveys meaning.[178] This means that the underlying raw data, as the bits and bytes in which personal data—or better 'information'—has been encoded, is not affected by personal data protection rules.

To further explain this distinction, reference can be made to the *UsedSoft* judgment where the CJEU has recognised ownership in a concrete dataset.[179] In this judgment, the CJEU had to decide whether digital exhaustion of the copyright concerning a computer program should be recognised with the result that copies of the computer program could be freely resold to third parties where the computer program was not acquired on a physical carrier, but in form of the possibility to download the program from the Internet. In this regard, the CJEU had to interpret Article 4 of the Computer Programs Directive[180], which vests an exclusive distribution right in the copyright holder[181], but simultaneously provides for the exhaustion of the right with the first sale in the EU of a copy of a program by the rightholder or with her consent.[182] In the underlying case, the copyright holder Oracle argued against exhaustion, *inter alia*, claiming that it only licensed the use of the computer program without selling anything.[183] The CJEU decided otherwise by holding that a first sale in the sense of the directive would require the transfer of property in a copy of the program and that allowing the download of a digital copy under a permanent licence would amount to the transfer of property in the digital copy.[184]

In this judgment, the CJEU has recognised ownership in data in a very specific and limited situation. This Court has not established a general ownership right in data.[185] Rather, the Court only used the property concept to justify a 'first sale' and, thereby, restricted the exclusivity of the copyright with the objective of promoting access to the copyrighted work.[186]

As regards the role of this judgment for the GDPR, it is to be noted that the CJEU distinguished two entitlements, namely, the entitlement in the copyrighted computer program as the intangible subject-matter that is encoded in form of digital data and ownership in the digital copy of the program. Transferred to the case of data protection, 'personal data' as digitally encoded information can equally be distinguished from the digital dataset in which the information is encoded. Nothing in the GDPR can be interpreted in the sense that the data subject's rights regarding her personal data would encompass a property right in the digital dataset from which the personal information can be extracted. Similar to the case of a copyright in a computer program, personal data protection does not amount to a property right in the underlying raw data in which the information is encoded.

Hence, the only question to be asked is whether the data protection rules of the GDPR convey a data ownership right on the semantic level of information. In this regard, it has to be noted upfront that the GDPR does not frame the relationship of the data subject in relation to her personal data in the style of property legislation. Property legislation typically identifies the subject-matter of protection—ie, of what is owned—and then fixes the scope of exclusivity with regard to the use of the subject-matter. In contrast, Article 1(1) GDPR describes data protection as a form of 'protection

[178] See also Zech (n 44) 140.

[179] Case C-128/11 *UsedSoft* ECLI:EU:C:2012:407.

[180] Computer Programs Directive 2009/24/EC (n 57).

[181] Art 4(1)(c) Computer Programs Directive.

[182] Art 4(2) Computer Programs Directive.

[183] *UsedSoft* (n 179) para 43.

[184] Ibid, paras 42-46.

[185] See, however, Alberto De Franceschi and Michael Lehmann, 'Data as a Tradable Commodity and New Measures for their Protection' (2015) *Italian LJ* 51, 60-63 (cautiously supporting a 'data usage right').

[186] See also Drexl (n 51) para 68.

of natural persons' and announces to establish rules on the processing of personal data. The Regulation thereby implements the fundamental right to data protection of Article 8 EU Charter of Fundamental Rights, which, in turn, is an emanation of the right to respect for private live in Article 7 of the Charter.[187] Accordingly, the Recitals of the GDPR refer to Articles 8(1) of the Charter and not to the property provision of Article 17.[188] Hence, the scope of protection of the GDPR is limited to protecting the privacy and autonomy of natural persons. Rights enabling the natural person to control the use of personal data are not an expression of owning this kind of information. These rights are only means to empower the data subject to take care of her privacy interests.

b) Comparing the control rights of the data subject with property

Still the GDPR vests specific rights to control personal data as information in the data subject, whereby it is for the data subject to decide whether others may use her personal data. Although data protection has a different foundation in the system of fundamental rights, the question can still be asked whether these control rights do not equal exclusive property rights.

To make the processing of personal data legal, the data processor is in principle in need of consent given by the data subject[189], unless specified rules allow for the processing of the data without consent[190]. The need to give consent provides the basis of the control rights of the data subject. These rights are especially strengthened by the right to withdraw consent at any time and, consequently, to obtain erasure of the personal data.[191] These latter rights the data subject go even further than the rights of the owner of an intellectual property right who has granted a permanent licence to use the right. The data subject is in no way bound by previously given consent.

Yet this does not mean that the right to give and withdraw consent make these rights an expression of a property right. They continue to protect the data subject as a natural person, and thereby establish a very high level of protection of personal autonomy. Nothing in the law says that personal autonomy rights cannot be stronger than property rights and that, if the level of control of property rights is reached, the underlying right changes its character and turns into a property right. Quite the contrary, it has to be argued that the right to withdraw consent at any time even argues against qualifying the right to data protection a property right, since the possibility to withdraw consent at any time excludes the necessary feature of any property right to provide third parties with the possibility of unrestricted use of that subject-matter of protection at least in the framework of a stable and enforceable licensing agreement.[192]

Because of its economic dimension, the right to data portability pursuant to Article 20 GDPR could appear as a much better candidate for a property right. This right shows that there is no absolute watershed between data protection as a right that protects the natural person, on the one hand, and economic rights, on the other. The right to data portability can namely be recognised as an economic right, which enables the data subject to overcome data lock-in by transferring the

[187] In the *Google Spain* case, the CJEU relied on both Arts 7 and 8 of the Charter to develop a right to be forgotten. See C-131/12 *Google Spain* ECLI:EU:C:2014:317, para 97

[188] Recital 1 GDPR.

[189] Arts 6(1)(a) and 9(2)(a) GDPR.

[190] As specified by Art 6(1)(b)-(f) GDPR.

[191] Art 17(1)(b) GDPR.

[192] See Luisa Specht, 'Das Verhältnis möglicher Datenrechte zum Datenschutzrecht' (2017) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 1040, 1043. With a similar conclusion Berger (n 24) 354.

personal data held by the data controller to the data subject or to other data controllers.[193] In Recital 68, with respect to the data portability right, the GDPR is even including ownership-style wording by referring to the data subject's 'his or her own data'.[194] Yet, despite its economic function, the data portability right does not go beyond a data access right regarding personal data. The data portability right does not depend on general recognition as a property right.

Yet the strongest argument against the qualification of the data protection rules under the GDPR as data ownership rights is that it does not frame data protection as an 'exclusive right' that would equal a right *in rem*. The EU legislature even explicitly states that the right to data protection is 'not an absolute right'.[195] Rather, the rights of the GDPR emerge from a balancing of various fundamental rights, whereby especially the freedom of expression and information of others is taken into account.[196] The GDPR thereby recognises the data subject as a social being, who should not be in complete control of all communication about herself.[197] This translates into particular limitations of the data protection rights. While the GDPR defines 'processing' very broadly in Article 4(2) GDPR, also covering the 'disclosure by transmission, dissemination or otherwise making available' of data, Article 2(1) GDPR only protects against the 'processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system'. More importantly, processing by a natural person in the course of purely personal or household activity is explicitly excluded from the scope of protection.[198] This shows that the GDPR only protects the data subject against certain forms of use in terms of data processing that appear as particularly dangerous to her personal autonomy. Data protection therefore only imposes restrictions on third persons on 'how' they treat personal data, without vesting a general exclusive right in the data subject against third persons to control the use the personal information.

The question remains whether use of personal data for economic purposes by the data subjects should lead to the recognition of an economic ownership right in personal data. Indeed, many operators of Internet platform, such as social platforms and search engines, provide services without claiming monetary consideration and finance their services through the commercialisation of personal data. The Commission's Proposal for a Digital Content Directive seems to confirm the economic role of personal data in the data economy by accepting that, personal data is often used just as a counter-performance for a service provided Internet platform operators.[199] Yet in this Proposal the concept of personal data as a counter-performance is only used to define the scope of

[193] This has already been part of the policy objective when the private Data Portability Projectstarted to advocate unrestricted data portability. On this project, see its website at: http://dataportability.org (accessed 31 July 2018). On the history of the data portability movement, see Van der Auwermeulen (n 114) 58-59.

[194] In contrast, in line with other provisions of the Regulation, Art 20(1) GDPR uses the term of 'personal data concerning him or her'. Nevertheless, De Hert et al (n 155) 201 take this as a sign of 'a first step to an idea of data subjects' default ownership of their personal data.

[195] Recital 4, 2nd sentence, GDPR. See also Denga (n 94) 1372 (confirming that data protection does not provide unlimited control over the use of personal data); Kerber (n 2) 990 (stating that data protection rights do not constitute exclusive rights). In contrast, Benedikt Buchner, 'Is there a Right to One's Own Personal Data' (2017) 9 *Zeitschrift für Geistiges Eigentum* 416 seems to argue differently by supporting a 'right to one's own personal data'. Yet he does not explain how such a right could be justified in the light of the right provided for by the GDPR.

[196] Recital 4, 3rd sentence, GDPR. The fact that the data protection rules are the expression of a balancing of conflicting fundamental rights is also the key argument for Heymann (n 26) 656-57 against qualifying data protection rights as an expression of a property right. According to Heymann, the criteria applied for this balancing are linked to the social functions of personal data and not economic considerations.

[197] The relevance of personal information for social life as the criteria for the balancing of data protection rights are well expressed in the Google Spain judgment. See C-131/12 *Google Spain* ECLI:EU:C:2014:317, paras 74 and 92.

[198] Art 2(2)(c) and Recital 18 GDPR.

[199] See Recitals 13-14 Proposal for a Directive of the European Parliament an of the Council on certain aspects concerning contracts for the supply of digital content, COM(2015) 634 final.

application of the Directive to avoid gaps in the protection of consumers in the context of contract law.[200] The Proposal simple acknowledges that such business models exist and that consumers make economic use of their personal data. At best, the categorisation of granting access to personal data as a counter-performance can be seen as a legal confirmation of the legitimacy of such use by the data subject. But even this does not add anything to the legal situation already established under the GDPR. This Regulation fully respects the data subject's autonomous motivation for agreeing on the use of personal data. Therefore, economic use of personal data does not run counter to the privacy orientation of the GDPR. Hence, the fact that the GDPR allows for economic use of personal data does not require recognising personal data as an object of property either.

Hence, when the data subject signs a contract in which she expresses consent to the use of personal data, she is not transferring 'property' in personal data. The reason is that such consent based on an economic motivation does not transform data protection into a tradable asset. To call personal data the 'new currency of the digital economy' is flawed because giving consent does not make the other party the owner of this personal data that can be re-used as a means of payment or as an asset to be traded against money or other assets in follow-on markets. The rights of the GDPR, not least the right to withdraw consent, are opposed to such an understanding.

An additional argument against conceiving data protection under the GDPR as a property regime arises can be drawn from how the GDPR deals with data protection after the death of the data subject. The GDPR does not apply to deceased persons and leaves it to the Member States to provide for rules regarding the processing of personal data of deceased persons.[201] If data protection were conceived as property, there would not only be a need to clarify how and by whom the personal interests of a deceased person are protected, but also the need to specify whether personal data as the object of property forms part of the estate of a deceased person that is passed on to the heirs pursuant to the applicable law of inheritance. 'Digital inheritance' is an emerging legal issue that can strongly be influenced by whether a property right's dimension of data is recognised or not. Yet Member States still seem to be far away from recognising personal data as an object of property that can be passed on to the heirs.[202]

In sum, it can be concluded that neither the GDPR nor the potential economic use of personal data amounts to an ownership right in personal data.

[200] See Art 3(1) Proposal for a Digital Content Directive.

[201] Recital 27 GDPR.

[202] Yet, in Germany, the Federal Supreme Court has most decided that the parents of a teenage girl who was killed by a train can claim access to the girl's Facebook account. This case showed very tragic features since the parents were hoping to find out through the Facebook account whether their daughter committed suicide or not. The Upper District Court of Berlin (*Kammergericht Berlin*), as the competent court of appeals, rejected that claim based on the argument that the applicable ePrivacy rules would not allow for such a claim. See *Kammergericht Berlin* of 31 May 2017, Case 21 U 9&16, available at: https://openjur.de/u/873426.html (accessed 30 April 2018). In contrast, the Supreme Court argued that the heirs indeed have a right to claim access to the Facebook account. However, the Court did not reach this result by concluding that the personal data contained in the account forms part of the estate of the deceased person. Rather, the Court limited its holding to the succession of the heirs in the deceased person's position as a party to the contract with Facebook. The fact that the Facebook account contains personal data of the deceased person was held irrelevant. Rather, the Court equalled the Facebook account with a diary which would also be part of the estate of the deceased person. The mere fact that an item or a contractual position, such as a diary or a social platform account, provides access to personal content, according to the Court, does not exclude it as part of the estate that is passed on to the heirs. See *Bundesgerichtshof* (Federal Supreme Court) of 12 July 2018, Case III 183/17, available at: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&sid=9a23fbfa57ca883020da84a3d318c696&nr=86032&pos=2&anz=4 (accessed 31 July 2018). This case shows that recognition of ownership in data is not necessarily needed to achieve appropriate results. In the same vein, Weber and Thouvenin (n 44) 57.

c) Recognition of an additional intellectual property regime for personal data?

Since under the current legal regime of the GDPR natural persons do not hold any property right in personal data, the question remains whether the legislature should change this situation and recognise such property right for the data subject. The point of departure however remains that, from a legal point of view, ownership in data is different from data protection. As Janeček puts it, ownership in data must relate to personal data as the object of a property right, while personal data in the current framework is only an intermediary tool for protecting personality rights.[203]

Hence, transforming data protection into a data ownership right would actually require recognising a separate pillar of legal protection in form of a property right's system. Even authors who argue in favour of an economic rights of exploitation in personal data, almost intuitively, seem to acknowledge this difference.[204]

The more important questions to be answered are however the following: Is there a justification for the introduction of a separate property right system for personal data, and can such system be coordinated with the existing data protection regime of the GDPR? Both questions have to be answered in the negative.

As regards the *first* question, concerning the justification for the introduction of a property rights system for personal data, there is a temptation to conclude from the mere existence of data protection that the law also has to recognise economic rights of the data subject in personal data.

In this vein, Wandtke argues in favour of an economic prong of data protection in the light of the commercialisation of personal data in the modern data economy.[205] However, he merely relies on ethical arguments, including human dignity. Based on this, he concludes that personal data 'belongs' to the data subject.[206] Yet such reasoning overlooks that the protection required by the fundamental right to data protection under Article 8 EU Charter of Fundamental Rights has conclusively been spelled out by the EU legislature in the framework of the GDPR. Therefore, it is not possible to derive from this fundamental right the need to recognise a property right in personal data that would allocate the economic gains from the use of personal data to the data subject.[207] It could even be argued that introduction of such a right on the national level would violate EU law.[208]

Fezer, who is the strongest academic advocate of a data ownership right in Germany, is strangely ambivalent as regards the justification of such a right. He seems to take personal data protection at least as the point of departure of a data ownership right by justifying ownership with the commercialisation of informational data generated by natural persons, referring to the protection of privacy and the right of informational self-determination.[209] But, on the other hand, he also advocates to go beyond personal data to include all behaviour-generated data as a subject-matter

---

[203] Václav Janeček, 'Ownership of personal data in the Internet of Things' *Computer Law & Security Review* (forthcoming) 11, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3111047 (accessed 31 July 2018).

[204] For instance, Wandtke seems to admit that current data protection rules cannot be perceived as ownership. Rather, he argues that a bundle of economic rights should be recognised by the legislature. Artur-Axel Wandtke, 'Diskussion des „Warencharakters" von Daten aus persönlichkeits- und urheberrechtlicher Sicht' (2017) *Multi-Media Recht* 6, 11.

[205] Ibid, 9.

[206] Ibid („Die persönlichen Daten gehören jedem Einzelnen".).

[207] In the same vein, Denga (n 94) 1375.

[208] The GDPR pursues the establishment of a 'strong and more coherent data protection framework' in the European Union. See Recital 7 GDPR. Member States are therefore only allowed to legislate on data protection within the scope of the GDPR where this Regulation provides for 'specifications or restrictions of its rules by Member States' and only 'as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply'. See Recital 8 GDPR.

[209] Fezer (n 4) 359.

of data ownership. Accordingly, he wants to vest a data ownership right in the user of a connected device as the data producer as regards all data generated through the use of the device.[210] He explicitly conceives personal data as only one segment of the data protected by this data ownership right and clearly distinguishes between personal data covered by the data protection rules and behaviour-generated data as the subject-matter of the new intellectual property right. To bridge the obvious justification gap, he seems to rely on the property clause of the German constitution.[211] However, this argument cannot answer why the property right should automatically be vested in the user of the device and not in another person.

In sum, this shows that data protection as such and the underlying fundamental right to data protection cannot justify a data ownership right of the data subject or the user of a connected device. Rather, the questions of whether such a new ownership right should be recognised in the first place and, if so, who should own machine-generated data have to be answered against the backdrop of the regulatory theory developed in Part 3 of this Study.[212]

As regards the *second* question of whether an intellectual property regime for personal data can be coordinated with the existing system of personal data protection, it is to be noted that such a legal regime would not fulfil the fundamental requirements for such a regime. This conclusion can be drawn by reliance on a recent analysis conducted by Specht. She advances three arguments three arguments against data ownership:[213] first, the difficulties to clearly distinguish between personal and non-personal data argues against taking the personal character of data as a criterion for the definition of the subject-matter of the property right. Such criterion would not allow attribution of rights in specific information to individual rightholders with sufficient legal certainty. Secondly, such a property system would not be able to achieve its goal to guarantee participation of the data subject in all the income that is generated in secondary markets. The reason is mostly one of feasibility and administrability. Since exploitation will often relate to aggregated data and data that has gone through several stages of processing, it will hardly be possible to identify and distinguish between the property rights of oftentimes an extremely high number of rightholders and allocate the income appropriately among them. Thirdly, data protection rules, which allow the data subject to withdraw consent at any time would not allow to provide sufficient stability for licensing agreements that guarantee the licensee to be able to use the data on a permanent basis.[214] If, on the contrary, a transferrable ownership right in personal data were created, such right could be relied upon by the rightholder to whom the right is transferred against the data subject and, thereby, undermine the very objective of data protection rules to protect the privacy concerns of the data subject.[215] It is this third argument that shows that a separate pillar of economic rights in personal data for the data subject cannot be established without the risk of curtailing existing data protection rules.

[210] Ibid, 357.

[211] Ibid, 359.

[212] This analysis will be undertaken at 5.1 below.

[213] Specht (n 192) 1040. Prior to the adoption of the GDPR, Zech (n 44) 141 distinguished data protection from data ownership based on the argument that the data protection rights cannot be transferred to the data controller. With the same argument see also Dorner (n 26) 624-25 (still on EU data protection law before the GDPR became applicable).

[214] These arguments will be further explored at 5.1 below when analysing the potential benefits of a data producer's right.

[215] This conflict of the recognition of data ownership with the objectives of personal data protection is clearly stated by Weber and Thouvenin (n 44) 56.

d) Conclusion

In sum, the analysis produces several insights that are important for the following analysis: first, the existing rules of data protection under the GDPR cannot be considered an already existing ownership regime concerning personal data. Secondly, data ownership in personal data would need to be devised as a separate pillar of legal protection in parallel to the GDPR. Thirdly, the fundamental right to personal data protection is not sufficient to justify adoption of an ownership right of the data subject in personal data. Fourthly, such an ownership right would run the risk of colliding with the right of the data subject under the GDPR to withdraw consent to the data processing. Fifthly, a new regime of ownership in personal data cannot live up to the requirements of a workable intellectual property rights system. Whether this latter insight also argues against a data ownership right in machine generated-raw data in general will be further explored in Part 5.1 below.

4.2 Sui generis database protection

The most obvious candidate for already existing data ownership rights is the sui generis database right under the Database Directive of 1996.[216] When the debate on data ownership started, authors have however quickly expressed doubts as to whether machine-generated data would fall under the sui generis protection regime of the Database Directive.[217]

a) The current position of the Commission on reforming the system

The question of whether the Database Directive adequately responds to the requirements of the modern data economy was considered in the framework of the Commission's recent evaluation of the Directive.[218] The results of this evaluation seem to answer this question in the negative, but still the Commission's conclusions on how to proceed remain ambivalent. The Commission implicitly confirms legal uncertainties by stating that 'the sui generis right does not *systematically* cover big data situations and single-source databases'.[219] Yet, rather than announcing a proposal for legislation to clarify the situation, the Commission prefers to wait and see how practice and especially the case-law of the CJEU will develop. The Commission only intents to closely track 'whether the sui generis right might in fact apply more broadly than what is generally assumed'.[220]

The accompanying Commission Staff Working Document provides further reasons but appears even more ambivalent. There, it is assumed that, in the light of the case-law of the CJEU, the sui generis right will not apply where data are the 'by-products of the main activity of an organisation'; hence, the sui generis right will not 'broadly' apply to the data economy.[221] The Document

[216] Arts 7-11 Database Directive 96/6/EC (n 20).

[217] In this sense already Drexl (n 51) paras 43-50; see also the comprehensive analysis by Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' in: Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos 2018) 27-57. For another analysis of the application of the sui generis right to the protection of raw data, see Kirsten J Schmidt and Herbert Zech, 'Datenbankherstellerschutz für Rohdaten—Wie Big Data-Anwendungen die Tatbestandsvoraussetzungen der §§ 87a ff. UrhG erfüllen können' (2017) *Computer und Recht* 417 (concluding that the sui generis database right cannot be used as a substitute for data ownership, at 426). Some authors tend to consider database protection as inappropriate rather than non-available. See Kerber (n 2) 991 (based on the argument that the right only protects databases but not individual data); Wiebe (n 102) 879.

[218] See Database Directive Final Evaluation Report 2018 (n 21).

[219] European Data Space Communication (n 1) 9. (Emphasis added by the author.)

[220] Ibid.

[221] Database Directive Final Evaluation SWD (n 21) 2.

concludes that launching a process for reforming the sui generis right would be 'largely disproportionate ... at this stage'.[222] The Commission Staff also argues that any substantial reform would 'need to be substantial' and that there would be 'a need to build a stronger case that takes into account the policy debates around the data economy'.[223]

The latter point is confirmed in the assessment of the 2017 consultation of the working of the Database Directive. Participants in the consultation criticised the Directive as 'an outdated legal framework that is no longer in line with the last technological developments'.[224] The Final Evaluation Report, exploring whether the Directive is still fit for the data-driven economy[225], highlights how much the way of collecting and generating data has changed from manual data gathering to automated processes.[226] Connected devices play a major role in this regard. Already here it is worrying that the survey of the Commission has produced the result that data gathered through sensor-equipped technologies are often not publicly available.[227]

This may well mean that database protection related to connected devices could create considerable barriers to free flow of data. Such concerns are supported by Leistner, who puts the finger on the problem that the low threshold for acquiring a sui generis database right will often lead to protection of sensor and machine-generated data.[228] The Final Evaluation Reports notes this problem, and even cites Leistner[229] who, in light of such problems, recommends a reform of the Directive. In addition, the survey on which the evaluation builds notes large support of experts for facilitating access to data through introduction of a compulsory licensing system, based on the consideration that access especially to sole source databases gathering machine-generated data should require another incentive-access balance.[230]

Ultimately, as regards machine-generated data, the Final Evaluation Report considers two major problems of the Database Directive to be taken care of.[231] The first one is joint ownership, since, in a world where data is increasingly generated in network structures, it becomes more and more difficult to identify the database maker. The second problem is that, with respect to sensor-generated data, the Directive may often lead to sui generis database protection for sole source databases and thereby negatively affect competition. On both accounts the authors of the Final Report consider options for reform, including introduction of a compulsory licensing system to address the competition problem. But the Final Report stops short of claiming the need for immediate reform. On joint ownership, the Final Report only indicates ways on how to reform the Directive; and on the competition law problem, it only mentions introduction of a compulsory licensing system as a 'potential solution'. Especially with this last statement, the Final Report only seems to recommend continuously monitoring the development in the framework of the Commission's duty to present a report on the working of the Directive every three years pursuant to Article 16(3) of the Directive rather than taking immediate action.[232] Even more, in the concluding

[222] Ibid.

[223] Ibid.

[224] Database Directive Final Evaluation Report, Executive Summary (n 21) iv.

[225] Database Directive Final Evaluation Report (n 21) 25-44.

[226] Ibid, 26.

[227] Ibid.

[228] Leistner (n 217).

[229] Database Directive Final Evaluation Report (n 21) 29.

[230] Ibid, 40.

[231] Ibid, 43-44.

[232] Ibid, 44.

part of the Final Report, its authors support the Commission with their advice to wait as regards a reform of the Directive with respect to the Internet of Things and machine-generated data.[233]

b) Where to go from here?

Against the negative experience with the introduction of the sui generis right 20 years ago, which has created never-ending criticism and for which the Commission also now confirms that its positive impact is hardly discernible[234], reluctance to launch a broader reform of the sui generis right with the objective of making better use of it as a modern basis for the protection of data seems understandable, on the one hand. But, on the other hand, to accept continuing uncertainty about the legal situation and the risk of foreclosing access to machine-generated data could easily distort the development of the data economy. Based on the same assessment of the current situation and the case-law of the CJEU, it would also be possible to come up with exactly the opposite conclusion, namely, to either adopt the necessary changes to make the sui generis database right fit for the data economy or to abolish this regime in its current form.[235]

Before diving into the analysis of the uncertainties of the current sui generis regime, which arise from many of its elements, it is important to understand in which direction this system would have to develop to better serve the modern data economy. In principle, a decision is to be made upfront between two conflicting policy approaches, depending on whether the data economy is considered as being in need of more exclusivity or whether there is a need to enhance access. In the first case, the preferred policy approach would consist in broadening the application of the sui generis right in the direction of a general data ownership right. In the second case, the reform would be inspired by the objective to guarantee that the sui generis right will not create undue barriers to data access.

In line with the preceding parts of this Study[236], the latter approach appears appropriate.[237] In the absence of a market failure that could justify the adoption of a general data ownership regime, problems may arise where the sui generis database right in fact grants protection according to the Directive as interpreted by the CJEU. Another reason for taking this position as the starting point relates to general objective of this Study to discuss the future legal framework for connected goods from the perspective of the user (consumer). As will be seen in the following, it is much more likely that the sui generis right, if at all, will be vested in the manufacturer as the relevant 'database maker' rather than the users.[238] Hence, the sui generis right is more likely to aggravate the problem of access of the user of such devices than to promote it. This also indicates that the potential effect of the sui generis database right runs counter to the idea of the Commission in its European Data

[233] Ibid, 141.

[234] The Commission continues to state that, despite some individual benefits for rightholders, the sui generis right 'continues to have now proven impact on the overall production of databases in Europe, nor on the competitiveness of the EU database industry'. See Database Directive Final Evaluation SWD (n 21) 1.

[235] This is indeed the conclusion of the profound analysis of the suitability of the sui generis database right by Leistner for the modern data economy published in 2017. This analysis has spelled out many of the considerations contained in the recent 2018 Database Directive Final Evaluation Report (n 21). See Leistner (n 217) 57 ('If these changes are not considered and made, however, in the interest of an efficient legal framework for the European data economy, the sui generis right in its current form could and should not survive its next [meaning the one that the Commission has just conducted] evaluation.').

[236] See, in particular, at 2.3 above.

[237] This standpoint is shared by other authors. See Hugenholtz (n 52) 85-88 and 98-99 (claiming to repeal the sui generis right); Leistner (n 217).

[238] See also the analysis of Leistner (n 217) 38-42.

Economy Communication of 2017 to vest a 'data producer's right' in the purchaser or user of such devices to promote access of this person to data.[239]

In the following, several elements of the sui generis protection regime for databases will be addressed. For all these elements, three questions need to be considered: (1) What is the current legal regime? (2) What are the options for reform? (3) What option should be preferred?

c) The distinction between creating and obtaining data

The reason why it is often argued that the sui generis database right will not apply to machine-generated data relates to the distinction between creating and obtaining data as introduced by the CJEU in its case-law.[240] This is also the baseline of the assessment in the 2018 Database Directive Final Evaluation Report. There, the Executive Summary states:

> In the current context, it seems that the Database Directive does not apply to the databases generated with the means of machines, sensors and other new technologies (such as the Internet of Things or artificial intelligence). In fact, the generation of these databases is closely interlinked with the *creation* of their content (i.e. data). However, case law *indisputably excludes investments in data creation from the scope of the sui generis right*.[241]

This distinction between creation and collection of data relates to the question of what kinds of investments can and have to be taken into account to assess whether there is a 'substantial investment' in 'either obtaining, verification or presentation of the contents' in the sense of Article 7(1) Database Directive. Thus, excluding the investment in the creation of data makes it more difficult for database makers to claim a sui generis database right.

By excluding investment in the creation of data, the case-law considerably reduces the likelihood that a sui generis right will exist in so-called 'sole source' databases with monopolistic effects. Mere data producers will therefore often fail to meet the requirements for qualifying as database makers.[242]

The distinction goes back to the *British Horseracing*[243] and *Fixtures Marketing*[244] judgments, where the CJEU, on the same day, decided to limit the concept of protected databases. The underlying cases were very suitable for introducing such a limitation. In the *British Hoseracing* case, the referring court had to decide whether the organiser of betting for horse races violated a sui generis database right by extracting information from the database created by the British Horse Racing Board.[245] In this regard, the CJEU hat to decide whether the investment going into the organisation of the horse races would need to be considered for applying the substantiality test. The Court answered the question in the negative, arguing that the sui generis right only pursues to protect

[239] See European Data Economy Communication 2017 (n 9) 13. See also at 2.3 above.

[240] See, for instance, Dorner (n 26) 622; Wiebe (n 102) 879. This is considered a shortcoming by Becker (n 25) 254.

[241] 2018 Database Directive Final Evaluation Report, Executive Summary (n 21) ii.

[242] Schmidt and Zech (n 217) 421.

[243] Case C-203/02 *British Horseracing Board* [2004] ECR I-10415 = ECLI:EU:E:2004:695.

[244] Case C-46/02 *Fixtures Marketing v Oy Veikkaus* [2004] ECR I-10365 = ECLI:EU:C:2004:694; Case C-338/02 *Fixtures Marketing v Svenska Spel* [2004] ECR I-10497 = ECLI:EU:C:2004:696; Case C-444/02 *Fixtures Marketing v Organismos prognostikon* [2004] ECR I-10549 = ECLI:EC:C:2004:697.

[245] The *Fixtures Marketing* cases relating to a database made by the organisers of football league matches presented analogue facts and were therefore decided exactly the same way.

the investment made in the database as such.[246] Thereby, the CJEU relied on the arguments of the governments of several Member States, according to which

> [t]he purpose of the protection by the sui generis right provided for by the directive is to promote the establishment of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database.[247]

This shows that the CJEU clearly distinguishes the sui generis right, which was adopted by the legislature for creating incentives to create databases, from an ownership right in data as elements of such a database.[248]

The distinction between creating and obtaining data can easily be applied where the underlying data were created by a person or entity that is different from the database maker. In the *British Horseracing* case, however, the database maker, as part of its principle activity, namely, the organisation of horse races, was also the creator of the underlying data. In such a case, the sui generis right is not excluded as such[249], but the database maker will often fail to show that obtaining or the verification of the data involved significant investment since the verified data will anyhow be available after having created it.[250] Hence, for successfully claiming a sui generis right, the database maker must make substantial investment in the 'collection of [the self-created] data, their systematic or methodical arrangement in the database, the organisation of their individual accessibility and the verification of their accuracy throughout the operation of the database'.[251]

Based on these principles, the British Horseracing Board failed to claim a sui generis database right since it could not rely on the investment made for organising horse races nor the verification of the individual data that would enter the database.[252] The same happened to the maker of a database used for betting on football matches in the *Fixtures Marketing* cases.[253]

As regards data generated by connected devices, the distinction between creating and obtaining data seems to exclude the investment made in the development and technical design of the connected devices for assessing whether there was substantial investment. However, the line between creating and obtaining and verification of data may be very difficult to draw especially in the case of connected devices.[254] In *British Horse Racing*, the data that entered the database was 'self-created'[255] in the sense that the horse races were organised by the data maker, and the information included in the database would not have existed without the investment of the database maker.[256] Connected devices, however, often collect data through observation. Examples may be data collected by a radar observing the sky or a satellite observing the surface of the earth.[257]

---

[246] Ibid, para 30.

[247] Ibid, para 31.

[248] See also Hugenholtz (n 52) 86.

[249] Ibid, para 35.

[250] Ibid, para 36.

[251] Ibid.

[252] Ibid, paras 38-41.

[253] Fixtures Marketing judgments (n 244).

[254] See, in particular, Leistner (n 217) 28 (arguing that how to draw the line has remained contentious) and Hugenholtz (n 52) 86-87.

[255] See also Hugenholtz (n 52) 87 (using the term 'synthetic data'); Leistner (n 217) 28 (arguing that creation needs to be equated with 'making-up' data).

[256] The same can be said about the *Fixture Marketing* cases (n 244), decided by the CJEU on the same day, concerning a data about the football league matches.

[257] Examples given by Hugenholtz (n 52) 87.

Smart meters measuring the consumption of power, water or fuel and cars sharing data about the density of traffic and informing each other at real-time about available parking space gather the relevant data trough observation. How should data gained through observation be placed in the CJEU's distinction between creating and obtaining data?[258]

To give a reliable answer is difficult, since the CJEU still needs to decide that question. However, national courts have already dealt with the issue.[259] In the *Autobahnmaut* case, the German Federal Supreme Court held that the private company Toll Collect, which is mandated by the German State to collect toll from the operators of lorries for the use of motorways, holds a sui generis right in the dynamic database used for billing the individual operators.[260] In doing so, the court also took into account the investment made by Toll Collect in the terminals that register the lorries using the motorways. It thereby recognised the existence of the CJEU judgment in *British Horseracing*,[261] but distinguished the *Autobahnmaut* case from *British Horseracing* by stating that the data registered by the terminals and vehicles was not 'created' by Toll Collect. Rather, the data existed independently of the investment made by the database maker.[262] According to the *Autobahnmaut* judgment, many cases relating to machine-generated data would seem to be covered by the sui generis database right.[263]

From an economic perspective, however, this distinction made by the German Federal Supreme Court has to be criticised. The recognition of a sui generis right in the *Autobahnmaut* case clearly restricted access to information. While Toll Collect updated its database every day, it informed the operators of the lorries about the amount they have to pay only through monthly billing. Yet the lorry operators had an interest in permanently monitoring their costs of doing business. Such service was provided through the alleged infringer of the sui generis right, an Internet service provider, who had access to Toll Collect's database as a partner of a company which distributes payment cars that were originally issued for paying fuel at filling stations and, under a cooperation agreement with Toll Collect, were extended to be used also for paying the toll. In a case like this, where the protection of the database provides the rightholder with a data monopoly, it should not make any difference whether the data are self-created or only observed. In addition, Toll Collect was not in need of the database right as an incentive to create the database, since the company is remunerated by the Federal Republic of Germany for the service of collecting the toll. However, the Federal Supreme Court rejected this latter argument, which was indeed advanced by the defendant[264], stating that the sui generis right, to come into existence, only requires a substantial investment, and is not excluded by the fact that another person or entity pays the database maker for the services provided by using that database.[265] This argument is certainly convincing in the light of the legal provisions that apply, but it also shows how questionable the recognition of a database right is where it is not needed as an incentive to create the database.

Yet the CJEU still has to decide a case like *Autobahnmaut*. In the light of the judgment of the German Federal Supreme Court, however, it cannot be taken for granted that the CJEU would show more

[258] In favour of considering investment in data that are especially observed by meters, Schmidt and Zech (n 217) 421-22 (yet requiring that the data be accessible for everybody to avoid monopolistic protection of sole source databases).

[259] On broader references to German law see Leistner (n 217) 28-29.

[260] Federal Supreme Court (*Bundesgerichtshof*) of 25 March 2010, Case I ZR 47/08 *Autobahnmaut* [2010] *Gewerblicher Rechtsschutz und Urheberrecht* 1004, also available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=53335&pos=0&anz=1 (accessed 30 April 2018).

[261] Ibid, para 18.

[262] Ibid, para 19.

[263] In a similar vein Leistner (n 217) 29.

[264] Ibid, para 25.

[265] Ibid, para 26.

economic understanding. Following the reasoning in the *Autobahnmaut* judgment, the CJEU would produce a negative impact on the emergence of new data services to the prejudice of consumers. To remedy a CJEU judgment in line with *Autobahnmaut*, the legislative process on the EU level would simply take too long. Therefore, the Commission would be better advised to go ahead with reforming the sui generis right and to exclude investment in the collection of data through observation in general or at least under the condition that the database turns out as the only source for that information.

With respect to connected devices the assessment of whether investment in the collection and processing of data would have to be considered for assessing substantiality requires a technologically more detailed analysis. According to the analysis so far, investment in the collection of information about the density of traffic by the sensors of a car would have to be taken into account according to the *Autobahnmaut* judgment, while, where the sensors of a car monitor the functioning of the wheel, the relevant investment would probably be excluded as investment by the car manufacturer in the creation of data. However, the registration of a malfunctioning of the wheels does not suffice to conclude that there is ice on the road. If, for drawing such conclusion, the autopilot of the car relies on meteorological data delivered by a third information provider, such data will have to be considered as pre-existing data for which investment in obtaining it would have to be taken into account for assessing substantiality. Still, this is not the end of the story. The car manufacturer also makes an investment in the data analysis made by the autopilot of the car. In this regard, to distinguish between creating and obtaining information seems particularly difficult. On the one hand, the conclusion that there is ice on the street appears as information that exists without the data analysis undertaken by the autopilot. On the other hand, the conclusion drawn by the autopilot is only the result of an analysis that is based on empirical probabilities and, therefore, may in fact be more or less reliable. This seems to argue against taking into account any investment in data analysis as the basis of generating data that is then included in databases for assessing substantiality. However, also in this regard, it is not clear at all how the CJEU would decide such a case in the future.

From a user and economics perspective, to exclude investment both in creating and obtaining data for the substantiality assessment seems the appropriate advice to be given to the legislature. Where the user legitimately seeks access to data and is exposed to a data lock-in, recognition of a sui generis database right would, as illustrated by the German *Autobahnmaut* case, have the potential of creating additional barriers to access to data. From an economics perspective, it is to be noted that the manufacturer has already received a price, paid either directly or indirectly by the user, for the connected device, which can be used to cover the investment in obtaining and processing whatever data is needed for operating the device. Hence, there is no public goods problem in terms of insufficient incentives for investment that would require recognition of a sui generis database right. As regards the user, such right would only lead to a data monopoly and empower the manufacturer to exclude the user, directly or indirectly, from data excess or to charge a second price.

d) The concept of a database

However, recognition of a sui generis database right may already fail, because the data generated by connected devices do not fulfil the basic requirements of a database.[266] Article 1(2) of the Database Directive defines a database as a 'collection of independent works, data or other materials

[266] Recital 45 Database Directive explicitly states that 'the right to prevent unauthorized extraction and/or re-utilization does not in any way constitute an extension of copyright protection to mere facts or data'. See also Dorner (n 26) 622.

arranged in a systematic or methodical way and individually accessible by electronic or other means'.

In legal writing it is argued that this definition 'squarely rules out protection—whether by copyright or by database right—of (collections of) raw machine-generated data'.[267] The strongest argument in this regard seems to be that the data need to be arranged in a systematic or methodological way, which will typically not be the case where large amounts of data are collected by a connected device.

Yet the situation may considerably change when the data is further processed and changed for making it usable for other purposes. In this regard, the German *Autobahnmaut* case provides further insights.[268] There, the Federal Supreme Court argued that the data concerning the identification of the lorries using German motorways which was part of the data transmitted to its cooperation partner who operated the payment cards, indeed constituted a database in the sense of harmonised German law. The reason was that the data collected from by the stationary terminals and vehicles used by the database maker Toll Collect for registering the lorries were combined with additional data, such as the day and intensity of the use of the motorway as well as the number plates of the lorries and the payment card numbers of the lorry operators, to constitute a systematic or methodological arrangement.[269] This shows that sui generis database protection can very well enter the picture when machine-generated data is combined and arranged systematically with other data. In addition, even the entirety of the data directly collected by a connected device can fulfil the requirement of a systematic arrangement, such as in the case of automated metering.[270] Hence, existence of a database will largely depend on the individual circumstances of the case.

Another limiting factor is that a database only exists where its elements are 'independent materials'. This requirement is above all helpful to exclude overlaps with copyright law and neighbouring rights legislation.[271] For instance, a song, a movie or a videogame may be composed of many different elements, but the work as such has to be considered as a whole. Hence, if somebody takes a sequence of a melody of a song and uses it for another song, this may violate the copyright, but not any sui generis database right since the individual notes are not considered to be independent. This is important to exclude a second layer of protection created by another intellectual property right potentially owned by a different person that could distort the economic exploitation of the work by the copyright holder.

However, in the *Verlag Esterbauer* judgment, the CJEU gave the concept of 'independent materials' a rather generous interpretation according to which even an individual geographical information that can be taken from a map can be considered independent material, making a geographical map a database in the sense of the Directive.[272] In the underlying case, an Austrian publisher produced and distributed materials, such as maps for cyclists, mountain bikers and inline skaters, based on information extracted from analogue topographic maps produced by an agency of the Free State of Bavaria.

[267] Hugenholtz (n 52) 88.

[268] *Autobahnmaut* (n 260).

[269] Ibid, para 15.

[270] Schmidt and Zech (n 217) 418 and 420.

[271] See also Hugenholtz (n 52) 88.

[272] Case 490/14 *Freistaat Bayern v Verlag Esterbauer* ECLI:EU:C:2015:735.

The CJEU considered the maps of the Free State of Bavaria as databases in the sense of the Directive[273], based on the argument that every piece of geographical information that can be taken from the topographical map can be regarded as independent material.[274] The CJEU reached this conclusion in the light of two considerations: first, the CJEU held that any 'information utilised for financial gain and in an autonomous manner (...) constitutes "independent materials" from a "database" (...) since once extracted, that information provides the customer of the company using that information with relevant information'.[275] With this reasoning, the CJEU seems to conceive protection under the Directive as a means to prevent third parties from free-riding. Secondly, the CJEU argued that such 'information as independent materials' also exists where the informative value only arises from the combination of two pieces of information, namely, in the case of a map by the combination of the geographical location indicated by the two-dimensional grid of the map combined with the 'signature' symbolising, for instance, a church.[276]

As regards the case of machine-generated data, the *Verlag Esterbauer* judgment seems important in two regards. On the one hand, it defines the concept of 'independent material' or 'independent data' very broadly. Every single piece of information that has commercial value can suffice.[277] In a world of big data analytics, even in a case of a dataset that contains most divers and unknown data, any data can have economic value for somebody.[278] The challenge of big data analytics consists in finding out which valuable information can be taken from such a dataset. On the other hand, it suffices if the commercial value arises from the combination of two or more pieces of information. This also responds to how datasets are analysed nowadays. The challenge in this regard consists in being able to 'read' and 'understand' the data. Hence, based on this analysis, the judgment in *Verlag Esterbauer* seems to work almost as a template for bringing big datasets into the scope of protection of the sui generis database right. However, there is still a missing link. In the light of the judgment it is more likely than not that the CJEU would also require that, as in the case of the map, the way of how to read the combination of two elements of information which finally create economic value, be encoded by the database maker. This appears clear from the very logic of the arguments of the Court according to which the economic value of the data needs to be generated by the database maker. In sum, this seems to exclude information that can only be generated through data analytics from a dataset as 'independent materials'.

Another question regards the stability of the database. Digital devices are often designed and will be used for real-time applications, such as in the case of connected cars. In contrast, the requirement of a 'collection of data' seems to convey a stable concept of a database. However, as illustrated by the German *Autobahnmaut* case, the sui generis database right may also need to be recognised in the case of dynamic data applications. The defendant in that case was providing a daily update of the costs of using motorways to the lorry operators. The Federal Supreme Court obviously did not see any problem in the dynamic character of the data. Rather, it qualified the data that was transmitted to its cooperation partner every day as separate databases.[279]

In addition, the provisions of the Database Directive do not at all exclude dynamic datasets from protection, as long as they fulfil the requirements of Article 1(2). Nor can the opposite be concluded

[273] Note, however, that the CJEU was not requested to decide whether maps are databases protected by copyright, by a sui generis right or whether they are protected at all under the Directive. The requirement of the existence of a database is a uniform, yet not a sufficient requirement for both copyright and sui generis protection.

[274] Note that the CJEU was not asked to decide whether there was substantial investment in making the database.

[275] Ibid, para 28.

[276] Ibid, para 18-24.

[277] In the same vein, Schmidt and Zech (n 217) 419.

[278] This view seems to be shared by Schmidt and Zech, ibid.

[279] Ibid.

from the regulation of the term of protection of the sui generis right in Article 10 Database Directive. It is certainly true that the notion of 'completion of the making of the database' in Article 10(1) indicates some stability; but this notion is only needed to fix the starting point of the term of protection. The very concept according to which the database right can revive with every 'substantial change' of the database pursuant to Article 10(3) shows that dynamic databases are conceivable. Another indicator of the recognition of dynamic databases as a subject-matter of protection arises from the term of 'verification' used in Article 7(1) Database Directive. Verification of the data entering into a database is especially needed where circumstances on which the database seeks to inform will change over time. Hence, according to this provision, costs of continuously monitoring—and adjusting—the veracity of the data included in a database need to be taken into account for assessing the substantiality of the investment and especially for assessing whether changes made amount to a new database in the sense of Article 10(3) Database Directive.[280]

To conclude, this could well mean that the sui generis database right may also exist where the elements of the database are constantly changing in real-time. In this regard, the question may well be whether such cases are of any practical relevance, since real-time applications only matter at the given moment while the sui generis database right protects against later use of the database by third parties. Yet it has to be noted that connected devices which continuously collect data do not only collect and process data for real-time applications. Devices that register the use of streets by motor vehicles for charging a toll, smart meters or devices that collect environmental data are designed for the purpose of continuously measuring or counting for later use of the aggregated data. In addition, data are often multifunctional. Data collected by cars on the density of individual streets can be used as real-time data to regulate traffic at a given moment, but they can also be used as historical data for purposes of infrastructure planning. For use of such data, the exclusive character of sui generis database rights may well restrict access to the data for persons and entities that want to make use of them.

e) The degree of substantiality

The requirement of substantial investment in Article 7(1) Database Directive is not precisely defined as regards the degree of substantiality. The provision only specifies that substantiality has to be understood both qualitatively and quantitatively.

So far, the CJEU has not yet been required to clarify the substantiality standard. Yet national case-law and the legislature[281] favour a rather lenient approach. For reasons of legal certainty, even sceptics of the sui generis database right prefer application of a *de minimis* standard to a 'market failure approach', under which protection would only be recognised where the right is needed as an incentive for making the database.[282]

If the CJEU confirmed this *de minimis* approach, the Court would however undermine the positive effects of the *British Horseracing* and *Fictures Marketing* case-law, excluding investment in the creation of data from the substantiality assessment. In a case of self-created data, investment in the verification and presentation of the data could still suffice to lead to the recognition of a sui generis database right.

[280] This is explicitly confirmed by Recital 55 of the Database Directive.

[281] See Estelle Derclaye, 'Database Sui Generis Right: What Is a Substantial Investment? A Tentative Definition' (2005) 36 *IIC* 2, 20-21; Matthias Leistner, 'Legal Protection for the Database Maker—Initial Experience from a German Point of View' (2002) 33 *IIC* 439, 448-49; id, 'The protection of databases' in Estelle Derclaye (ed), *Research Handbook on the Future of EU Copyright* (Cheltenham, UK and Northampton, MA: Edward Elgar 2009) 429, 430; Schmidt and Zech (n 217) 423.

[282] In this sense Leistner (n 217) 30.

f) The database maker

For the purpose of this Study, the identification of the database maker as the owner of the sui generis database right is of utmost interest. Article 7(1) of the Database Directive has to be read in the sense that the person making the substantial investment in the database is considered the maker of the database and, hence, the holder of the sui generis database right. This is confirmed by Recital 41, which defines the database maker as 'the person who takes the initiative and the risk of investing'. In the practice of the modern data economy, this definition may however lead to a high degree of legal uncertainty because data will often be created and collected within larger networks, for instance, through data sharing platforms to which an indefinite number of players may contribute data.[283] In such circumstances, Article 7(1) may lead to joint ownership in the emerging databases.[284] Yet the Directive does not answer how to deal with joint ownership, and the Database Directive Final Evaluation Report only counts three Member States (Ireland, the UK and Poland) that have adopted specific rules on joint ownership when implementing the Directive.[285]

Yet, in the context of connected devices, the criterion of initiative will more likely lead to identifying the manufacturer as the maker of the database rather than the purchaser or user of a connected device.[286] This result, however, has to be criticised as a matter of policy for two reasons: first, the manufacturer will not be in need of the sui generis database right in order to control the data collected by the device, since the manufacturer is anyhow the *de facto* holder of the data and, thereby, able to commercialise the data. Secondly, to vest the database right in the manufacturer runs counter to the objective of the Commission in the 2017 European Data Economy Communication to conceive a data producer's right as a means to enhance access to data for the user of connected devices. In line with the latter, in its recent evaluation of the Directive, the Commission also concludes that ownership of the manufacturer in the database will increase the need for instruments to guarantee legitimate access of the user to the data.[287]

The effect of introducing a data producer's right for users of connected devices in addition to a potential sui generis database right of the manufacturer would be most harmful to the development of the data economy. The combination of two separate rights held by different persons would aggravate the blocking situation distorting access of third parties to the underlying data. None of the two rightholders could license the use of the data without consent of the other person. In addition, the data producer's right, even if it explicitly included a right of data access, would fail to achieve its goal, if the manufacturer could refuse access to the data based on a conflicting sui generis database right.[288]

---

[283] This problem is particularly noted in the recent evaluation of the Directive. See Database Directive Final Evaluation Report (n 21) 32.

[284] On the resulting problems and the ways to deal with them, see Leistner (n 217) 35-38.

[285] Database Directive Final Evaluation Report (n 21) 31.

[286] With the same conclusion, Leistner (n 217) 27. See also Database Directive Final Evaluation Report (n 21), 32 (concluding that the manufacturer will often be the database maker and not the operator of the machine of device).

[287] Database Directive Final Evaluation Report (n 21) 32, quoting Leistner (n 217) 37.

[288] It is to be noted that the standard for an abuse of market dominance in the case of a refusal to license an intellectual property right is higher than in the case of a simple refusal to deal case. According to the case-law of the European courts, the person seeking access has to show that the refusal prevents the emergence of a new product to the prejudice of consumers (so-called new product rule). See Case T-201/04 *Microsoft v Commission* [2007] ECR II-3601 = ECLI:EU:T:2007:289, para 334 (interpretation of the case-law of the CJEU by the General Court). See also at 2.3 c) above.

Therefore, the Commission would be better advised to reform the sui generis data protection regime in a way to guarantee that it will not additionally foreclose access to the data generated by such devices to the detriment of the users of such devices.

g) The scope of protection

Additional problems arise from the scope of protection of the sui generis database right. Article 7(1) Database Directive recognises a very broad right of the database maker 'to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database'. In Article 7(2), the two sub-rights to prevent extraction and to prevent re-utilization are defined more concretely.

From the perspective of the data economy, the most pertinent question is how to construct the requirement of the use of a 'substantial part of the contents of the database'. If this provision protected against any extraction or (re)utilization of data that is contained in a protected database, the sui generis database right would amount to a far-reaching right to control the use of information.

In the *Verlag Esterbauer* case[289], a judgment that solely concerned the concept of a database[290], the CJEU arguably also addressed the question of an extraction of information from a database in an indirect way. Since the sui generis right aims to provide protection against any commercially valuable use of information taken from a database, the Court considered any such piece of information that can be extracted as independent material in the sense of the definition of a database.

Yet it has to be doubted whether the CJEU would go so far to conclude that extraction of a single piece of information already suffices to infringe a sui generis right. The wording of Article 7(2)(a) and (b) Database Directive requires the extraction or (re)utilization of a 'substantial part of the contents of the database'. This was interpreted by the CJEU in the *British Horseracing* judgment in a rather narrow sense. According to the Court, Article 7(1) and (2) of the Directive only prohibits extraction 'which ... would lead to the reconstitution of the database as a whole or, at the very least, of a substantial part of it'.[291] In British Horseracing, the Court also defined the substantiality concept of the extraction or utilization of a 'substantial part' both in quantitative and qualitative terms.[292] The Court stated that there can be only an extraction or utilization of a quantitatively substantial part if the creation of the extracted or utilized part by itself required the employment of substantial resources.[293]

This should make sufficiently clear that the mere extraction of single pieces of information will fail to constitute use of a protected database. In particular, the holder of the sui generis database right will only be protected against other persons that extract substantial parts of the database according to the *British Horseracing* judgment and thereby are able to gain a competitive advantage by making use of extracted materials as part of their own databases. In fact, the latter was exactly the situation in the *Verlag Esterbauer* case.

Whether however this limitation sufficiently hedges in the exclusivity of the sui generis data base right in a big data context remains quite doubtful. Third persons who seek access to the information

[289] *Verlag Esterbauer* (n 272).

[290] See at d) above.

[291] *British Horseracing* (n 243) para 87.

[292] Ibid, paras 70-71.

[293] Ibid, para 70.

contained in a database with the objective of offering their own data-related services will typically want to have access to more than one piece of information[294] and, hence, will include all the information they need in their own databases.[295] In addition, it is argued that big data analysis will always lead to use of the database right, since such analysis requires a copying of the data, which is always to be considered a case of an extraction of a substantial part of the database.[296]

While the *British Horseracing* judgment has limited the scope of protection by requiring that the infringer include substantial parts of the contents of the protected database in its own database, the CJEU and national courts have interpreted the forms of use that fall within the exclusivity of the right under Article 7 Database Directive very broadly. In *Directmedia Publishing*[297], the CJEU held that 'extracting' in the sense of Article 7(2)(a) of the Directive does not even require a physical copying of the data. In particular, it is not required that the data disappear from the original medium.[298] Rather, based on the goal of the sui generis right to protect the database maker against any free-riding on the investments in the making of the database[299], the CJEU defined extraction extensively as 'any unauthorised act of appropriation of the whole or a part of the contents of a database'.[300] Thus, an infringement was even confirmed in the situation where the infringer only selected parts of the verses from the original list of verses to publish a separate, and hence very different, selection of poems. In *Innoweb*, the CJEU held that meta-search engines that allow for automatic gathering of information from other websites and search engines—in the concrete case a meta-search engine for searching the Internet for car ads—can constitute a (re)utilization of the parts of the contents of a database in the sense of Article 7(2)(b) of the Directive.[301] Following the line of the previous case-law, the Court defined the concept of '(re)utilization' very broadly as 'any unauthorised act of distribution to the public of the contents of a protected database or a substantial part of such contents'.[302] As in *Directmedia Publishing*, the 'nature and form of the process used' were not considered to be relevant.[303] In the light of this broad scope of protection, it has been argued that the limitation to 'substantial parts' of the contents of the database will not work as an effective means to safeguard competition and to prevent leveraging potentials of the sui generis right with regard to big data uses.[304]

Yet the most important right of the database maker in the digital economy is the one of making available to the public in Article 7(2)(b) of the Directive. In the *Autobahnmaut* case[305], the German Federal Supreme Court has given this right an extremely broad reading. In the underlying case, the lorry operators visiting the website of the defendant to acquire knowledge about their daily status of billing for the use of German motorways certainly constituted an indeterminate group of persons and, hence, a public in the sense of the right of making available to the public, on the on hand. But, on the other hand, the defendent only allowed the lorry operators limited access to the information concerning the lorries operated by them. Hence, no piece of information was made available to

[294] See also Leistner (n 217) 31 (arguing that third parties will typically be in need of access to complete data to produce sensible results).

[295] This was also the case in the abovementioned *Autobahnmaut* case (n 260).

[296] Schmidt and Zech (n 217) 424.

[297] Case C-304/07 *Directmedia Publishing* [2008] ECR I-7565 = ECLI:EU:C:2013:850.

[298] Ibid, paras 29-30.

[299] Ibid, para 33.

[300] Ibid, para 34.

[301] Case C-202/12 *Innoweb* ECLI:EU:C:2013:850.

[302] Ibid, para 37.

[303] Ibid.

[304] Leistner (n 217) 31.

[305] *Autobahnmaut* (n 260).

more than one operator. Still, based on a construction of harmonised German law in conformity with Article 7 of the Database Directive, the Federal Supreme Court held that there was an infringement.[306] The Federal Supreme Court thereby relied on the case-law of the CJEU, including the judgment in *Directmedia* publishing, in favour of a of a broad reading of the right of making available to the public to protect the database maker not only against competing products but also against any significant detriment, evaluated qualitatively or quantitatively, to the investment.[307]

This reading of the making available right is problematic since it seems to go much further than the understanding of the making available right, as part of the right of communication to the public in the field of copyright protection under Article 3(1) Information Society Directive.[308] For the concept of the communication to the public, the CJEU has always advocated a broad reading.[309] Yet, as regards the public, the Court requires an indeterminate number of persons.[310] In the *SGAE* case, following the principle of broad interpretation, the Court accepted to look at the hotel guests having access to broadcasts from their individual hotel rooms cumulatively and, hence, considered these guests as members of the relevant public.[311] But, still, in this case, the individual hotel guests, as an indeterminate group of people, had access to the same copyrighted content.[312] In Internet-related cases and, hence, as regards the making available right in particular, the situation is not substantially different. Internet use only differs by its interactive character where users try to access content at the time they prefer. But the same content should to be accessible to an indeterminate number of persons to form a public.[313] In copyright cases, the CJEU even requires a 'fairly large number of persons' to affirm communication to a public.[314]

In contrast, the Federal Supreme Court reads Article 7(2)(b) of the Database Directive in the sense that there is still a making available 'to the public' although the indeterminate number of persons having access to the allegedly information service will never have access to the same part of the contents of the database.[315] Granting access to the lorry drivers online to the information that only concerns them is not different from a communication of the same information through individual e-mails. The mere fact that communication takes places over the website of the defendant should therefore not suffice to consider it a communication to the public. While it is not by itself excluded that the making available right under Article 7(2)(b) of the Database Directive can be given a broader reading than the making available right under EU copyright law pursuant to Article 3(1) Information Society Directive in the light of the different subject-matter of protection[316], to grant broader

[306] Ibid, para 35.

[307] Ibid, para 37. Here, the Federal Supreme Court relied on Recital 42 of the Database Directive.

[308] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, [2001] OJ L167/10.

[309] Ever since Case C-306/05 *SGAE* [2006] ECR I-11519 = ECLI:EU:C:2006:764, para 36.

[310] Ibid, para 37. Case C-351/12 *OSA* ECLI:EU:C:2014:110, para 27.

[311] Ibid, paras 38-39.

[312] However, the CJEU seems to be somewhat ambivalent in this regard. It does not only refer to the cumulative effect of access of viewers in different rooms at the same time, but also to the quick succession of viewers as regards individual hotel rooms to argue a public. Ibid, para 38.

[313] As in the case of Internet live streaming of TV programs; see Case C-607/11 *ITV Broadcasting* ECLI:EU:C:2013:147, para 31 (pointing out that the TV programs 'must also in fact be communicated to a "public"').

[314] Ibid, para 32; confirmed in *OSA* (n 310) para 23.

[315] See explicitly *Autobahnmaut* (n 260) para 38.

[316] This could be read into the reasoning of the Court in *Autobahnmaut* (n 260) para 38, where the Federal Supreme Court argues that provision of individual information to members of the public constitute a 'typical form of exploitation' of a database.

protection to the non-meritorious sui generis databases than to copyright protected works can hardly convince.

From the perspective of the users of connected devices, the *Autobahnmaut* judgment of the Federal Supreme Court has to raise particular concerns. Under the condition that the manufacturers of such devices can in fact claim a sui generis database right, they could well prevent other online information service providers, as occurred in the *Autobahnmaut* case, from making accessible the specific information that was produced by using the devices.

h) Exceptions and limitations

The sui generis protection regime is particularly criticised for providing much more limited exceptions and limitations than those available under copyright law.[317] The list of merely optional exceptions and limitations in Article 9 Database Directive, which may or may not be implemented by the Member States, is much shorter than the corresponding list in Article 5 Information Society Directive in the copyright field. Therefore, it is claimed in legal writing that the exceptions and limitations of the latter Directive should also be made applicable to databases protected by the sui generis database right.[318] To make the Digital Single Market work, such exceptions and limitations would also have to be made mandatory.[319]

i) Potential introduction of a compulsory licensing system

The current digital revolution fuels a revival of the claim that that Database Directive should be reformed through introduction of a compulsory licensing system applicable to sole source databases.[320] Such a system was originally included in the Commission Proposal for the Database Directive[321], but ultimately it was not accepted by the European legislature.[322] The initial Commission Proposal shows that already in the 1990s the Commission was aware of the risk that the Directive could give rise to data monopolies. In line with this earlier Commission Proposal, such a compulsory licensing system could now be introduced not least with the effect of promoting access of the user of a connected device to data collected by such devices whenever the data is included in databases for which the manufacturer can claim a sui generis database right.

The Database Directive Final Evaluation Report extensively discusses the pro and cons of the introduction of a compulsory licensing.[323] Its authors admit that there are three reasons that count in favour of such a system: (1) doubts regarding the ability of the case-law of the CJEU on the exclusion of investment in the creation of data for assessing the availability of protection to address the problem of sole source databases; (2) the importance of access to 'big data' and sensor-generated data; and (3) the possibility of a reversal of the case-law on the exclusion of investment

[317] See Annette Kur et al, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases—Comments by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich' (2006) 37 *IIC* 551, 556-57. See also, from the perspective of the modern data economy, Leistner (n 217) 46-49.

[318] Leistner (n 217) 47.

[319] In the same sense Leistner (n 217) 48.

[320] See, in particular, Leistner (n 217) 42-46.

[321] Art 8 of the Proposal of the Commission of 13 May 1992 for a Council Directive on the legal protection of Databases, COM(92) 24 final.

[322] The idea was opposed by several Member States on the Council. On the legislative history concerning the compulsory licensing system see Database Directive Final Evaluation Report (n 21) 36-38.

[323] Database Directive Final Evaluation Report (n 21) 34-43.

in the creation of data.[324] Then, however, the authors discuss key issues that would need to be addressed.[325] Their analysis shows that a compulsory licensing system has to respect the confidential character of information and personal data protection rules. Whether the mandatory licence should only be available according to competition law standards, namely, for a licence seeker who intends to offer a 'new product'[326] and in which procedures and according to which criteria adequate remuneration should be assessed are among the most difficult questions. Ultimately, the authors of the Final Report do not express any strong claim in favour of introducing a compulsory licensing system. They only recommend carefully considering the effects of the Database Directive on competition with a particular 'close eye on sensor-produced technologies'. Compulsory licensing is finally called a 'possible solution' to the problem.[327]

Leistner seems to favour adoption of a compulsory licensing system, yet not without taking into account more recent considerations, such as personal data protection and data portability, that are important for the future working of the data economy.[328] The logic of such proposal is however not without doubt. It is still based on the assumption that the holder of the database right should receive fair and reasonable compensation for the investment she has made.[329] In fact, the original Commission proposal provided for a system to license at 'fair and reasonable terms'.[330] Accordingly, Leistner claims that users of the database should in principle be required to pay.[331]

This proposal is based on the assumption that, where the requirements for the sui generis right are fulfilled, the logic of this form of intellectual property protection will always justify a duty to pay for the use of the database. This assumption, however, can be contested. It has to be noted that a compulsory licensing system controlling the exercise of sui generis database rights cannot replace legislation on access rights to solve the problems of data lock-ins that result from *de facto* data control. The compulsory licensing system as part of the legislation on the sui generis database right would constitute a second layer of access regulation, which would not only complicate the enforcement of access rights; it could even create incentives for *de facto* data holders to try to claim a sui generis database right to make life more difficult for those who seek access to data.

Hence, the better approach is to concentrate on the formulation of data access rights. In principle, such data access rights should prevail over any sui generis database right. In the framework of the various access regimes, especially those taking the form of sector-specific regulation,[332] the question of whether the person seeking access to data has to pay a price to the data holder will anyhow have to be considered. Such regimes that provide for granting access at fair, reasonable and non-discriminatory (FRAND) terms are flexible enough to allow for taking account of the investment made in the obtaining and provision of the data without the need to discuss whether a sui generis right exists in the first place. On the other hand, there is no reason why the access interests of persons seeking access are not strong enough to prevail over the interests of the

[324] Ibid, 39-40. The latter argument is not self-understanding. It is inspired by claims made by businesses active in the commercialisation of sports events during the evaluation process. Those businesses claimed to reverse the the CJEU's case-law with the objective to enable them to collect remuneration through licensing the use of fixture lists. In case of such a reversal, a compulsory licensing system would appear even more needed. Ibid, 40.

[325] Ibid, 41-43.

[326] Standard for the availability of a compulsory licence under Article 102 TFEU under the *Magill* case law. See at 2.3 b) above.

[327] Database Directive Final Evaluation Report (n 21) 44.

[328] Leistner (n 217) 43-45.

[329] See also Leistner (n 217). 43-44 (nevertheless expressing the reservation 'if the legislative incentive ratio behind the sui generis right is at all valid').

[330] Art 8(1) Proposal for a Database Directive.

[331] Leistner (n 217) 43-44.

[332] See the 2017 Position Statement of the Max Planck Institute (n 9) paras 23-25.

database maker in receiving remuneration for the use of the sui generis database right. In particular, the interest in access to personal data could easily be considered a justification to mandate access to data for free even if this data are included in sui generis protected databases. More generally, no interest can be identified to charge a royalty rate for access to data generated by a connected device. The manufacturer of the device can anyhow charge a price for the sale or the use of the device, which will have to be paid, either directly or indirectly, by the user of the device. The manufacturer, and potential maker of the database, is thereby able to vector in the costs of making any database it is in need of for conducting its business.

In sum, instead of implementing a compulsory licensing system within the legal framework for the sui generis database right, the European legislature would be better advised to concentrate on the formulation of data access rights against *de facto* data holders, irrespective of whether they can claim a sui generis database right or not. What needs to be implemented in the Database Directive is a general exception according to which the sui generis database right does not apply where, and to the extent to which, other legal rules oblige the database maker to grant access to data. This rule would liberate any negotiation on data access from additional discussions about the existence and scope of sui generis database rights.

j) Coordination of access to personal data with the sui generis database right

Regarding the relationship between data access rights and potential sui generis database rights, it is to be noted that the right of access to personal data in Article 15 GDPR and the right to data portability in Article 20 GDPR are not satisfactorily coordinated with the application of the Database Directive. Both Article 15(4) GDPR and Article 20(4) GDPR provide that these two rights 'shall not affect the rights and freedoms of others'. Yet the construction of this wording remains rather obscure. As regards the data portability right, it is clear that the data processor should be allowed to refuse to grant data portability where data is pluri-personal, i.e., where granting data portability to one person would violate the data protection rights of another person. But it is quite unclear to which extent this provision also provides a justification for refusing data portability based on trade secrets protection and intellectual property rights, including intellectual property rights of the data processor.[333] The obvious candidate for such a right would be the sui generis database right.

In its Recital 63, the GDPR in fact mentions the role of intellectual property rights by stating:

> That right [meaning the right of access to data] should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.[334]

Article 29 Working Party has taken up this exact wording of the recitals in its Guidelines on data portability also with regard to the interpretation of the data portability right in Article 20(4) GDPR,[335] which is understandable given the complementary wording in Article 15(4) GDPR. But Recital 63 does not particularly increase legal certainty. On the one hand, Articles 15(4) and Article 20(4) GDPR seem to apply to all kinds of intellectual property rights of others, and therefore do not exclude reliance on the sui generis database right as a limitation to the right of access to personal data and the right to data portability. At the same time, Recital 63 is unclear as to whether it only relates to the rights of third persons or whether such rights can also be those of the data processor. The

[333] The lack of precision of this provision is also stated by others. See Lucio Scudiero, 'Bringing Your Data Everywhere: A Legal Reading Of the Right To Portability' (2017) 3 *European Data Protection Law Review* 119, 127.

[334] Recital 63, 5th and 6th sentence, GDPR.

[335] Article 29 Data Protection Working Party, Guidelines on the Right to data portability (n 156) 12.

analysis of the sui generis database right shows that database rights of the data controller, could easily undermine the working of the data access and data portability rights of the data subjects.

In contrast, some authors have argued that the data portability right could make online business models 'obsolete' if the trade secrets and certain intellectual property rights of the data controller were not respected.[336] These authors illustrate this argument by the example of True Fit, an online service provider who helps users of online clothing retailers to find the right cloth sizes for their shoppers, based on personal data shoppers provide to True Fit.[337] However, this argument is not convincing. On the contrary, the data portability right would specifically fulfil its function of opening up the market to competitors of True Fit through enabling shoppers to switch more easily. Without making the business model 'obsolete' for True Fit, data portability only facilitates imitation of this business model by competitors. The business model as such is not protected, neither under trade secrets nor intellectual property legislation. In addition, the authors do not even explain on what kind of protection or intellectual property rights True Fit could rely. In particular, the personal data of the shoppers does not seem to fulfil the requirement of trade secrets. Even without data portability, they could provide the same information relating to their height, weight and measurements as well as what kind of brands and clothing they prefer independently to any other party. Yet it is not at all excluded, in the light of the above analysis, the True Fit holds a sui generis database right as regards the dataset that needs to be provided in fulfilling the data portability right. This only confirms the negative impact of the sui generis database right on the data portability regime.

The wording of Articles 15(4) and 20(4) GDPR is also peculiar in the sense that it does not explicitly state that the data portability right only applies 'without prejudice to' the rights and freedoms of authors. In the light of the more cautious wording, some commentators characterise these provisions as balancing clauses that do not require full prevalence of rights and freedoms of others over the data access rights.[338] This may explain why the Article 29 Working Party argues that conflicting fundamental freedoms or rights of others should not give rise to a refusal to provide all information to the data subject. Yet, even if such reading of Articles 19(4) and 20(4) GDPR was followed[339], it would still be unclear whether, or to which extent, this suffices to exclude reliance on intellectual property rights owned by the data controller *per se*.

Hence, it will be for the CJEU to clarify the relationship between the right of access to personal data and the right to data portability, on the one hand, and potential sui generis database rights especially of the data controller, on the other. In particular, if the CJEU confirmed the character of Articles 15(4) and 20(4) GDPR as balancing clauses that allows for considerable flexibility to decide cases in the light of the particular circumstances, Article 20(4) GDPR would give rise to considerable legal uncertainty. In sum, it is recommended that Articles 15(4) and 20(4) GDPR, by referring to the rights of 'other', should be read to not refer to trade secrets and intellectual property rights of the

[336] Diker Vanberg and Ünver (n 114) 5. See also Weber (n 95) 68, who argues that data portability may go too far in the light of the investment, for instance, the operator of a social network has made in the data analysis of personal data. In this regard, however, it has to be remembered that the data portability right does not extend to 'derived' or 'inferred' data. On the scope of the data portability right, see at 4.5 b) below.

[337] Diker Vanberg and Ünver (n 114) 5. On this business model, see the website of the company: www.truefit.com (accessed 31 July 2018).

[338] In this sense, see De Hert et al (n 155) 198.

[339] It should be noted that other language versions do not necessarily reflect the more cautious English version. The German version provides that the data portability right '*darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen*', which would need to be read more in the sense of 'must not restrict the rights and freedoms of other persons'. The French wording—'*ne porte pas atteinte aux droits et libertés de tiers*'—equally seems to argue for full respect of the rights and freedoms of others. Based on the English text, in contrast to De Hart et al, other authors have argued that the wording indicates that the right to data portability 'enjoys a lower rank compared to the rights and freedoms of others'. Scudiero (n 334) 126.

data controller. Otherwise, the sui generis database right would especially have the potential of seriously compromising the effectiveness of the data access rights of the data subject.

k) Conclusion

The analysis of the sui generis protection regime shows that access of the users to the data generated and processed by connected devices could be seriously compromised by the legal uncertainties and potential frictions that broad protection of sui generis database rights could produce. The sui generis right, where applicable, would strengthen the anyhow existing exclusivity position of the manufacturer as *de facto* data holders and, as illustrated by the German *Autobahnmaut* case, enable them to prevent third parties from providing additional information services.

So far, the sui generis database right does not seem to be invoked in a consistent manner by database makers. One of the reasons may be that the availability of this form of protection anyhow plays a very limited role when firms make a decision to invest in the production of databases. At the same time, database makers may refrain from claiming the sui generis right because of the legal uncertainties surrounding that right. Yet it would be wrong to ignore the negative potential impact and even disruptive role sui generis database rights can play. Apart from the early *British Horseracing* and *Fixtures Marketing* cases, more recent case-law on the EU and national level has strengthened and broadened the scope of protection, which enables rightholders to largely restrict access to data and freedom of information. Against this backdrop, the sui generis database right can also apply to machine-generated data, especially in form of independent data 'observed' by a connected device.

While many of the uncertainties of the case-law could still be satisfactorily resolved by the CJEU, the current attitude of the Commission to wait and see has to raise serious concerns. On the one hand, how the CJEU will decide open questions is unpredictable and could considerably harm the development of the data economy. On the other hand, immediate legislative action is anyhow advisable with the objective of safeguarding that existing and future access rights, including those granted to the users of connected devices, will not be compromised by potential sui generis database rights.

Hence, the perspective that future legislation should adopt is not to modernise the sui generis database right with even broader scope of protection, but to contain its potential negative impact on the development of the data economy and the access rights needed for guaranteeing free flow of data. The current development of the data economy may even make claims to completely abolish the sui generis database right as a non-meritorious intellectual property right more convincing than ever.[340] Yet complete abolition of the right may be too difficult to be implemented for political reasons. But immediate precautions should be taken to make sure that the sui generis right will not compromise access. The best solution for achieving this objective is not to revive the old idea of creating a compulsory licensing system for the sui generis database right. Rather, the EU legislature should create a new exception in the Database Directive that gives precedence to any existing and future data access regimes over the sui generis database right. The negative impact of the absence of such rule can already now be observed in the context of the uncertainties regarding the relationship of the data access right and the data portability right pursuant to Articles 15 and 20 GDPR, on the one hand, and potential sui generis database rights of data processors, on the other.

[340] Also in favour of abolishing the sui generis rights regime and even prohibiting the Member States from maintaining such a regime, Hugenholtz (n 52) 98-99.

4.3 Other exclusive rights in data

The sui generis database right is not the only right that has the potential of blocking access to data. In the following, the analysis will shed more light on other intellectual property rights, namely, copyright law and patent law, as well as the civil law concept of property.

a) Copyright law

As already explained further above[341], EU copyright law has inbuilt features that prevent it from negatively affecting free flow of information. Although many copyrighted works (computer programs, music, books, films, computer games, photographs) are nowadays exploited in a digitised form, copyright protection will not result in data ownership. Copyright only protects works as immaterial assets on an abstract level irrespective in which format—digital or analogue—the works are represented. The copyright holder does not own the raw data in which copyrighted work is encoded on the computer of a user.[342]

The same holds true for copyright-protected databases.[343] According to Article 3(1) of the Database Directive, in the case of databases, the character of the author's 'own intellectual creation' has to relate either to the selection or the arrangement of the contents of the database. According to the CJEU, the originality requirement is satisfied if 'through the selection or arrangement of the data which [the database] contains, its author expresses his creative ability in an original manner by making free and creative choices (...) and thus stamps his "personal touch"'.[344] These requirements will hardly be fulfilled where connected devices generate data. One reason is that such datasets may not even be considered the result of human authorship.[345] Even where at least the arrangement of the data were indirectly influenced by the person designing the device in a creative manner, extraction of an individual piece of information from such a database would not amount to an infringement of the copyright, since information as such will not represent the creative selection or arrangement of the data. If, in contrast, somebody copied the whole database and is thereby reproducing the creative elements of the database, copyright protection would be available.

Yet it is not that clear that copyright law will never cause problems for the modern data economy. A new and important issue that deserves more attention and still requires profound legal research is the question whether potential copyright protection for so-called application programming interfaces (APIs) can cause and aggravate data lock-ins.[346] APIs are most important for establishing interoperability between different data formats and, thus, for enabling data access and data portability. APIs are tools that allow the exchange and communication of data and digital content between different websites, computer programs and content providers; they enable access to, so far, closed datasets. Hence, data interoperability, which has already been identified as a most important issue by the Commission in its European Data Economy Communication of January 2017[347], may therefore depend on the use of APIs by persons seeking data access. The question therefore is whether APIs are proprietary in the first place; or to put it differently, whether they are

[341] At 2.2 d) above.

[342] In this context, see also the discussion of the *UsedSoft* judgment of the CJEU at 4.1 a) above.

[343] See also Dorner (n 26) 621; Hugenholtz (n 52) 83-85.

[344] Case C-604/10 *Football Dataco v Yahoo! UK* ECLI:EU:C:2012:115, para 38 (adopting the general originality concept of EU copyright law as developed by the Court for other categories of works to database works).

[345] For this reason, Hugenholtz (n 52) 85 rejects the character of a copyrighted database for databases generated by machines without human intervention.

[346] Due to the complexities of the issues, this research will not be conducted in this Study.

[347] European Data Economy Communication (n 9) 15-16.

owned by somebody. If this were the case, situations could arise that are similar to those known from the mobile telecommunications sector where standard-essential patents (SEPs) create a situation in which implementors will not have easy and sufficient access to such technology at reasonable royalty rates.[348] Whether this is indeed a realistic concern depends on whether (1) APIs can enjoy intellectual property protection in general, (2) the underlying IP right is used by a third person when establishing data interoperability, and (3) whether the user can rely on any exceptions and limitations. As part of computer programs, the best candidate for the protection of APIs is copyright law. However, in the EU, neither the Courts nor scholarship have so far considered whether APIs qualify for copyright protection. In the US, in the *Oracle v. Google* case, the Court of Appeals for the Federal Circuit has more recently confirmed that copyright protection would be available under copyright law.[349] The most troubling aspect of this judgment is that the Court did not only confirm the existence of copyright protection for the API at hand, but more importantly also argued that the defendant Google could not rely on the fair use exception of US copyright law.[350] Under EU copyright law, which does not provide for any flexible fair use principle, if APIs indeed enjoyed copyright protection and if creative parts of the API were used by a firm that establishes data interoperability of data, copyright protection of APIs would therefore be even more likely. Indeed, EU copyright law does not provide for the necessary exceptions and limitations to allow for establishing data interoperability without the consent of the owner of the copyright.[351] Hence, the European legislature may have to consider the need for legal reform by adopting an additional exception in the Computer Programs Directive on the use of APIs to enable data interoperability.

b) Patent law

In the debate on data ownership, the potential role of patent law is often overlooked.[352] In fact, patent law may come into the picture as a potential source of data ownership where somebody has been granted a process patent. The reason is that the scope of protection of process patents under national patent laws typically extends to the 'products' that are obtained through a patented process (so-called 'derivative product protection'). In a similar vein, Article 25(c) of the—yet not effective—Agreement on a Unified Patent Court[353] stipulates that a process patent also provides the right to prevent a third party from 'offering, placing on the market, using, or importing or storing for those purposes a product obtained directly by a process which is the subject-matter of the patent'.

The question in this context is whether data can be 'products' that are obtained by using a patented process. The question becomes specifically relevant where data are generated in a factory based on

[348] From an EU competition-law perspective, see Case C-170/13 *Huawei Technologies* ECLI:EU:2015:477 (on using Art 102 TFEU to control the licensing practices of dominant SEP holders in the field of mobile telecommunications technologies).

[349] *Oracle America, Inc v Google LLC* (Fed. Cir., 27 March 2018) available at: http://www.cafc.uscourts.gov/sites/default/files/opinions-orders/17-1118.Opinion.3-26-2018.1.PDF (accessed 31 July 2018).

[350] See also the Brief of the American Antitrust Institute as Amicus Curiae in Support of Petition for Rehearing en Banc, Oracle America, Inc. v. Google LLC (12 June 2018) available at: http://www.antitrustinstitute.org/sites/default/files/AAIRehearingAmicusBrief.pdf (accessed 31 July 2018), arguing that the judgment of the Federal Circuit fails to consider the need for data interoperability as well as the need to create a balance between exclusive rights and competition. The Brief explicitly draws a comparison with the problems arising from SEPs in the patent world (at 6-7). This Brief also argues that the API might not even be copyright-protected under US law or that its use should at least be legal under the fair-use doctrine (at 8-9).

[351] See the exceptions and limitations in Arts 5-6 Computer Programs Directive (n 57).

[352] See, however, Drexl (n 51) 57-61.

[353] Agreement on a Unified Patent Court, [2013] OJ C175/13.

a patented production method or, maybe even more relevant, in the context of a process patent applied in medical diagnostics. If the question were to be answered in the affirmative, the patent owner would also 'own' the result of the diagnosis.

Of course, such protection would only become relevant where the patent is used without the consent of the patent holder. Only if the patented process is used without a licence does the patent holder have a right to prohibit the commercialisation of the product as the offspring of the process. The objective of this legal design is to protect the holders of process patents similar to the holders of product patents. In both cases, patent law aims to enable the patent holder to control secondary product markets. This is meant to guarantee that the incentives to innovate do not substantially differ between product and process patents. In addition, indirect product protection seeks to prevent a specific cross-border problem. Without indirect product protection, third parties could be tempted to move the application of the process patent to jurisdictions without patent protection and still sell the products without consent of the patent holder in jurisdictions where the process is patented.

The latter situation also characterises the *Hunde-Gentest* case where the District Court of Düsseldorf denied protection for the patent holder.[354] In addition, the Court had to decide whether indirect product protection would also apply to information, namely, in the form of the results of a gene test. In this case, the underlying process patent for the gene test for dogs was protected in Germany, but not in Slovakia. The defendant, who had previously applied the test in Germany, moved the testing to Slovakia to avoid a patent infringement. Therefore, the Court was only requested to decide whether the plaintiff could rely on the process patent to prevent the defendant from communicating the test results to Germany. The Court denied such protection, arguing that the test results as mere information cannot be considered the product of the process. The Court noted that, since information is directly accessible for humans without any further technical process, information as such lacks technicity and therefore cannot be patented. Yet the Court refrained from arguing that the 'product' of a process patent needs to be patentable as such to be protected within the scope of the process patent.[355] Rather, the Court showed sensitivity for the interest in free flow of information. It rejected protection with the objective to avoid using patent law as a kind of trade secrets protection. In particular, the Court stressed that patent law should not support a claim to ban communication of the test result to anybody in Germany, which, in the last resort, would even include denying a person who knows about the test result entrance to the German territory.

Yet the German Federal Supreme Court went a step further, simultaneously applying a more differentiated approach, in the more recent *Rezeptortyrosinkinase II* case.[356] Similar to the scenario in *Hunde-Gentest*, this case related to process patents for gene tests. The Court denied protection for the information as an indirect product of the application of the process patents since communication of information as such is excluded from the scope of product patents. Thereby, the Court guaranteed that the exclusion of product patents cannot be circumvented by applying for process patents.[357] Furthermore, the Court considered whether a series of digital raw data in which

[354] District Court (*Landgericht*) Düsseldorf of 16 February 2010, Case 4b O 247/09 *Hunde-Gentest*, available at: https://www3.hhu.de/duesseldorfer-archiv/?p=813 (accessed 31 July 2018).

[355] Such requirement is also rejected by the European Patent Office (EPO). See EPO, Decision of the Enlarged Board of Appeals, Case G 1/98 *Transgenic plant/NOVARTIS-II*, [2000] OCJ EPO 111, 138. The Enlarged Board of Appeals confirmed the availability of process patents, including protection of the products deriving from the process according to Article 64(2) European Patent Convention (EPC), even in a case where the product would be a plant, which is excluded from patentability under Article 53(b) EPC.

[356] Federal Supreme Court (Bundesgerichtshof) of 27 September 2016, Case X ZR 124/15 *Rezeptortyrosinkinase II*, available at: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=77138&pos=0&anz=1 (accessed 31 July 2018).

[357] Ibid, para 13.

the result of the analysis was encoded can be considered a protected derivative product of a process patent.[358] Still, for such protection, the Court held that two requirements need to be met: first, the data must be capable of being repeatedly used for the same purpose just like a tangible product, and, second, the series of digital data must, according to its very nature, in principle be capable of qualifying for protection by a product patent (but without fulfilling the specific patentability requirements, including novelty and inventive step).[359] In the earlier *MPEG-2 Videosingalcodierung* case, these requirements were held to be fulfilled for the encoding of a video, not because the data sequence contained the video, but because of the technical features the encoding had used.[360] According to the Court this distinction pursues to guarantee that only information that has a technical character be protected by the patent law; other information with no technical character, even if conveying economic benefits, would fall outside the scope of patent protection.[361] Based on these considerations, in *Rezeptortyrosinkinase II*, the Court denied derivative product protection for the series of digital data, since its characters only consisted in the digital encoding of the results of the gene test.

In sum, this shows that, at least under German patent law, approaches have already been developed to restrict the availability of patent protection for data. Yet derivative product protection could be claimed for digital data in the rare instances where the encoding demonstrates a technical character. What is important to note in such cases is that patent protection relates to the syntactic level of the data. In addition, the judgment of the Düsseldorf District Court shows particular sensitivity for the public interest in free flow of information, and even free movement of persons within the EU. This approach, however, would still need to be confirmed by the higher courts in Germany.

c) Civil law property

Finally, civil law countries are nowadays very likely to discuss whether the concept of property found in the national Civil Code, which is usually limited to the ownership of tangible objects and land, should be opened to also include data. For instance, both the *Deutsche Juristentag*[362], which is the most important private organisation for discussing legal reform in Germany, bringing together legal professionals from all different sectors, and the *Privatrechtslehrervereinigung*, the Association of German speaking private law professors[363], more recently considered whether the German Civil Code is in need of a digital update.

Yet equating data with tangible objects as a subject-matter of property is a rather risky undertaking. The risk is that, as an expression of general enthusiasm and striving for modernisation, the legislature or courts will not give sufficient consideration to the different economics that distinguish markets for non-tangible objects from those for tangible objects.

---

[358] In fact, this was the Court's holding in a previous case relating to the sequence of digital data representing a video. See Federal Supreme Court (Bundesgerichtshof) of 21 August 2012, Case X ZR 33/10 *MPEG-2-Videosignalcodierung* [2012] 194 BGHZ 272, paras 21-22.

[359] *Rezeptortyrosinkinase II* (n 356) para 21.

[360] *MPEG-2-Videosignalcodierung* (n 358) para 20.

[361] *Rezeptortyrosinkinase II* (n 356) para 22.

[362] The debates of the Deutsche Juristentag revolve around *Gutachten* (expert opinions), which are usually drafted by law professors. Convening in Essen on 13-16 September 2016, the Deutsche Juristentag discussed a 'digital up-date' of the German Civil Code in the light of the *Gutachten* by Florian Faust, *Digitale Wirtschaft—Analoges Recht—Braucht das BGB ein Update? Gutachten A zum 71. Deutschen Juristentag* (Munich: C.H. Beck, 2016).

[363] On 10-12 September 2017, the conference of the *Zivilrechtslehrervereinigung* in Zurich was dedicated to '*Digitalisierung und Privatrecht*' (Digitisation and Private Law). The contributions to this conference are expected to be published in *Archiv für civilistische Praxis*.

Hence, the question of whether civil law is in need of being 'updated' should be considered carefully and within the specific context of protection. To transfer the principles of contractual liability developed for the sale of tangible goods to defects of digital goods is one thing;[364] to recognise a property right for holders of data with exclusionary effects on third parties is another thing. In Germany, the debate is strongly triggered by certain limitations of tort law. Under Section 823(1) German Civil Code, there is only a claim for damages if somebody injures the 'life, body, health, freedom, property or another right' of someone else.[365] Whereas it can still be argued that, if data stored on a physical carrier are deleted by a third person, this will harm the property in the physical carrier[366], reliance on property in the physical carrier will not provide sufficient protection where the person who has a legitimate interest in protection is different from the person owning the physical career. Such situations are becoming increasingly frequent in the data economy where the role of the physical carrier is decreasing. Nowadays individuals often store 'their' data on servers of Internet service providers. In the case of cloud computing it may even be practically excluded to identify the physical carrier on which the data was stored.[367]

German Courts have continuously extended the range of 'other rights' to include, for instance, the general personality right, but they have also limited those rights to 'absolute rights'. This explains the current discussion on whether courts should recognise 'data ownership' as another absolute right to protect the integrity of datasets against injuries committed by third parties.

Recognition of tort liability in case of deletion of data would still restrict property rights protection to the integrity interest of the data holder. Yet tort protection under Section 823(1) Civil Code is automatically complemented with the availability of injunctive relief to prevent injury. For that purpose, German courts rely on an analogy to Section 1004 Civil Code, the legal basis for injunctive relief in case of unlawful interference with property.

Injunctive relief raises the important question whether injunctions should also be used in the case of misappropriation and unauthorised use of data. Property in tangibles basically provides two sub-rights, a right of integrity and a right to exclude others from any use.[368] While the debate on data ownership is inspired by the lack of protection as regards the integrity of data, recognition of a right to exclude other persons from *any* use of the data would amount to a powerful intellectual property right that would have the potential of negatively affecting free flow of information.[369] From an economic standpoint, a right to exclude others from the use of data is less needed than in the case of tangibles because information is non-rival in nature.[370] Accordingly, from an economic perspective, it is easier to justify protection of the integrity of data than to provide full intellectual property-style protection, including injunctive relief against any form of use of data.[371]

Tort protection of the integrity of datasets is absolutely needed for the functioning of the data economy. Data security is among the most serious concerns and can only be guaranteed by using a toolbox of different instruments, including technical protection measures, tort liability and

[364] See the Commission Proposal for a Digital Content Directive (n 199).

[365] English translation of the *Bürgerliches Gesetzbuch* available at: http://www.gesetze-im-internet.de/english_bgb/ (accessed 30 April 2018).

[366] See, for instance, by Redeker (n 26) 636; Zech (n 44) 142.

[367] See also Wiebe (n 102) 880.

[368] As regards the right to exclude under German law, see Section 903 Civil Code. On the distinction between the three different rights of property regarding data ownership, including (1) possessing data—with the possibility to exclude access—, (2) using data, and (3) destroying data (right of integrity) see Zech (n 93) 56-57.

[369] See also Hugenholtz (n 52) 94-95; Wiebe (n 102) 882.

[370] See also at 2.3 above.

[371] In contrast, Zech (n 44) 139-40 includes the right of integrity and the right to exclude others from use on the same level of his concept of data ownership without taking account of the different economics of the two rights.

criminal measures against data espionage, data phishing or computer sabotage. Such instruments also act in the interest of the users of connected devices. Even where it is the manufacturer that can rely on tort liability or criminal law to protect the integrity of the data collected from users, such instruments will have at least the indirect effect of protecting the user against the loss of data.

However, neither tort nor criminal liability protecting the integrity of data force the legislature or the courts to recognise a general data ownership right, including a right to control and license the use of the data in secondary markets. In particular, such a conclusion is not mandated by criminal law provisions. While it is true that criminal law provisions against computer sabotage also protect underlying private interests in data integrity, such provisions do not have to be interpreted as a legislative recognition of a general data ownership right.[372]

4.4 Trade secrets protection

With the Trade Secrets Directive[373], the EU disposes of a more recently adopted legal instrument that nevertheless remains rather obscure with respect to its application to the digital economy.[374] This can be criticised, on the one hand. But the Trade Secrets Directive necessarily strives to establish a generally applicable, technology neutral regime of protection, on the other hand. Trade secrets protection is about protecting specific information against misappropriation. Nowadays, such misappropriation is most likely to occur in a digital environment. The rapid development of the data economy has not only increased the vulnerability of personal data, but of course also of trade secrets. Hence, to clarify the application of the Trade Secrets Directive in a digital environment in general and with respect to connected devices in particular is of great importance.

As a form of tort liability, trade secrets protection appears as a less intrusive instrument for protecting data than the sui generis database right or any potential data ownership right. The Directive also describes trade secrets protection merely as a 'complement' or an 'alternative' to intellectual property rights.[375] The fact that trade secrets protection is a different field of law is also proven by the fact that enforcement of trade secrets protection does not follow the rules of the IP Enforcement Directive[376] but the ones of the Trade Secrets Directive as *lex specialis*.[377]

With respect to the needs of the data economy, the different legal character of trade secrets protection could be assessed in three very different ways. One possible conclusion could be that this field of law is insufficient to provide adequate protection against the growing vulnerability of trade secrets in the digital environment, and that, at best, it works as a 'legal intensifier' of the *de facto* exclusivity of data holders.[378] Secondly, its less intrusive character could make trade secrets

[372] Against Thomas Hoeren, 'Dateneigentum—Versuch einer Anwendung von § 303a StGB im Zivilrecht' (2013) *Multi-Media Recht* 486. See also Sebastian J Golla and Sebastian Thess, 'Das Strafrecht als schlechtes Vorbild—Betrachtungen zum "Dateneigentum" und § 202d StGB' in: Moritz Hennemann and Andreas Sattler (eds), *Immaterialgüterrecht und Digitalisierung* (Baden-Baden: Nomos, 2017) 9; Wiebe (n 102) 881; Zech (n 44) 143 (like here rejecting the idea that the criminal law provisions have to be interpreted as the attribution of property rights in the sense of private law).

[373] Trade Secrets Directive 2016/943 (n 22).

[374] See also Wiebe (n 102) 880 (arguing that the drafters of the Directive did not have big data in mind).

[375] Recital 2 Trade Secrets Directive.

[376] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, [2004] OJ L 157/45.

[377] Recital 36.

[378] This seems to be the standpoint of Herbert Zech, 'Information as Property' (2015) 6 *Journal of Intellectual Property, Information Technology and E-Commerce* 192, para 26 (criticising that trade secrets protection allows for acquisition based on independent discovery and use and on the risk of termination of protection through loss of secrecy).

protection particularly promising by responding more adequately to the needs of protection of data holders in the data economy without unnecessarily distorting free flow of data.[379] And thirdly, trade secrets protection may still go too far or protect the wrong interests in the data economy and, therefore, its rules may be considered as being in need of a restrictive interpretation or even reform.

This sets the perspective for the following analysis of the working of the Directive in the context of the modern data economy with a particular focus on connected devices to decide which of the three assessments is the appropriate one.

a) The concept of trade secrets

The concept of trade secrets is defined in Article 2(1) Trade Secrets Directive as information that has to meet three cumulative requirements, namely,

> (a) it is *secret* in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
>
> (b) it has *commercial value because it is secret*;
>
> (c) it has been *subject to reasonable steps* under the circumstances, by the person lawfully in control of the information, *to keep it secret*.[380]

Each of these requirements presents challenges for interpretation and application as regards data collected by connected devices.

According to the definition of trade secrets, the subject-matter of protection is information. This clearly locates trade secrets protection on the semantic level of data. This means that a set of raw data as such, namely, as an aggregation or sequence of bits and bytes, cannot be considered trade secrets. However, trade secrets can be digitally encoded. Under such circumstances, digital data can 'contain' trade secrets. This is not so different from the analogue world. A folder of printed papers or even a document or the text printed on it should not be considered trade secrets as such. It is the information that can be found in the folder or a text that constitutes trade secrets. It is very important to distinguish the information (data on the semantic level), on the one hand, from the signs in which it is encoded (data on the syntactic level) as well as from the physical carrier, on the other hand. Trade secrets can even exist independently of such signs and physical carriers, namely, as pure information known by people working in a firm. Trade secrets protection is therefore very different from whatever kind of data ownership or a data producer's rights that the legislature may intend to limit to the syntactic level of raw data.

Conversely, the kind of information that can be considered trade secrets is in no way limited. Trade secrets may in particular consist in know-how as technical information or any other business information.[381] Hence, nothing excludes data collected through connected devices, or more

---

[379] See Tania Aplin, 'Trading Data in the Digital Economy: Trade Secrets Perspective' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 59 (proposing trade secrets protection as an alternative to the introduction of a data producer's right); see also Josef Drexl, Reto M Hilty et al, 'Data Ownership and Access to Data—Position Statement of the Max Planck Institute for Innovation and Competition on the Current European Debate' (16 August 2016) paras 18-28, available at: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf (accessed 31 July 2018).

[380] Emphasis added.

[381] See also Recital 14.

precisely the information that such data contains as well as the information that can be drawn from such data, namely, through big data analysis, from the subject-matter of trade secrets protection. Limitations arise from the other three additional cumulative requirements mentioned in Article 2(1) Trade Secrets Directive.

The first of these requirements is *secrecy* of the information. Article 2(1)(a) defines secret information as information that is not, 'as a body or in the precise configuration and assembly of its components', generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question. The wording of 'as a body or in precise configuration and assembly of its components' is difficult to understand. Other language versions indicate that the necessary secrecy will be missing where the information as a whole or in its individual components[382] is generally known or is readily accessible within the relevant circles. This shows that secrecy should not only be related to the each and every piece of information in isolation but also to its entirety or to how individual pieces of information relate to each other.

The role of this limitation becomes clearer in the context of the second requirement, according to which there has to be a causal link between the secrecy and the *commercial value*. Commercial value can accordingly arise from the whole body of the secret information or the particular arrangement and composition of its individual components. The value requirement excludes trivial knowledge or skills of employees. This requirement also highlights that only information that enhances the competitiveness of the firm in the market can be considered a trade secret.[383]

Thirdly, to secure protection, the holder of the secret must have taken *reasonable steps to keep the information secret*. Hence, acquisition of protection is not effortless. The holder of the trade secret may use technical protection measures and confidentiality agreements imposed on its employees and trading partners to maintain the secrecy.[384]

In sum, the definition of the trade secrets shows that only information where there is a legitimate interest in keeping the information secret (because confidentiality produces commercial value) and where there is a legitimate expectation that confidentiality will be maintained (because reasonable steps were taken to keep the information secret) will be protected under the Directive.[385]

With respect to data generated by connected devices, several open questions need to be discussed.[386] One question is whether individual data—or better a specific piece of 'information'—can fulfil the requirement of a trade secret. On this issue, the 2017 European Data Economy Staff Working Document convincingly argues that individual information contained in machine-generated data will regularly lack economic value, but such value can well arise from the combination of different pieces of information contained in the same dataset. Indeed, as regards the raw data generated by connected devices, trade secrets protection will generally relate to the whole of the information that is contained in the often constantly changing dataset.[387] This also

[382] The French text reads: 'dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments'. The German text reads as: 'in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile'.

[383] Recital 14 Trade Secrets Directive.

[384] In the light of the requirements of trade secrets protection, it cannot be criticised that *de facto* data holders use technical protection measures to acquire such protection. This is too easily put aside by Mezzanotte (n 45) 168-69, arguing that taking reasonable measures to guarantee the secrecy is just one of several cumulative requirements for trade secrets protection, and, therefore, use of technical protection measures by *de facto* data holders will conflict with the general principles of intellectual property. In particular, Mezzanotte overlooks that trade secrets protection cannot be equated with intellectual property protection. See at c) below.

[385] Recital 14 Trade Secrets Directive.

[386] On this see also Aplin (n 379) 65-67.

[387] Similarly Aplin (n 379) 66 (mentioning additional reasons).

makes sense since it will be the dataset in its entirety that is the object of measures to protect the secrecy of the information contained in it.

Still, several uncertainties exist in other regards. In particular, the Directive is silent on the quantitative threshold of the commercial value; the recitals only indicate that the test has to be harm-based and that even potential value may suffice.[388] In this regard, the question arises whether the individual dataset produced by a single connected device suffices to fulfil the requirement of economic value or whether this dataset needs to be combined with the data that originate from other devices controlled by the same manufacturer.

This question mandates a differentiated answer. In general, based on a harm and competition-based test, sufficient value should be affirmed if there is a proper market in which the secrecy with regard to a particular dataset enhances the competitiveness of the manufacturer. With respect of the dataset produced by an individual device, this can regularly be answered in the affirmative, since the device in collecting and processing the data will typically provide the consumer with utility and, therefore, provides the manufacturer with better chances to sell the device. But the question is also whether there is a causal link between the secrecy and the economic value. In fact, access of competitors to the information will not necessarily destroy the competitive advantage of the manufacturer. Yet such causal link may exist where data relates to the technical functioning of the individual device. Such data will typically help the manufacturer to improve such devices and enable him to provide maintenance services to the user of the device. Hence, in many instances, only part of the data that a single connected device generates will be capable of being considered a trade secret. In particular, where the data produced by a connected device is very limited and no particular secrecy interest exist, neither on the part of the manufacturer nor of the customer, such as in the case of a smart meter measuring the consumption of energy, such data will most likely not be protected as a trade secret.

Trade secrets protection will also not be needed and, hence, fail to come into existence when the data produced by connected devices will be exchanged on large data sharing platforms, for instance, to enable automated or autonomous driving. Where the manufacturer has an inherent interest in sharing data, trade secret protection is no issue.

Trade secrets protection will matter most where the manufacturer aggregates data collected from different devices for the purpose of conducting his own main business. Manufacturers will aggregate data on the functioning of all connected devices in order to further improve and develop these devices. Moreover, specific categories of data may also be aggregated in an anonymised form to commercialise these data in secondary markets. For such purposes the manufacturer will also need to keep the information contained in these datasets secret to be able to charge a price for granting access to the information contained in the data.

The aggregated datasets of manufacturers can also become the object of big data analytics. The goals of big data analysis can be more or less concrete. It is the possibility to 'mine' big sets of data with large variety, such as customer data, for random correlations.[389] In such cases the nexus between the interest in secrecy and control of access to the dataset, on the one hand, and the secrecy relevance of the concrete information, on the other hand, may be very lose. But the wording of Article 2(1)(a) Trade Secrets Directive seems sufficiently flexible to justify protection also in this case, since the secrecy interest does not have to relate to all pieces of data individually. It is also to be noted that in the case of big data analyses the economic value is always generated from the information contained in the underlying dataset. The only uncertainty relates to the lack of *ex ante* knowledge what correlations will produce most valuable insights. But this does not argue

[388] Recital 14 Trade Secrets Directive.

[389] On this scenario see also Aplin (n 379) 68.

against at least 'potential' economic value of such a dataset as an entire body of information in the sense of Article 2(1)(a) of the Directive.

No doubts arise with respect to the protection of big data analysis tools and computer programs. Irrespective of the availability of copyright protection, such tools can easily qualify as trade secrets under the Directive.[390]

b) The holder of the trade secret

Exact identification of the person holding the trade secret is important since it is the holder of the trade secret who can claim the enforcement remedies under the Trade Secrets Directive in case of a violation. Article 2(2) Trade Secrets Directive defines the holder of the trade secret 'as the natural or legal person controlling the trade secret'. Problems of interpretation and application arise from the requirement of control. In the case of the data collected in a connected device, it is not necessarily clear whether the manufacturer exercising *de facto* control over the data or the user of the device, physically possessing and operating the device, is controlling the trade secret in this sense. Yet another possibility would be to consider both persons as co-holders of the trade secret.[391]

In principle, vesting protection in the manufacturer of the device, irrespective of whether the trade secret relates to the data produced by a single connected device or to the aggregated datasets controlled by the manufacturer, should appear as the most appropriate solution. This conclusion arises from an interest-based application of Article 2(2) of the Directive. The criterion of controlling a trade secret correlates with the requirements for trade secret protection in Article 2(1) of the Directive. In line with these requirements, the person or entity who has a competitive interest in keeping the information secret and, most importantly, takes specific steps to guarantee the secrecy, will have to be regarded as the person controlling the secrecy in the sense of Article 2(2), even if somebody else is in the possession of the connected device that collects the data.

Hence, the user of a connected device will usually not be considered a holder of a trade secret contained in the data produced by that device. However, exceptions may nevertheless exist. Especially a business operator using a connected device may have a particular interest in keeping that information collected by the device confidential. An example would be machines or robots in which sensors are embedded and that collect data in the factory of an industrial customer. As part of a confidentiality agreement, the latter can request the supplier of these devices to guarantee that others, especially competitors of the user of the device, be excluded from access to that information.[392] Based on such an agreement, the supplier may well have to take specific measures to prevent access to the relevant data by third parties on behalf of the customer. This shows that the holder of a trade secret, in certain circumstances, can also be another person than the holder of the raw data (typically the manufacturer of the connected device) in which the trade secret is encoded.

In contrast, consumers using connected devices cannot be considered holders of trade secrets. They may however be obliged by the manufacturers to safeguard confidentiality where manufacturers provide access to the data collected by the device to the individual consumer. Hence, if the manufacturer grants the user access to the data, this does not automatically have to exclude trade secrets protection for the manufacturer.

---

[390] See also Aplin (n 379) 68.

[391] On those uncertainties see Aplin (n 379) 69.

[392] Since the manufacturer of the machine still controls access to the data, the operator of the factory and the manufacturer of the connected machine can be considered co-holders of the data as trade secrets, as also argued by Wiebe (n 102) 880.

In addition, where data is generated and processed in larger networks, which will be frequently the case in sectors where devices 'communicate' with each other, identifying the person(s) controlling the data can be particularly difficult and undermine the usefulness of trade secrets protection as a protection system.[393] Therefore, where different players cooperate in building up data-processing and data-sharing platforms, they should take care of their confidentiality concerns through contractual means as part of their data governance und additionally use technical protection measures to keep the data secret. In such instances, data as trade secrets will have to be considered as being 'co-held' by several players.

c) The scope of protection

In particular, it is the scope of protection that distinguishes trade secrets protection from intellectual property. Trade secrets protection only provides 'defensive' rights against unlawful acts, but no exclusive rights in the use of the information.[394] When the information loses its secrecy, the former holder of the secret can no longer claim protection. Hence, trade secrets protection does not give rise to exclusive property rights in the information. Rather, it only aims to safeguard the secrecy of the information.[395] Yet trade secrets protection adds a legal layer of tort protection to *de facto* data holding, where the requirements of trade secrets protection are fulfilled.

This concept is implemented in the Trade Secrets Directive. The recitals of the Directive explicitly state that 'the provisions of the Directive should not create any exclusive right to know-how or information protected as trade secrets'.[396] Therefore, the Directive refrains from stipulating any 'rights' of the holder of the trade secret. Rather, the Directive only distinguishes lawful and unlawful conduct in form of acquisition, use and disclosure of a trade secret in Articles 3 and 4. Unlawful conduct empowers the competent judicial authority, upon request by the applicant[397] or the injured party[398], to grant certain remedies. This concept is also followed in Article 7 on 'exceptions', which are not formulated as exceptions and limitations to rights, but as an obligation of the Member States to ensure that the competent judicial authority will not take any measures in such cases. Hence, the core of EU trade secrets legislation is to be found in the definition of unlawful conduct. Yet, Article 3 of the Directive first defines which acquisition, use and disclosure will be considered lawful before Article 3 turns to the definition of unlawful conduct

Article 3 Trade Secrets Directive confirms that the holder of the trade secrets does not 'own' the underlying information. According to Article 3(1)(a), if another person makes a parallel and independent discovery, the holder of the trade secret cannot prevent this person form using this information according to Article 3(1)(a) of the Directive.[399] Unlike patent law, there is no principle of priority in the sense that only the first inventor applying for a patent qualifies for protection.

A particularly strong argument that a trade secret is not 'owned' by its holder can be found in Article 3(1)(b)[400], which allows reverse engineering of a product or object for the purpose to acquire the

[393] See also Wiebe (n 102) 880.

[394] See also Zech (n 44) 140.

[395] Dorner (n 26) 623; Wiebe (n 102) 880.

[396] Recital 16, 1st sentence, Trade Secrets Directive.

[397] Art 12(1) Trade Secrets Directive (on injunctions and corrective measures).

[398] Art 14(1) Trade Secrets Directive.

[399] See also Recital 16, 2nd sentence. Zech (n 380) para 26, seems to criticize this, by arguing that trade secrets protection remains 'incomplete'.

[400] In this sense also the reasoning of the German Ministerial Bill for the implementation of the Directive of 19 April 2018: Regierungsentwurf des Bundesministeriums der Justiz und für Verbraucherschutz—Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie

trade secret. The purpose of this provision is exactly to enable access and use of the trade secret by others to promote innovation through dissemination of technical knowledge.[401] This rule will not apply, if the product or object was made available to the public or the product or object is lawfully in the possession of the acquirer unless this person is under a legally valid duty to refrain from acquiring the information.

Particular effort to achieve a fair balance of interest is also expressed by Article 3(1)(d) of the Directive. This provision grants the judge enormous flexibility by stating that 'any other practice which, under the circumstances, is in conformity with honest commercial practices' should be allowed. Here, the Directive integrates EU trade secrets protection into a broader unfair competition law framework, whereas protection under intellectual property law is not limited to cases of 'unfair' use.

Moreover, Article 3(2) of the Directive explicitly states that the acquisition, use or disclosure of trade secrets shall be considered lawful to the extent that this is allowed by Union or national law. This provision gives precedence to any other legal provision over the Directive.

Pursuant to its Article 4(1), the Trade Secrets Directive provides protection against unlawful acquisition, use or disclosure of trade secrets. Then, Article 4 distinguishes between unlawful acquisition in its paragraph 2 and unlawful use and disclosure in paragraph 3. Furthermore, Article 4(4) and (5) extent protection to certain acts committed by third parties who have not themselves violated a trade secret in the sense of Article 4(2) or (3) but knew or should have known that the trade secret was violated.

Finally, Article 5 Trade Secrets Directive provides for four exceptions, namely, (a) for exercising the fundamental right to freedom of expression and information; (b) revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest (thereby guaranteeing the trade secrets protection cannot be used against whistleblowing)[402]; (c) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions; and—again providing flexibility to judges—for the purpose of protecting a legitimate interest recognised by Union or national law.

From the perspective of the data economy, the question is how robust and appropriate this framework is to provide sufficient protection to data holders without producing unwanted restrictions to free flow of data.

At the level of the creation and collection of information, Article 3(1)(a) of the Directive guarantees that anybody can independently create the same kind of information. This seems particularly important for dynamic data, which is only publicly available at a given moment at a particular location. Where several connected devices register such data, the individual manufacturers can use them without violating the trade secrets of any other manufacturer. The underlying (identical) information can constitute a trade secret for each of the manufacturers.

The provision on reverse engineering in Article 3(1)(b) could be read in the sense that it also allows the user of a connected device to circumvent technical protection measures implemented by the manufacturer to get access to the data stored in the device. This could conflict with the interests of the manufacturer to commercially exploit the data in its own interest. Here, the provision allows the

rechtswidriger Nutzung und Offenlegung, p 23 (commenting on Sec 2(2)) available at: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_GeschGehG.pdf;jsessionid=F730E2554199EE0259D9EB70F7F9A8E4.1_cid297?__blob=publicationFile&v=1 (accessed 31 July 2018).

[401] Recital 16, 3rd sentence, Trade Secrets Directive.

[402] See also Recital 20.

manufacturer to use contract terms that would prevent the purchaser of connected device to get access to the data.

Article 4(2)(a) of the Directive provides protection against 'unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced'. In the case where the manufacturer has designed a connected device in such a way that the data stored in the device is protected against access and, thereby, can control access, this provision will protect the manufacturer, in the case that this manufacturer is the holder of the trade secret, against misappropriation by any third person. This provision thereby strengthens the *de facto* exclusivity position of the manufacturer as a data holder by adding a layer of legal protection.

Article 4(3) extends legal protection against use and disclosure of such the trade secret, without the consent of the holder of the trade secret, against anybody who has unlawfully acquired the trade secret or breaches any contractual duty to limit the use or—typically based on a confidentiality agreement—not to disclose the trade secret. In the data economy, this provision is helpful in two regards: first, where the commercial user of a connected device is the trade secret holder, such as a manufacturer using connected devices in a factory, this provision grants protection against the manufacturer of the device against any unauthorized disclosure of the trade secrets. Second, where the manufacturer is the holder of the trade secret, this allows imposing confidentiality obligations and use limitations whenever access to the data is granted to third persons for the purpose of commercialising the data collected through connected devices.

While it can be argued that Article 4(3) does not add much to anyhow available protection through contract law, this provision is, pursuant to Article 4(4) and (5) of the Directive, nevertheless important as a basis for protection against third persons that are not directly bound by such contractual duties.

Article 4(4) of the Directive addresses the case of acquisition, use or disclosure of the trade secret by a third person if, at the time of the acquisition, use or disclosure, this person knew or ought to have known that the trade secret had been obtained directly or indirectly from a person who was using or foreclosing the trade secret unlawfully within the meaning of Article 4(3). Without trade secrets protection, the holder of the trade secret would not have any direct claim against such third person. In a digital context, Article 4(4) could indeed be of great relevance, since machine-generated data is frequently shared through data-sharing platforms. As in the case of personal data, it can be argued that also trade secrets have become much more vulnerable in the advent of the digital economy and, thus, Article 4(4) is most important to protect against expansive dissemination of trade secrets. On the other hand, liability of third people is problematic from the perspective of free flow of data. Yet it seems that with the knowledge requirement in Article 4(4) the Directive strikes an appropriate balance. To show that a third party that was granted access to data through data sharing should at least have known that the trade secret was obtained from a person who acted in the sense of Article 4(3) will be very difficult and often prevent holders of trade secrets to claim protection against third persons.

With Article 4(5), the Directive creates very broad scope of protection of trade secrets by extending production to 'infringing goods'.[403] Pursuant to this provision unlawful use can also consist in the 'production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes (...) where the person carrying out such activities knew, or ought, under such circumstances, to have known that the trade secret was used unlawfully within the meaning of paragraph 3'.

[403] Aplin (n 379) 70, considers this protection as 'potentially excessive'. See also Tania Aplin, A Critical Evaluation of the Proposed EU Trade Secrets Directive' (2014) *Intellectual Property Quarterly* 257, 268-69.

This provision creates problems of interpretation especially in the digital context. According to Article 2(4) of the Directive, 'infringing goods' are defined as 'goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed.' In this English version, the term 'good' seems to be understood as a manufactured item. However, the French and German versions use terminology—'*bien*' and '*Produkt*'—which seem to indicate that the concept of good could be understood more broadly.[404] In particular, in the light of the objective of Article 4(5), nothing seems to argue against applying this provision to 'digital goods', such as computer programs or digital versions of other copyright-protected works. Hence, the provision could apply to the distribution of such digital goods through Internet downloads too.

Yet, from the perspective of the data economy, the most important question is whether new information can also constitute an 'infringing good'. If this was to be answered in the affirmative, Article 4(5) could be applied to data analytics as a 'production process' in the meaning of Article 2(4) of the Directive. In principle, such reading would respond to the very objective of this form of protection. Requiring that use of the trade secret 'significantly benefits' the production of the good instead of making it an indispensable condition, Article 2(4) clarifies that the scope of protection is meant to be wide. Access to a particular dataset that contains information qualifying as trade secrets is not necessarily indispensable for producing new insights. But to make the counter-argument that analysis of the information contained in a particular dataset did not 'significantly benefit' the generation of new insights, unless these insights are rather self-evident, seems practically excluded.

Where big datasets are analysed and, based on empirical probabilities, new information is generated, application of Article 4(5) would in fact prohibit not only the 'production'—hence, the analysis as such—but also the 'offering or placing on the market of infringing goods'. This could be understood to include the use of the information for commercial information services on the Internet or sharing of such new data on data sharing platform. Moreover, the definition of an infringing good in Article 2(4), using the term of 'significantly benefiting', does not seem to exclude indirect use of the information as trade secrets where big data analyses run through different stages s. This would correspond to the case that unlawfully disclosed know-how was first used to produce an intermediary product by a third person to be then used by another manufacturer as an input into the production of final product. Whether this final product will be considered infringing will only depend on the threshold for a 'significant benefit' and knowledge of the manufacturer of that product.

This has to raise the question whether such interpretation does not excessively restrict freedom of information. However, since Article 4(5) of the Directive only applies where the person engaging in the production, offering or placing on the market of infringing goods knows or ought to know that there was unlawful use of the trade secrets in the sense of Article 4(5) of the Directive, the impact of the application to big data analyses may be rather limited. It is also to be noted that, in conformity with the general pro-competitive objective of trade secrets protection, the purpose of Article 4(5) is also to prevent commercial free-riding on the trade secrets of others where the free-rider should at least have known that it made direct or indirect use of a trade secret.

[404] In French, '*bien*' can be any tangible or intangible asset. In German, a '*Produkt*' is typically broadly understood in the sense of the English term 'goods and services'; 'good' is typically translated as 'Ware', which is understood as a tangible object of trade.

d) Remedies

The effectiveness of trade secrets protection depends on the availability of adequate remedies and their enforcement. In this regard, only a few remarks seem appropriate since the data economy does not present substantially different challenges.

On the one hand, the Directive is designed to promote access to justice by implementing procedural safeguards that the confidentiality of trade secrets will be preserved in legal proceedings (Article 9 Trade Secrets Directive). Conversely, also in the remedies part, the Directive aims to implement precautions to guarantee that protection does not go too far and that a fair balance of interests will finally be reached.

In particular, Article 7(1)(a) stipulates a general principle of proportionalities as regards procedures and the measures and remedies that a court may grant. Much more concretely, Article 7(2) obliges the EU Member States to provide for procedures that allow the respondent to seek remedies, such as damages, where claims based on trade secrets protection are manifestly unfounded and proceedings have been started abusively and in bad faith.[405] In Article 12, the Trade Secrets Directive obliges Members States to guarantee that the competent judicial authority, in case of unlawful conduct, 'may' order corrective measures of an injunction. In contrast, the word 'may' in missing in the corresponding text of Article 14(1) on ordering damages. Hereby, the provisions do not merely reproduce the wording of the IP Enforcement Directive.[406] These rules could also be understood in the sense that, in conformity with the Common Law tradition that injunctive relief as an equitable relief is not automatic,[407] a court may well have discretion when deciding on the grant of injunctive relief at least in applying the proportionality test. This reading corresponds to the belief that injunctions against violations of intellectual property rights, and maybe also in cases of trade secrets infringements, can be sought abusively with the intention to either exclude competitors from the market or to extract excessive royalty rates (so-called 'hold-up').[408] This may help the CJEU recognise a European *eBay* rule in the future without having to make a distinction between intellectual property law and trade secrets protection. Accordingly, this shows that injunctive relief will, in principle, not more easily be available in case of trade secrets infringements than in intellectual property cases.

e) The interface with data protection

Another question of great importance regards the interface of personal data protection and trade secrets protections. Whenever connected devices generate data, such data will often include personal data of the user. The question is whether such data can also constitute trade secrets under EU rules and, if answered in the affirmative, how the rules of the two protection systems will interact.

Against the backdrop of the definition a trade secret in Article 2(1) Trade Secrets Directive nothing argues against considering personal data as potential trade secrets of the manufacturers of connected devices. Since the kind of information is not limited to any kind of data, information that

[405] Art 3(2) IP Enforcement Directive (n 120), reproducing parts of Art 41(1) WTO/TRIPS Agreement, also mentions the principle of proportionality and requires Member States to provide for safeguards against abuses, but does so by remaining very general and giving the importance of these principles much more weight in the general structure of the Directive.

[406] The same wording can be found in Art 11 and 13 IP Enforcement Directive (n 120).

[407] See, in particular, *eBay Inc. v. MercExchange, LL.C.*, 547 U.S. 388 (2006) (establishing a test of four cumulative factors that need to be fulfilled for an infringement being granted also in intellectual property cases).

[408] While US courts also apply the so-called eBay rule to control injunctive relief sought by the holders of standard-essential patents, the CJEU preferred to correct such claims by relying on competition law. See Case C-170/13 *Huawei* ECLI:EU:C:2015:477.

can qualify as a trade secret is not upfront limited to non-personal information. In addition, the three requirements for trade secrets protection may easily be fulfilled. Specific personal data collected by connected goods may also be known by other persons and entities, but this does not necessarily mean that data is therefore automatically generally known or readily accessible in the sense of Article 2(1)(a) of the Directive. In addition, especially customer data may be of considerable commercial value for firms of the digital sector, especially if they (also) generate income from advertising services to customers by keeping such data secret in the sense of Article 2(1)(b). Finally, the third and last criterion according to Article 2(1)(c) will also typically be fulfilled, since, also as a matter of data protection law, the manufacturer as a data processor will take measure to guarantee data security and confidentiality.[409] To conclude, this result shows that especially datasets with customer data will typically be covered by trade secrets protection.

The fact that both forms of protection can coincide seems to be confirmed by Recital 35 of the Directive where it is explicitly stated that the right to 'protection of personal data of any person whose personal data may be processed by the trade secret holder when taking steps to protect a trade secret, or of any person involved in legal proceedings concerning the unlawful acquisition, use or disclosure of trade secrets under this Directive, and whose personal data are processed, be respected'. In this context, personal data protection is only addressed from the perspective of the holder of a trade secret who, simultaneously, will be the processer of personal data of others. This will typically occur when the same piece of information is part of the personal data processing and part of the trade secrets that the data processor is trying to protect.

In addition, data protection and trade secrets protection do not necessarily conflict. To a large extent, the trade secrets protection and the remedies available to the manufacturer of a connected device as the holder of a trade secret may indirectly benefit the users of such a device with regard to their personal data. If somebody misappropriates the trade secrets of a manufacturer of connected devices and thereby gets access to the personal data of the users of such devices and then starts to use this data, this person will typically fulfil the requirements of a data controller in the sense of Article 4(7) GDPR and, thereby, become an addressee of the obligations under the GDPR. As a starting point, the processing by another person who has infringed the trade secret will hardly ever fulfil the requirements for legal processing under Article 6(1) GDPR. In particular, this person will often not have received consent from the data subject according to Article 6(1)(a) GDPR. In any instance, the data subject can at any time claim to erase the personal data. Yet the problem is that the data subject will oftentimes not get to know that another person had access to her data and is processing it. Although under a duty to inform the data subject pursuant to Article 14 GDPR, it will be more common than not, that the infringer of the trade secret will not fulfil this information duty. Conversely, the manufacturer of a connected device whose trade secret regarding personal data collected through connected devices got violated is more likely both to detect the infringement and to sue the infringer. The remedies of trade secrets protection have a deterring effect on potential infringers and thereby may contribute to the data security the holder of the trade secret has to provide to the data subject under the data protection rules. Conversely, the fact that the GDPR has increased the rights of the data subject and the fact that, in case of detection, the infringer would also have to face infliction of fines as a matter of personal data protection, will similarly increase the changes of deterrence also in the interest of the holder of the trade secret.

Still, conflicts between the two regimes are not fully excluded, but can be solved. If at all, conflicts can only arise from the rights the GDPR vests in the data subject. The right to erasure (Article 17 GDPR) goes against the economic interest of the holder of the trade secrets to maintain the integrity of the data under its control. Yet, since trade secrets does not protect the integrity and existence of the data on the semantic level, but only against unlawful acquisition, use and disclosure, no legal conflict exists. Such conflict may more easily be confirmed if the data subject claims the right of access to data pursuant to Article 15 GDPR or the right to data portability according to Article

[409] See Art 5(1)(f) GDPR (n 23).

20 GDPR. The reason is that both Article 15(4) and 20(4) GDPR seek to guarantee that the 'rights and freedoms of others' be not negatively affected. According to the recitals to the Regulation[410], this wording is meant to include trade secrets. But it is not that clear whether also the data processor or only third persons can claim respect of their rights and freedoms under these rules.[411] Moreover, the Recitals of the Trade Secrets Directive argue exactly the other way around, namely, in favour of giving precedence to the data protection laws.[412]

f) Recognition of defensive rights similar to trade secrets protection

In the context of the European Data Economy Communication of 10 January 2017, the Commission staff also discusses potential introduction of 'defensive rights' framed according to the legal regime established by the Trade Secrets Directive as an alternative to a data producer's right as a right *in rem*.[413]

The cornerstone of such defensive rights are as follows: first, the Commission staff considers these rights as 'elements' of a right *in rem*[414], or, in other words, as a 'carve-out' of an exclusive data ownership right. Similar to trade secrets protection, these defensive rights should only provide the rightholder with the possibility to sue other parties in case of misappropriation of the data.[415] Hence, the substance of these rights would consist in a right to claim injunctions against use of the data as well as against the commercialisation of products built on the basis of such misappropriation[416] and, finally, a right to claim damages.[417]

Secondly, these defensive rights seem to differ from the concept of trade secrets protection to the extent that, following the concept of the data producer's right as a right *in rem*, such defensive rights would only protect machine-generated raw data as their subject-matter and not information on the semantic level. This could well mean that such defensive rights could overlap with trade secrets protection by protecting the same data, but the two systems would do so on the different—the syntactic and the semantic—level of the data. The defensive rights also seem to be more easily available since their coming into existence would only depend on the fact that they are machine-generated without any need to fulfil the legal requirements of a trade secret. The only limitation that seems to exist is that such rights would not be granted where the machine-generated raw data encodes personal data, which obviously would raise legal uncertainties against the backdrop of the difficulties to distinguish between personal and non-personal data.

Thirdly, the Commission is not very consistent with respect to who the holder of such defensive rights should be. On the one hand, the Commission conceives the right as a layer of legal protection for the *de facto* data holder.[418] These rights are characterized as legal protection of *de facto*

[410] Recital 63 GDPR.

[411] On the conflict with a sui generis database right of the manufacturer of a connected device, see at 4.2 j) above where it is argued that the two provisions should be interpreted in the sense of only preserving the rights and freedoms of third persons, excluding those of the data processor.

[412] Art 35 Trade Secrets Directive.

[413] European Data Economy SWD 2017 (n 9) 33-34. These 'defensive rights' are not explicitly mentioned in the European Data Economy Communication 2017 (9). On the concept of such 'defensive rights' the Commission is using here, see also the analysis by Kim (n 8) 702-703.

[414] European Data Economy SWD 2017 (n 9) 33.

[415] Ibid, 33-34.

[416] The Commission does not specify whether such product could also consist in 'information' generated through data analyses. On the interpretation of the Trade Secrets Directive see at sub-part c) above.

[417] European Data Economy SWD 2017 (n 9) 34.

[418] Ibid, 33.

'possession' rather than an expression of data 'ownership'.[419] On the other hand, it is hard to understand how such rights of the *de facto* holder can be considered as an alternative to the data producer's right as a right *in rem*, since the text of the Communication is very clear in its choice to vest this right in the 'owner or long-term user' of the connected device[420], with the expectation that such right would provide this person with access to the data typically controlled by the manufacturer. Hence, it is the manufacturer who, in the context of data generated by connected devices will typically be regarded as the *de facto* data holder exercising *de facto* control over access to the data.

The evaluation of the suitability of such defensive rights has to occur against the backdrop of the objectives of such rights. The Commission claims that such rights could enhance the sharing of data.[421] Indeed, the Commission has a point, since the sharing of data with others increases the risk of misappropriation. Hence, creating additional legal protection against misappropriation could conversely enhance the willingness of *de facto* data holders to share data. This may explain why the Commission considers vesting the defensive rights in the *de facto* data holder. In contrast, the owner or long-term user of a such a right is not *per se* technically capable of sharing the data with others. First and foremost, the owner or long-term user of a smart device will also be in need of access to the data. Defensive rights allocated to the owner of long-term user of the device cannot provide such access to this person against the *de facto* data holder. Rather than a substitute, such defensive rights can therefore at best work as a complement to data access rights.

However, the question whether such defensive rights against misappropriation can be considered appropriate has to be answered in the negative for both the manufacturer and the owner or user of a connected device, but for slightly different reasons.

With respect to the manufacturer, the question has to be asked whether there is a need for such protection in the first place, given the fact that the manufacturer could already rely on trade secrets protection. Of course, defensive rights against misappropriation of raw data would be automatically available without the need to show that the raw data contains a trade secret. But this is a problem rather than an advantage. Automatic protection of machine-generated raw data without the need to meet the requirements of trade secrets protection, especially a showing of economic value resulting from the fact that the information encoded in the raw data is secret, would undermine the balance pursued by trade secrets protection between the commercial interests of the holder of the trade secrets and the interest of the public in freedom of information. Trade secrets protection would not work as a role model for a new form of protection against misappropriation. Rather, it would be pushed aside as irrelevant by automatic availability of the same remedies without any further requirements for protection of the data. The intention to concentrate these defensive rights on raw data will be of no help. Protection cannot be concentrated on the syntactic level without negatively affecting the free flow of innovation on the semantic level.[422] Third parties will only seek access to and use of raw data, because they are interested in the information encoded in the data. Injunctions against further use of the raw data will necessarily prevent the other party from getting access to and using the information contained in the data. The right to exclude the commercialisation of a product based on the argument of misappropriation of data, as proposed by the Commission Staff,[423] has as its purpose to create sanctions against the use of the information

[419] Ibid, 34.

[420] European Data Economy Communication 2017 (9) 13.

[421] European Data Economy SWD 2017 (n 9) 33.

[422] See also Aplin (n 379) 68; Kerber (n 2) 997.

[423] European Data Economy SWD 2017 (n 9) 34.

contained in the raw data that was used for manufacturing other products.[424] In addition, it should not be overlooked that the remedies under a 'defensive rights regime' are not different from the 'defensive rights' that intellectual property systems grant in case of an infringement. The reason why trade secrets protection is much less intrusive than intellectual property rights is not primarily to be found in its character as a tort law regime, but much more in the fact that it does not provide remedies against all cases of use of the trade secret. In particular, protection is only granted where the information is used and disclosed by violating duties of confidentiality; and protection as such can be lost by the mere fact that the information becomes publicly available.

The situation of the owner or user of a connected device holding such defensive rights would be very different. In particular, such a person cannot rely on trade secrets protection. Yet where a third party appropriates and uses personal data collected by a connected device, the data subject—in many cases the owner or user of the device—will be able to rely on the rights granted under EU data protection rules. Hence, defensive rights will at best be able to fill a gap with respect to non-personal data. However, in this regard, the question is whether appropriation of such data will produce any injury to the owner or user of a connected device, since neither any privacy interest nor any property right will be negatively affected. The situation of the consumer is very different from the situation of the manufacturer, who has a commercial interest in protecting the secrecy of certain information as a basis of its competitiveness in the market. In some instances, a consumer may also have to rely on access and use of the non-personal data generated by connected devices, for instance, to link household devices to enable smart homing. But use of the same non-personal data by third parties will not restrict the consumer in pursuing this interest. Nor are defensive rights of the owner or user really needed by the owner or a user of a connected device to unlock the data generated by such device. Such effect can already be achieved through data access rights that provide the owner or user of a device with a claim against the manufacturer to grant access to the data also to a third person designated by the owner or user.

In sum, the idea of introducing defensive rights against misappropriation has to be rejected. Trade secrets protection suffices to provide appropriate and balanced protection against misappropriation of the information contained in the data. In contrast, defensive rights against misappropriation of machine-generated raw data would undermine the system of trade secrets protection and unjustifiably restrict freedom of information.

g) Comparing sui generis database rights, trade secrets protection and defensive rights against misappropriation in practice

To conclude the analysis of trade secrets protection, in the following analysis the Study will compare how the three protection systems—sui generis database rights, trade secrets protection and defensive rights against the misappropriation of raw data differ in their practical application. This will be done against the backdrop of the *Autobahnmaut* case, where the German Federal Supreme Court confirmed a violation of a sui generis database right.[425] The facts are very suitable to analyse the case also from the perspective of the other two protection system.

In *Autobahnmaut*, the data collected by the terminals of Toll Collect on the use of German motorways by lorries has to be considered as highly sensitive. Since Toll Collect is registering the number plates of the lorries as well as where and when the lorries enter and leave the motorways, the data treated by Toll Collect has the character of data that relates at least to 'identifiable' natural

[424] Equally critical on the remedies in case of misappropriation, Kim (n 8) 702-703 (arguing that such protection would in fact correspond to very broad ownership protection).

[425] See at 4.2. c) above.

persons, namely, the operators and the drivers of the lorries.[426] Conversely, it is not that clear whether the data also constitute a trade secrets of Toll Collect. The collection of the data constitutes the core of Toll Collect's business. But the question is whether this data has economic value and whether this is so because Toll Collect keeps it secret. The argument against this is that the competitiveness of Toll Collect does not depend on the secrecy of the data that is collected. Toll Collect acts as an exclusive service provider to the government of Germany. Hence, Toll Collect's activity takes place in an environment of public procurement, where firms compete prior to the service contract in the framework of a public tender. This procedure may be repeated for the time after the service contract expires. To win a public tender, it is not the billing data that matters, but the technology and business method for collecting the data which enables Toll Collect to submit a superior offer to the German government. This already shows that the defendant in *Autobahnmaut* was certainly using data originating from Toll Collect, but its business did not negatively affect the business opportunities of Toll Collect. The analysis based on the sui generis right looks very different. The only argument there is that Toll Collect has acquired an intellectual property right and, hence, in case of an infringement, Toll Collect can claim injunctive relief and damages.

In addition, trade secrets protection would only be available in *Autobahnmaut* if the credit card company or the defendant as a partner of the issuing company were under a contractual duty of confidentiality. Only then the defendant could be considered an infringer either in the form of a direct of indirect infringer of the trade secret of Toll Collect according to either Article 4(3)(b)—in the case of a direct duty of confidentiality—or Article 4(4) Trade Secrets Directive under the condition that he knew or ought to have known that the disclosure to him by the payment card company breached a duty of confidentiality.

Even if the data was considered a trade secret and if the defendant had acted unlawfully in the sense of Article 4(3)(b) or 4(4) Trade Secrets Directive, liability can still be excluded pursuant to Article 3(1)(d) Trade Secrets Directive, if the conduct by the defendant can be considered honest commercial practice. This provision requires the judge to enter into a broader weighing of interests. It is argued here that such weighing should be conducted in the framework of the regulatory theory described in Part 3 of this Study. Trade secrets protection is located at the interface of innovation and public interest. On the one hand, this form of protection seeks to create incentives for innovation, but especially Article 3 of the Trade Secretes Directive provides for a framework that takes the public interest in guaranteeing legitimate access to information into account. Already against the backdrop of these two considerations, the interests of the defendant should prevail. In fact, it is the defendant that provides an innovative information services (daily updates on the billing information) that the plaintiff did not want to provide.[427] Hence, granting protection would restrict innovation rather than promoting it.[428] In addition, also the other two policy objectives argue in

[426] On the data protection rules applicable to the operation of Toll Collect, 'Datenschutz und Sicherheit' (2018) available at: https://www.toll-collect.de/de/toll_collect/service/fragen___antworten/datenschutz___sicherheit/fragen___antworten_zu_datenschutz___sicherheit.html (accessed 30 April 2018).

[427] This is in line with the unfair competition judgment of the German Federal Supreme Court in *Hartplatzhelden*. In the underlying case, financed through ads, a website operator provided the possibility to upload private videos of adolescent football players scoring goals. The operator was sued by a regional football association on the basis of the German Act against Unfair Competition making the argument that the Internet operator was free-riding on the investment of the football association in organising the football matches. The Court rejected this claim by arguing that the association could have operated its own websites of same kind. If the association decides otherwise, it will not be able to argue an act of misappropriation. See Federal Supreme Court of 28 October 2010, Case I ZR 60/09 *Hartplatzhelden* [2010] 187 BGHZ 255. This case stands for a restrictive approach to grant protection against misappropriation as a matter of unfair competition law. See also Ansgar Ohly, 'Hartplatzhelden.de oder: Wohin mit dem unmittelbaren Leistungsschutz?' (2010) *Gewerblicher Rechtsschutz und Urheberrecht* 487.

[428] The case also shows great resemblance with the competition law case of the CJEU in *Magill* (n 554). It is obvious that the information held by Toll Collect was an essential input for the business of the defendant. By suing the defendant for an infringement, Toll Collect as a right holder excluded the defendant from remaining in the market and prevented the emergence of a new product (the daily updates) to the detriment of consumers. Unfortunately,

favour of the defendant. First, an injunction based on potential trade secrets protection is not needed to make markets work. The plaintiff is anyhow paid for its service by the German government and therefore can recoup the whole of its investment in running its business.[429] Secondly, personal data protection is certainly a side aspect of this conflict. But the privacy concerns of the persons concerned are fully respected. The operators of the lorries are informed that the defendant has acquired access to the data and therefore can rely on all their data protection rights. More importantly, the lorry operators, who are also the data subjects in terms of the GDPR, are the recipient of the innovative service and, hence, are interested in keeping the defendant in the market.

Under 'defensive rights' protecting against misappropriation of raw data, as considered by the Commission Staff, the results of the case would not necessarily differ from the judgment of the Federal Supreme Court, unless the legislation includes fairness conditions following the example of Article 3(1)(d) Trade Secrets Directive. Even worse, since the plaintiff would neither have to prove that the data constitute a database and that there was substantial investment, protection would become practically automatic.

Hence, practical application shows that a balanced approach to applying the Trade Secrets Directive can produce results that are in line with the proposed regulatory theory, while sui generis database protection and defensive rights against misappropriation of raw data would lead to excessive protection, thereby restricting free flow of data without any justification.

h) Conclusion

The EU Trade Secrets Directive has not been specifically drafted against the backdrop of the challenges of the modern data economy. Despite the fact that the Directive constitutes most recent legislation, application of the Directive in a digital context will present difficult questions of interpretation. It will be for the CJEU to answer these questions and turn EU trade secrets protection into a useful element of the legal framework for the European data economy.

Yet the analysis shows that the provisions of the Directive can be applied in a fruitful and balanced way to provide a useful layer of legal protection of *de facto* data holders.[430] Trade secrets protection cannot only be claimed by the manufacturers of connected devices, but in principle also by commercial purchasers and users where these devices, especially if used for smart manufacturing, collect trade secrets held by these persons.

In sum, trade secrets protection, following the tradition of unfair competition law, strikes a better balance between the commercial interests in getting protection against misappropriation of information, on the one hand, and the public interest in safeguarding freedom of information, on the other.

---

neither the defendant nor the Federal Supreme Court considered whether reliance of Toll Collect on the sui generis database right restricted competition. The *Magill* judgment is also referred to by the Database Directive Final Evaluation Report as an argument in favour of introducing a compulsory licensing regime in the Directive. See Database Directive Final Evaluation Report (n 21) 35-36.

[429] The fact that the sui generis database right is recognised where the creation of the database is only a by-product of the main business and that, therefore, additional incentives for creating the database are not needed, is also criticised by others. See, for instance, Carsten König, 'Der Zugang zu Daten als Schlüsselgegenständen der digitalen Wirtschaft' in: Moritz Hennemann und Andreas Sattler (eds), Immaterialgüter und Digitalisierung (Baden-Baden: Nomos, 2017) 89, 100-102 (also criticizing protection in Case C-30/14 *Ryanair* ECLI:EU:C:2015:10 where protection of an airline for its database was directed against the operator of a price comparison platform).

[430] Against Becker (n 25) 254, who criticises trade secrets protection for its lack of transparency and inability to provide a sufficient legal framework for the exchange of data.

4.5 The rights of consumers in relation to data generated by connected devices

Concerning the rights of consumers in relation to data generated by connected devices, a distinction has to be made between absolute rights of control in form of property rights and data protection rights, on the one hand, and contractual rights, on the other.

a) Property rights

The preceding analysis of the control rights has demonstrated that in principle consumers do not hold any property rights in the data. Yet limited property rights can be identified. National law can provide tort law protection against the destruction of the data embedded in the connected device. Tort law claims of the consumer will be easier to be justified where the consumer is the owner of the connected device and the destruction of the data destroys or restricts the usability of the device. Depending on the case and the applicable law this may even be considered an injury caused to the property of the consumer in the device. National law may also recognise data that is deleted as proper subject-matter of protection of tort law. In Germany, where tort law liability in principle depends on the infringement of an absolute right, this leads to the discussion of whether data should at least be recognised as property for the purpose of protecting data integrity.[431]

The CJEU has recognised ownership of the person downloading a computer program in the data for the purpose of justifying copyright exhaustion, enabling this person to resell acquired digital copies of the program.[432] Today, it is still open whether the CJEU will extend digital exhaustion also with respect of other kind of copyrighted works, allowing consumers also to resell downloaded e-books, music, videos or computer games. The reason for this uncertainty is that exhaustion is addressed by different rules in the Computer Programs Directive[433] and the Information Society Directive.[434]

b) Data protection rights, including the data portability right

Apart from these limited property rights, the strongest rights of consumers concerning data generated by connected device arise from the data protection rules as provided for by the GDPR.[435]

---

[431] See at 4.3 c) above.

[432] *UsedSoft* (n 179). See also at 4.1 a) above

[433] Art 4(2) Computer Programs Directive (n 57).

[434] under the Information Society Directive (n 308), exhaustion is placed at the interface of the right of communication to the public in Art 3 and the distribution right in Art 4. Article 3(3) explicitly excludes exhaustion of the making available right, while Art 4(2) provides for exhaustion of the distribution right in basically the same way as Art 4(2) Computer Programs Directive. In *UsedSoft*, the CJEU regarded the provisions of Computer Programs Directive as *lex specialis* and, hence, left open how a similar case would have to be decided for other categories of works under the Information Society Directive. See *UsedSoft* (n 179) para 51.

[435] The consumer protection dimension of the data portability right is also highlighted by Van der Auwermeulen (n 114) 59-60; Wiebe (n 102) 878 (identifying data protection rules as 'part of consumer protection'). For a more detailed analysis of the interaction of data protection and consumer protection rules, see Natali Helberger, Frederik Zuiderveen Borgesius and Augustin Reyna, 'The Perfect Match? A Closer Look at the Relationship Between EU Consumer Law and Data Protection Law' (2017) 54 *Common Market Law Review* 1427; Phlipp Schmechel, 'Verbraucherdatenschutzrecht in der EU-Datenschutzgrundverordnung' in: Hans-Wolfgang Micklitz, Lucia A Reisch, Gesche Jost and Helga Zander-Hayat (eds), *Verbraucherrecht 2,0—Verbraucher in der digitalen Welt* (Baden-Baden: Nomos, 2017) 265.

The most important right with an economic connotation is the data portability right of Article 20 GDPR.[436]

The scope of application of the data portability right is limited in several regards. First, it only applies to personal data. Secondly, Article 20 only applies to data 'provided by the data subject' to the data controller, while other provisions of the GDPR apply to all personal data in whatever way the data controller has acquired the data. This latter limitation could be interpreted in two very different ways, namely, restrictively, in the sense of data the data subject has explicitly provided to the data controller, or, broadly, including all data that the data controller has collected with the consent of the data subject or in the framework of a contract.[437] The latter would also include 'observed' data.[438]

When Article 20 GDPR was adopted, the idea was that the provision should apply when users want to move their data from one online platform to another. Accordingly, the provision covers personal data that users have uploaded on the website of a social platform.[439] Application of the provision becomes especially doubtful in the case of data collected by connected devices, such as a fitness tracker or other smart wearables used for mobile health care, checking the bodily functions of a patient.[440] In the latter cases, the person may not be fully aware that and what kind of data is collected. A patient will typically know that she is wearing such a device; and in fact the data protection rules require her consent to collect personal data also in this case. But the outer limits of the wording of Article 20(1) GDPR are still difficult to be defined, such as in the case of a car controlling the physical fitness of the driver and interrupting the operation of the car even against the clear will of the driver. In these cases, the question is indeed whether data collected by a device can be understood as 'data provided by the data subject'.[441] In line with the abovementioned broad interpretation, the question should be answered in the affirmative.[442] Also in these cases there is an active element fulfilled by the data subject, namely, the consent given to the data controller for the data collection. More importantly, data portability is also needed in the case of data collected by connected devices. An obvious example would be a device embedded in a car that collects data on the driving habits of the driver; for changing the car insurer, the holder of the car will depend on the portability of the data to get a lower insurance premium.[443] Yet many of the devices will not store the data that is constantly generated and there is not always a legitimate interest of access of the user of the device to the data. To cater for such cases, it has therefore been proposed that a

[436] See at 4.1 above.

[437] De Hert et al (n 155) 199, while distinguishing these two readings, consider these as the only two possible interpretations. Yet, as will be demonstrated in the following, an intermediary interpretation should be adopted.

[438] Ibid, 199-200.

[439] Indeed, the Commission wanted to target the operators of social platforms in particular when it proposed the data portability right. See also Graef, Verschakelen and Valcke (n 114) 9. Yet control over the data of their users is considered a most crucial competitive parameter of social platforms according to Weber (n 95) 67.

[440] Examples also used by Janal (n 156) para 8.

[441] Ibid, para 9.

[442] Ibid, para 10 (also referring to Recital 60 GDPR where, in a different context, it seems that the legislature is considering data collected from the data subject as data that the data subject is 'providing' to the data controller). This broad reading is also supported by De Hert et al (n 155) 200.

[443] Car insurers offer special telematics tariffs. They grant reductions on the insurance premium if the holder of the car agrees to controlling certain features of the driving, such as whether he or she respects the speed limit, how much the person accelerates, how the driver uses the breaks, but also whether the car is more used in cities than outside of the cities and at what time. The latter is based on the experience, that more accidents happen in cities and during rush hour. All these data are personal data. See information delivered by the Cosmos insurance company on telematics tariffs, available at: https://www.cosmosdirekt.de/betterdrive/telematik-datenschutz/ (accessed 30 April 2018). See also Brian O'Connell, 'Telematics Could Cut Your Car Insurance, but There Are Privacy Risks', TheStreet (21 February 2018) available at: https://www.thestreet.com/story/14493364/1/telematics-could-cut-your-car-insurance-but-there-are-privacy-risks.html (accessed 30 April 2018) (reporting that some US insurers allow cuts of up to 50% if a telematics device is used to collect data on the driving habits).

proportionality test should be read into Article 20 GDPR with respect to data collected by connected devices to limit its scope of application.[444] Finally, this broad reading has also been confirmed by the Article 29 Data Protection Working Party, stating that data portability could also be claimed where personal data is merely 'observed'.[445] Yet such broad reading is not without limitations. As argued by the Working Party as well, the right to data portability does not extend to 'inferred' or 'derived' data that is generated by the data controller through the processing of the data.[446] This leads to a considerable limitation of the data portability right as regards access to machine-generated data that is generated by a connected device as of the first additional step of data processing.[447]

A third limitation results from technical difficulties linked to data portability. Article 20 GDPR only provides a right against the existing data processer to claim portability of the data in a 'structured, commonly used and machine-readable format and . . . to transmit those data to another controller'.[448] Where no such commonly used format exists, the data subject will have no right to claim data portability.[449] In its recitals, the GDPR only encourages data controllers to create interoperable data formats[450] and explicitly states that there is no obligation on the part of the data controller to adopt and maintain technically compatible processing systems.[451] These technically unavoidable limitations and the resulting need for standardisation of data formats has led commentators to characterise the data portability right a 'declaration of principle' rather than a 'real and effective tool for individual self-determination'.[452]

In addition, there is no right against the new data processor to accept such data either[453] and no guarantee that the new data processor is technically capable of accepting the data. Hence, the greatest impediment to data portability arises from insufficient data interoperability. This problem has also been addressed by the Commission in the 2017 European Data Economy Communication, where Part 5 only deals with data portability, interoperability and standards.[454] There, the Commission takes account of the existence of the data portability right as regards personal data, but justifies that such right is not (yet) available for non-personal data by the fact that data portability can be 'technically demanding and costly' and that 'different providers of the same services may store data differently'. This may explain why Commission so far seems very hesitant to

[444] Janal (n 156) para 10 (arguing that the data portability right should only be recognised where there is a legitimate expectation that the data will be available over time).

[445] Article 29 Data Protection Working Party, Guidelines on the Right to data portability (n 156) 10.

[446] Ibid. The Working Party's interpretation is broadly accepted in legal writing. See, for instance, De Hert et al (n 155) 200; Scudiero (n 334) 122-23; Lachlan Urguhart, Neelima Sailaja and Derek McAuley, 'Realising the right to data portability for the domestic Internet of things' (2018) 22 *Personal & Ubiquitous Computing* 317, 319.

[447] See also at 5.2 c) below.

[448] On these requirements, see Scudiero (n 334) 120.

[449] Ibid, 15. This is criticised as too permissive by Graef, Verschakelen and Valcke (n 114) 9-10 (indicating that the legislature should have created an obligation of the data controller to develop technical measures for the transmission of personal data). However, this criticism seems to overlook that such obligation would have been particularly burdensome for small and medium-sized enterprises (SMEs). Application of the data portability right to SMEs is otherwise seen critically by the same authors. Ibid, 9. In addition, data interoperability cannot be established unilaterally by the entity being obliged to grant data portability. It has to be agreed upon collectively to enable data portability in broader communities. See Van der Auwermeulen (n 114) 59 (with reference to the position of representatives of the private Data Portability Project).

[450] Recital 68, 2nd sentence, GDPR.

[451] Recital 68, 6th sentence, GDPR.

[452] Scudiero (n 334) 119.

[453] This is specifically highlighted by Janal (n 156) para 4.

[454] European Data Economy Communication 2017 (n 9) 15-17.

the idea to take inspiration from Article 20 GDPR as a template for additional data access rights.[455] Yet data interoperability will always be an issue whatever the legal framework for data access is.[456] This means that also a data producer's right as a legal instrument to promote data access cannot avoid technical barriers arising from lack of data interoperability.

As regards its scope, the data portability right of Article 20 GDPR is very broad in the sense that it can be claimed at any time. Therefore, the data portability right may in particular become relevant when the data subject wants to terminate a contract to switch to another supplier. But the data portability right does not depend on the termination of the underlying contract between the data subject and the data controller. For instance, Article 20 GDPR allows for data portability of historical data on the use of a connected device on which the data processor does not have to rely anymore for providing its service. An example would be transfer of the data collected by a fitness tracker to a medical doctor. Here, the data subject continues the contract with the supplier of the tracker, while she also wants to enable her doctor to have access to check past development of the data for diagnostic purposes.

The wording of Article 20 GDPR seems to indicate that the right to data portability only includes a right to 'transfer' the data to a new data controller. But, in the light of its objectives, the right should also cover a right to connect a new controller with the pre-existing controller for real-time sharing of data. Accordingly, the provision should not be read in the sense that the data subject must have 'provided' the data to the existing data processor and then data portability is claimed with respect to already collected data. Data portability may thus already be claimed *ex ante* to establish a data stream for the purpose of sharing data that a connected device will collect in the future. At least Article 20(2) GDPR make clear that the data subject can claim direct transmission of the data from one controller to another.

c) Towards a digital update of consumer contract law

From a consumer policy perspective, consumers should enjoy the same level of protection under consumer contract law whatever the object of consumption is. In this regard, the Commission has taken important steps to implement a 'digital update' of consumer contract law.[457] The first step was made with the proposal of two new directives in 2015, namely, for an Online Sales Directive[458] and a Digital Content Directive[459]. On 11 April 2018, the Commission has made another step by presenting the so-called 'New Deal for Consumers' initiative.[460] This initiative includes in particular a proposal for a reform of the Consumer Rights Directive[461].[462]

---

[455] See, in contrast, the Position Statement of the Max Planck Institute of 26 April 2017 (n 9) para 25.

[456] Note, however, that potential copyright protection for application programming interfaces (APIs) can create a legal barrier to data interoperability. On this, see at 4.3 a) above.

[457] For proposals on a potential digital update see also the contributions in Hans-Wolfgang Micklitz, Lucia A Reisch, Gesche Joost and Helga Zander-Hayat (eds), Verbraucherrecht 2,0—Verbraucher in der digitalen Welt (Baden-Baden: Nomos, 2017).

[458] Proposal of the Commission of 9 December 2015 for a Directive of the European Parliament and the Council on certain aspects concerning contracts for the online and other distance sales of goods, COM(2015) 635 final.

[459] Proposal for a Digital Content Directive (n 199).

[460] Communication of the Commission of 11 April 2018—A New Deal for Consumers, (COM)2018, 183 final. See, also, European Commission, 'A New Deal for Consumers: Commission strengthens EU consumer rights and enforcement', Press release of 11 April 2018, available at: europa.eu/rapid/press-release_IP-18-3041_en.htm (accessed 31 July 2018).

[461] Directive of the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer rules, [2011] OJ L 304/64.

[462] Proposal of the Commission for a Directive of the European Parliament and of the Council amending Council Directive 93/13/EC of 5 April 1993, Directive 98/6/EC of the European Parliament and of the Council and Directive 2011/83/EC of

These reforms touch upon rights that are most important for consumers in the digital environment. The adoption of the Digital Content Directive has the objective of introducing mandatory contractual liability for the non-conformity of digital content with the contract and, what is very important for this Study, at least according to the Commission's initial proposal, contractual portability rights of the consumer in the case of termination of the contract. The reform of the Consumer Rights Directive aims at extending the information duties and the right to withdraw from a contract to contracts on so-called 'free digital services' where consumers provide personal data instead of paying with money.[463]

The adoption of the Digital Content Directive has proven to be rather difficult. The legislative process has now reached the trilogue procedure where diverging positions of the Commission, the European Parliament and the Council need to be negotiated.[464]

The two key issues that are at dispute are of high relevance for connected devices. The overarching questions that arises both with regard to the Digital Content Directive and the Reform of the Consumer Rights Directive is to which extent these reforms should also be made applicable to connected devices, respectively to the data-based services linked to the use of these devices. This question is key for consumers purchasing or using connected devices to enjoy non-discriminatory consumer protection as regards the right to withdraw from a contract, remedies for the non-conformity of the product or service with the contract and contractual data portability rights in the case of termination of the contract. Instead of analysing these rights with respect to connected devices right away, the following analysis will first address the two overarching issues that are currently under discussion in the framework of European legislation with an emphasis on connected devices. These two issues are the need to extend consumer contract law to contracts where consumers do not pay with money but make data accessible to the other party[465] and the definition of the terms of 'digital content' and 'digital service' in the two proposed directives[466].[467] As regards the latter issue, the main substantive question is whether the consumer contract law should also be applied to cases of embedded software and embedded digital services.

d) Extension of consumer contract law to cases where data is provided as a counter-performance

The proposal of the Commission for a Digital Content Directive has caused a lot of debate and academic attention by introducing the concept that data can be considered a counter-performance for digital content.[468] According to Article 3(1) of the Commission Proposal, the

---

the European Parliament and of the Council as regards better enforcement and modernisation of EU consumer protection rules, COM(2018) 185 final.

[463] New Deal for Consumers Communication (n 460) 5. On this aspect, see also Helberger, Zuiderveen Borgesius and Reyna (n 435) 1442-49 (also discussing how especially the fact that no money is paid translates in applying the consumer protection rules, such as the standard of conformity with the contract).

[464] See the more recent position statement of the German Weizenbaum Institute for the Networked Society (German Internet Institute), which is also reporting on the different positions of the three EU institutions: Axel Metzger, Zohar Efroni, Lena Mischau and Jakob Metzger, 'Data-Related Aspects of the Digital Content Directive' (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce* (*JPIITEC*) 90.

[465] See at d) below.

[466] See at e) below.

[467] These two issues are also focused upon in the position statement of the German Weizenbaum Institute: Metzger et al (n 464) para 10.

[468] See, among others, Axel Metzger, 'Dienste gegen Daten: Ein synallagmatischer Vertrag' (2016) 216 *Archiv für civilistische Praxis* 817; id, 'Data as Counter-Performance: What Rights and Duties Do Parties Have?' (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce* 2.

Directive should also apply where the 'consumer actively provides counter-performance other than money in the form of personal data or any other data'. While this provision only defines the scope of the application of the Directive and, hence, does not provide for a rule that providing data has to be considered as a counter-performance as a matter of law, this proposal is nevertheless seen as a confirmation by the Commission that commercialisation of personal data is accepted.[469] This has given rise to the concern that such understanding may run counter or undermine the particular human-rights dimension of data protection. The European Parliament and the Council have taken up this concern proposing amendments to the Digital Content Directive that would avoid the term 'counter-performance'. Yet both institutions support the idea that the Directive should also be applied to contracts where the consumer does not pay with money but undertakes to provide personal data to the trader.[470] Proponents of maintaining the Commission's reference for the sake of guaranteeing a high level of consumer protection where data is commercialised in consumer contracts may nevertheless overlook that the term 'as a counter-performance', as compared to the Parliament's and the Council's position, could also be interpreted as an additional requirement that would make it harder to apply the Directive.[471] In the new proposal for reforming the Consumer Rights Directive, the Commission now seems to have accepted the milder wording preferred by the Parliament and the Council. For a new Article 2(16) Consumer Rights Directive, the Commission proposes that the right to withdraw from the contract should also apply to contracts on digital content where a 'consumer provides or undertakes to provide personal data to the trader', thereby avoiding the term 'counter-performance'.

As regards the case of connected devices, the question is not so much whether the supply of personal data can be considered a counter-performance. Rather, the question is whether excluding connected devices and the digital services linked to it from the scope of application of the two Directives would create a loophole in consumer contract law as regards connected devices. The answer to this question depends on whether there are or whether there could be business models where connected devices are supplied to consumers 'for free', while these devices extensively collect personal data from the users in the economic interest of the supplier. Proponents of the extension of the Digital Content Directive to software and digital services embedded in connected devices indeed hint at such scenarios, arguing that electronic devices will get constantly cheaper and that the growing market for data will increase incentives to distribute such devices without any monetary charge.[472]

An example at hand are businesses for the sharing of dockless bikes. Such businesses are able to collect large amounts of valuable data through the bike-sharing app and GPS devices installed in the bikes.[473] In the case of such bike-sharing, consumers may enter into long-term contracts without being able to assess the quality of the bikes and of the service. Hence, there seem to be good

[469] See also Metzger *et al* (n 464) para 13 (supporting this conclusion).

[470] See the comparison of the different positions for the wording of Art 3 in Metzger *et al* (n 464) 92. It is to be noted here that the proposals of the European Parliament and the Council are narrower than the one by the Commission by making the Directive only applicable to the provision of personal data, thereby excluding cases where the consumer only provides non-personal data.

[471] The argument could be that the provision of personal data cannot be a counter-performance where such data is needed to guarantee the consumer optimal use of a connected device, meaning that the provision of the data does at least not exclusively take place in the interest of the supplier of the device but also in the consumer's own interest.

[472] Metzger *et al* (n 464) para 31.

[473] Recent research shows that tracking data on the use of bikes can have a huge value for urban planning. At the same time, the data collected constitutes highly sensitive data (including credit cards numbers and geo-tracking of the users). See Christopher Pettit, 'They know where you go: Dockless bike sharing looms as the next disruptor—if key concerns are fixed', The Conversation (6 December 2017) available at: http://theconversation.com/they-know-where-you-go-dockless-bike-sharing-looms-as-the-next-disruptor-if-key-concerns-are-fixed-88163 (accessed 30 April 2018) (reporting on a study in Australian cities tracking 120,000 cycle journeys by 7,600 users over three-and-half years).

arguments to extend the legislation which is now proposed for contracts on digital content and digital services in the framework of the Digital Content Directive and the Consumer Rights Directive also to connected devices. To attain this objective, however, the European legislation would have to widen the scope of application of the two directives by opening up the concepts of 'digital content' and 'digital services'.

e) Extension of consumer contract law to embedded digital content and services

The key issue in the current debate is in fact whether digital content and services embedded in connected devices should be covered in the framework of the two reforms. In fact, in the framework of the two directives, the Commission has proposed an approach which appears too restrictive.

As regards the Digital Content Directive, according to the Commission, this Directive would only apply to contracts on digital content, whereby digital content is defined as

> (a) data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software,
>
> (b) a service allowing the creation, processing or storage of data in digital form, where such data is provided by the consumer, and
>
> (c) a service allowing sharing of and any other interaction with data in digital form provided by other users of the service; ...[474]

As spelled out in the explanatory memorandum to the Commission Proposal, this definition includes 'downloaded or web streamed movies, cloud storage, social media or visual modelling files for 3D printing, in order to be future-proof and to avoid distortions of competition and to create a level playing field'.[475] In the proposed Recitals, the Commission in fact pretends that this would create a broad definition of digital content for the purpose of guaranteeing that consumers are protected without discrimination whatever the digital object of the contract is.[476] But the Commission also states that the definition of digital content should exclude 'digital content which is embedded in goods in such a way that it operates as an integral part of the goods and its functions are subordinate to the main functionalities of the goods'.[477] While the question of when the functions of digital content are subordinate to the main functionalities of the good would compromise legal certainty, the Commission clearly intends to exclude software embedded in a connected device from the scope of application of the Digital Content Directive.

The more recent proposal for an amendment of the Consumer Rights Directive pursues a similar goal of providing non-discriminatory protection to consumers for all contracts concerning digital services irrespective of whether consumers pay with money or provide personal data.[478] But

[474] Art 2(1) Proposal for a Digital Content Directive. It is however to be noted that the final text of the Directive may well distinguish between the two concepts of 'digital content' in the sense of proposed Article 2(1)(a), on the one hand, and 'digital services' as mentioned in Art 2(1)(b) and (c), on the other. Such distinction is proposed by both by the European Parliament and the Council. See Draft European Parliament Legislative Resolution of 27 November 2017, Doc. A8-0375/2017, amendments proposed for Art 2(1) Digital Content Directive, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0375+0+DOC+PDF+V0//EN (accessed 30 April 2018). This distinction has now also been taken up by the Commission in its more recent proposal for reforming the Consumer Rights Directive. On this, see at g) below.

[475] Proposal for a Digital Content Directive (n 199) 11.

[476] Recital 11 Proposal for a Digital Content Directive.

[477] Recital 11, last sentence, Proposal for a Digital Content Directive.

[478] Commission Proposal (n 462) 3, 6 and 19. See, also, New Deal for Consumers Communication (n 460) 5.

according to the Commission's Proposal, digital services may only come in two forms: (1) as a service 'allowing the consumer the creation, processing or storage of, or access to, data in digital form'; or (2) as a service 'allowing the sharing of or any other interaction with data in digital form uploaded or created by the consumer and other users of the service, including video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media'.[479] The first case relates to cloud services, the second one to social and sharing platforms, such as Facebook and YouTube. Accordingly, the Recitals to the proposed Directive mention the following cases: cloud storage, webmail, social media and cloud applications.[480] Again, this seems to exclude software and data services embedded in a connected device. The extension to such free digital services is obviously explained by the objective of providing consumer with the possibility to test such services, which are typically provided for a longer period of time, before the contract becomes finally binding after the 14-days period granted for the withdrawal from the contract. Likewise, Article 16(m) Consumer Rights Directive in its current version excludes the right of withdrawal in the case of supply of digital content, such as a song, a video or a computer game, from the very moment the performance of the contract—through download or streaming—has taken place.

The question to be explored in the following is whether the exclusion of software and data-based services embedded in a connected device creates a loophole in consumer contract law. The question needs to be answered in the affirmative against the backdrop of the rules that would otherwise apply. The rules that would otherwise apply, namely, those of the Consumer Sales Directive[481] and the Online Sales Directive[482] do not provide sufficient protection.

Here, it is to be noted that adoption of Online Sales Directive is proposed by the Commission with the objective to increase consumer protection also as regards goods, such as household devices and toys, 'where the digital content is embedded in such a way that its functions are subordinate to the main functionalities of the goods and it operates as an integral part of the goods'.[483] It thereby reacts to the problem that the Consumer Sales Directive, still based on the principle of minimum harmonisation, allows for different standards of liability for online traders when selling across borders within the EU, especially preventing SMEs from benefitting from the internal market.[484] By proposing a fully harmonised and advanced framework of consumer protection for online sales, the Commission aims to increase legal certainties both for online traders and consumers.[485]

Yet this new piece of legislation has several shortcomings regarding connected devices. First, it sticks with the traditional definition of a sales contract according to which the Directive would only apply if the consumer 'pays or undertakes to pay the price'[486], obviously not considering the possibility, as set out in the Proposal for a Digital Content Directive, that consumers could nowadays provide personal data as a counter-performance.

This, however, is neither the only nor the most important shortcoming. Secondly, the Directive would only apply, following the model of the Consumer Sales Directive, to sales contracts. Hence,

[479] Proposed new Art 2 Consumer Rights Directive.

[480] Recital 21 Proposed Directive. See also the explanatory memorandum to the Commission Proposal (n 462) 3.

[481] Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees, [1999] OJ L171/12.

[482] Proposal for a Directive of the European Parliament and the Council of 9 December 2015 on certain aspects concerning contracts for the online and other distance sales of goods, COM(2015) 635 final.

[483] Ibid, 14 (Explanatory Memorandum) and Recital 13 Proposal for an Online Sales Directive.

[484] Recitals 5-6 Proposal for an Online Sales Directive.

[485] Recital 9 Proposal for an Online Sales Directive.

[486] Art 2(a) Proposal for an Online Sales Directive. This provision is to be read as only applying to monetary remuneration. See Metzger et al (n 464) para 30.

neither the Consumer Sales Directive nor a future Online Sales Directive provide protection against defects of connected devices where such connected devices are leased or lent to consumers.[487]

Thirdly, in cases where a contract has elements of both sales of goods and provision of a service, the Online Sales Directive will only apply to the sale of goods[488], exclusively covering defects of the embedded digital service that are subordinate to the main functions of the device. If, as proposed, the Digital Content Directive does not cover embedded software and services, the consumer will have to prove that the physical device or the service embedded in it, which has to be subordinate to the main function of the device, is defective to get protection. Accordingly, EU law would create a loophole in consumer protection. Of course, Member States could extend the application of legislation implementing the Digital Content Directive also to embedded software to create non-discriminatory protection for all cases for which protection is needed.[489] But this would allow for unjustified disparities in consumer protection across Member States.[490]

Fourthly, it is not necessarily so that the operation of a connected device will always be guaranteed by the party selling the device to the consumer. In many instances, such as regarding a connected car or a connected household device, the seller of the device will often be a regular retailer, while the consumer still is required to conclude a service contract with the manufacturer who guarantees the functioning of the device.[491] Even more, parts of the ancillary digital services could be provided by very different economic agents. Modern consumer law has to adequately respond to such hybrid contractual relationships with multiple sellers and service providers.[492] To restrict contractual liability in the framework of consumer contract law to cases where embedded software is subordinate to the main functions of the device, will not make any sense. Nothing argues against providing contractual protection based on the sales contract with a retailer pursuant to the rules on the Consumer Sales Directive and the Online Sales Directive if the device does not function properly in such cases. But there is no reason either why direct contractual liability with another economic agent should be excluded where the consumer has concluded a separate service contract with that agent. Direct contractual liability of the such third agent—in most cases, the manufacturer—seems particularly required in cases where the functioning of the embedded software serves the main

[487] See also the criticism expressed by Metzger et al (n 464) para 30.

[488] Recital 12 Proposal for an Online Sales Directive.

[489] Based on the argument that the case where embedded software whose functions are not subordinate to the main functions of the connected device does neither fall with the scope of full harmonisation of the Online Sales Directive nor that of the Digital Content Directive.

[490] In this context, even if embedded software and connected services were included in the Digital Rights Directive, the problem still remains that the consumer would have to prove which Directive—the Online Sales Directive or the Digital Content Directive—applies. In this regard, Metzger et al propose that the consumer should be free to choose under which Directive he asserts consumer rights and that the supplier should only be allowed to challenge this choice where it is obvious that this choice was incorrect, namely, in the sense that 'it is apparent without further investigation and expertise' that the expertise lies in the physical part of the device, if the consumer asserts rights under the Digital Content Directive, or in the embedded content, if the consumer asserts rights under the Online Sales Directive. Metzger et al (n 464) para 44.

[491] This is not only a problem with regard to connected devices. In many instances, digital business models, such as business models of the sharing economy, create problems for consumers to identify the person with whom the contract is concluded. On possible legislation to address this problem, see Hans-Wolfgang Micklitz, 'Lösungsoptionen—Sachverständigenrat für Verbraucherfragen (SFRV)' in: Hanns-Wolfgang Micklitz, Lucia A Reisch, Gesche Josst and Helga Zander-Hayat (eds), *Verbraucherrecht 2,0—Verbraucher in der digitalen Welt* (Baden-Baden, Nomos 2017) 9, 15.

[492] In this regards, see in particular Christiane Wendehorst, 'Besitz und Eigentum im Internet der Dinge' in: Hans-Wolgang Micklitz, Lucia A Reisch, Gesche Josst and Helga Zander-Hayat (eds), *Verbraucherrecht 2,0—Verbraucher in der digitalen Welt* (Baden-Baden: Nomos, 2017) 367, 368-69 (differentiating between six different components, one of them being embedded digital content).

function of the device, to guarantee direct claims against the manufacturer where it fails to provide appropriate updates to the embedded software.[493]

In sum, to create effective consumer protection for consumers with regard to connected devices, the most appropriate approach would consist in an extension of the scope of application of the Digital Content Directive to 'embedded digital content and services'.[494] This solution is preferable to a potential extension of the scope of application of the Consumer Sales Directive, since the latter would still exclude consumer protection in rental and lending situations.[495] Another advantage of this solution is that it would also extend the application of the data portability rights proposed for the Digital Content Directive to data generated by connected devices.[496]

In sum, this analysis in principle supports the position of the European Parliament to include 'embedded digital content' within the scope of application of the Digital Content Directive.[497] Quite rightly, the Parliament's proposed amendment would clarify that application of the Digital Content Directive in such cases would not curtail the application of other parts of EU law with regard to other parts of such goods in which digital content is embedded, thereby guaranteeing that the Consumer Sales Directive and a future Online Sales Directive would still apply where physical parts of a connected device are not in conformity with the contract.[498]

Yet, also the proposal of the Parliament suffers from certain shortcomings. Contractual liability of the trader will be limited to the lack of conformity of the embedded digital content or an embedded digital service 'which exists at the time of delivery of the goods in which the digital content or digital service is embedded and which becomes apparent within two years from the time of delivery'.[499] This would ignore the fact that consumers do not only conclude one-point-in-time contracts with retailers on the sale of connected devices, but enter into a permanent service contract especially with the manufacturer under which the latter should be held liable for any defective update of the embedded software or failure to update the software to maintain its appropriate function.[500] In addition, by requiring that the digital content or digital service be embedded in the device, the proposal runs the risk of allowing manufacturers to circumvent mandatory liability by 'embedding' the digital content or service in the cloud.[501] Accordingly, the appropriate approach would be to make the Digital Content Directive applicable to digital content and digital services ancillary to a

[493] Argument made by BEUC in favour of extending the Digital Content Directive to embedded software. See BEUC, 'Digital Content Directive—Key recommendations for the trialogue negotiations' (2018) 2, available at: http://www.beuc.eu/publications/beuc-x-2018-003_digital_content_directive.pdf (accessed 30 April 2018).

[494] This is also argued by Metzger et al (n 464) paras 32-34 (calling the exclusion of 'embedded digital content and service' from the Digital Content Directive a 'resounding mistake' at para 32).

[495] So far, BEUC has expressed its view that consumers should also be protected with regard to 'embedded software', but it has also left open whether this should be implemented by an extension of the scope of application of the Digital Content Directive or a reform of the Consumer Sales Directive. The only argument in favour of a reform for the Consumer Sales Directive is that the Digital Content Directive would otherwise gradually empty the application of the Consumer Sales Directive. See BEUC (n 493) 2. However, the latter argument should not be considered as relevant given the shortcomings of the Consumer Sales Directive with regard to its limited application to sales contract and lack of full harmonisation.

[496] Whether, however, the EU legislature will finally follow the Commission's proposal to introduce data portability rights in the Digital Content Directive that go beyond the Data Portability Right of Art 20 GDPR, has by now become rather unlikely. See at i) below.

[497] See the comparison of the different proposals of the Commission, the Council and the Parliament in Metzger et al (n 464) 97.

[498] Art 3(3), last sentence, of the proposed amendment to the Digital Content Directive.

[499] Proposed amendment for Art 9(1)(c) Digital Content Directive.

[500] See also the criticism by Metzger et al (n 464) para 36 (arguing that even in cases where the software gets 'installed' after the sale, the Parliament's proposal would fail to provide protection).

[501] As to this argument see Metzger et al (n 464) para 35.

good 'irrespective of the way in which [the digital content or the digital service] is delivered'.[502] In this context, it is also important to guarantee that the notion of a 'trader' is not limited to the person selling, leasing or lending the good but also to any third service provider entering into a contract with the consumer on the provision of digital content or digital service ancillary to such a good.

f) Overview on the contractual consumer rights regarding the use of data

The contractual rights of consumers with respect to data collected by connected devices can vary considerable depending on the purpose of the collection and later use of the data. Where the data are the basis of the working of the device, low quality of the data could translate into liability under the Consumer Sales Directive because the connected device does not live up to the expected purpose and performance.[503] In such cases, low quality of data will be caused by a technical defect of the device either in form of a malfunctioning of the sensors collecting data or the software processing of the data. Contractual liability for the non-conformity of the embedded—or better: 'ancillary'—digital content and digital service is also at the heart of the preceding debate on extending the scope of application of the Digital Content Directive.

The focus of the following analysis will however turn to the rights of consumers concerning the use of data and possible rights of access of consumers to data collected by connected devices. In this regard, three aspects of the emerging EU consumer law framework are of particular importance: (1) the rights of consumers to withdraw from the contract[504]; (2) possible contractual data portability rights[505], and (3) control of standard contract terms relating to the collection and processing of data[506]. All these issues are currently under consideration by the European legislature in the framework of the already mentioned proposals. Similarly, for all these issues, the following analysis has to take into account the interface with data protection rules.

g) The right to withdraw from a contract

Consumers are not guaranteed a general right to withdraw from a contract concerning a connected device only because this device collects data when being used.

Yet the most recent so-called 'New Deal for Consumers' initiative of the Commission of 11 April 2018[507] to reform, *inter alia*, the Consumer Rights Directive[508], would clarify that consumers are vested with the same rights of information[509] and the right to withdraw from the contract within a 14-day period where the contract relates to a digital service and for which consumers provide

[502] Proposal by Metzger et al (n 464) para 38. To implement this solution, Metzger et al (n 464) para 40, propose to delete Art 9(3)(c) Digital Content Directive as proposed by the Parliament, since Art 9(3)(b) would already appropriately cover liability by the provider of ancillary digital content or digital services.

[503] See Art 2(1)(b)-(d) Consumer Sales Directive (n 481). Where a connected device is sold in the framework of a distance sale, the new Online Sales Directive would apply instead of the Consumer Sales Directive.

[504] See at g) below.

[505] See at i) below.

[506] See at j) below.

[507] Proposal for a Directive on better enforcement and modernisation of EU consumer protection rules (n 462).

[508] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, [2011] OJ L304/64.

[509] In line with its general orientation, this Study refrains from discussing the extension of duties to inform to digital online services.

personal data instead of paying with money. With this proposal, the Commission seeks to put consumers on the same level of protection in case of distance contracts irrespective of whether the consumer pays with money or provides personal data.[510] As a result, consumer for instance subscribing to a dating platform would be provided with a testing period before the contract finally becomes binding.

According to the Commission's Proposal, digital services may come in two forms: (1) as a service 'allowing the consumer the creation, processing or storage of, or access to, data in digital form'; and (2) as a service 'allowing the sharing of or any other interaction with data in digital form uploaded or created by the consumer and other users of that service, including video and audio sharing and other file hosting, word processing or games offered in the cloud computing environment and social media'.[511] As examples, the recitals to the proposed Directive mention the following cases: cloud storage, webmail, social media and cloud applications.[512] The definition of digital services is identical with the second and third sub-category of digital content in the Proposal for a Digital Content Directive.[513] In line with this, the Commission proposes to change the definition of a service contract. This definition is supposed to include both forms of 'digital service contracts' even where the users provide access to personal data instead of paying with money.[514] This leads to a withdrawal right under Article 9(1) Consumer Rights Directive where the digital service contract is concluded as a distance contract in the sense of Article 2(7) Consumer Rights Directive.

In contrast, the question of whether consumers should also enjoy a right to withdraw from a distance contract that relates to the first category of digital content in the sense of the Proposal for a Digital Content Directive, namely, in the case of 'data which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software'[515] is not sufficiently clarified by the Commission's Proposal for reforming the Consumer Rights Directive. Quite the contrary, the proposed revision of the definition of service contracts in Article 2(6) Consumer Rights Directive may even be read in the opposite sense to exclude contracts on the supply of such content. This conclusion is supported by the fact that the definition of 'contracts on distance sales' should remain unchanged. According to Article 2(5) Consumer Rights Directive, sales contracts need to be directed at the transfer of ownership in goods, whereby Article 2(3) Consumer Rights Directive is limited to 'tangible' moveable good. Hence, contracts on the provision of digital content in form of video, audio, applications, digital games and other software do not fulfil the requirement of a sales contract. Yet it has to be noted that the general definition of a service will also remain unchanged. This definition is worded very broadly. Pursuant to the current and revised Article 2(6) Consumer Rights Directive a 'service contract' is defined as 'any contract other than a sales contract'. This means that contracts on the provision of 'digital content', covering all three categories in the sense the Proposal for a Digital Content Directive, would in fact fall within the concept of a service contract.[516] The proposal of the Commission to now add another sentence to Article 2(6) Consumer Rights Directive according to which the terms 'service' and 'service contracts' also refer to 'digital service' and 'digital service contracts' seems therefore misleading. Such service

[510] Commission Proposal (n 462) 3, 6 and 19. See also New Deal for Consumers Communication (n 460) 5.

[511] See Article 2 of the Proposal.

[512] Recital 21 Proposed Directive. See also the introductory part of the Commission Proposal (n 462) 3.

[513] Art 2(1)(b) and (c) Proposal for a Digital Content Directive. See also at e) above. On the need to align the text of the Consumer Rights Directive with the Digital Content Directive see Proposal of the Commission for a Directive on better enforcement and modernisation of EU consumer protection rules (n 462) 6 (Explanatory Memorandum).

[514] Proposed Art 2(6) of the amendment to the Consumer Rights Directive.

[515] Art 2(1)(a) Proposal for a Digital Content Directive.

[516] See also Recital 22 Proposal for a Directive on better enforcement and modernisation of EU consumer protection rules (n 462) (confirming that the Consumer Rights Directive already applies to contracts on digital content that is not supplied on a digital medium).

can also exist in the provision of 'digital content' as defined in a newly proposed Article 2(11) Consumer Rights Directive, which imports the definition of the first category of digital content in the Proposal for a Digital Content Directive into the text of the Consumer Rights Directive.[517] This latter definition is in need for bringing precision to the already existing exclusion of contracts on the 'supply of digital content which is not supplied on a tangible medium' in Article 16(m) Consumer Rights Directive. Such exception is hence limited to the first category of digital content in the sense of the Proposal for a Digital Content Directive.

Against the backdrop of this analysis, three questions arise with regard to connected devices: (1) Do consumers already enjoy a right of withdrawal when they conclude distance contracts with connected devices as an object? (2) Will consumers be given more extended rights following the new proposal of the Commission for a reform of the Consumer Rights Directive with regard to connected devices? (3) Do such rights suffice to protect consumers adequately?

First, consumers already enjoy a right to withdraw from a distance contract pursuant to Article 9(1) Consumer Rights Directive when they buy a connected device in the framework of a distance contract. The right to withdraw from the contract within 14 days after acquisition of the physical possession of the device enables the consumer to test the product also with regard to the functioning of embedded software and embedded services.

The situation gets more complex when consumers acquire the device from one person, such as a retailer, and enter into a separate contract with another person or entity, such as the manufacturer of the device, whereby this latter contract relates the use of embedded software or to the provision of an ancillary service. In these cases, the question is whether the consumer also enjoys a separate right to withdraw from this contract.[518] Pursuant to its very broad definition of a 'service contract', namely, as 'any contract other than a sales contract' pursuant to Article 2(6) Consumer Rights Directive, such contract can also give rise to a withdrawal right, since such contract will typically be concluded in form of a distance contract in the sense of Article 2(7) Consumer Rights Directive, for instance where the consumer has to accept a click-wrap licence to be able to use the device. Yet, the availability of the withdrawal right under current rules still depends on two additional requirements: first, the contract must include an obligation on the part of the consumer to pay for the service[519], and, secondly, the withdrawal right must not be excluded according to Article 16(m) Consumer Rights Directive. The latter provision is also limited in scope, namely, by only excluding contracts on the 'supply of digital content which is not supplied on a tangible medium'. Similar to the case of the distance sale of the copy of a computer program delivered on a CD-ROM, the withdrawal right therefore seems to apply where the consumer enters into a separate licence agreement for the use of software that is embedded in a connected device.

Secondly, turning to the question of how the new Commission proposal would change the legal situation, the above analysis shows that the inclusion of the concepts of 'digital services' and 'digital service contracts' as well as 'digital content' and 'contracts for the supply of digital content which is not supplied on tangible medium' should not be understood in the sense that the reform will only

[517] Hence, the distinction between 'digital content', on the one hand, and 'digital services', on the other, within the proposal for an amended Consumer Rights Directive seems to conflict with the Proposal of the Commission for a Digital Content Directive according to which the two categories of 'digital services' are defined as sub-categories of 'digital content'. This may however be interpreted as an indication that the Commission is now ready to change the concepts of the Digital Content Directive accordingly, which indeed corresponds to a proposal for revision by both the Parliament and the Council. See Draft European Parliament Legislative Resolution (n 474), amendments proposed for Art 2(1) Digital Content Directive.

[518] It is to be noted that such right does not depend on the characterisation of the contract for the sale of the connected device as a distance contract. In cases where the consumer acquires the device in the physical premises of a retailer, the service contract may be concluded on distance, especially from the consumers home, when starting the use of the device.

[519] Art 2(6) Consumer Rights Directive.

now lead to an extension of the scope of application of the rights under the Directive, especially the rights to withdraw, to such contracts. Rather, the purpose of this proposal consist, on the one hand, in the alignment of the Consumer Rights Directive with the Digital Content Directive, resulting in a clarification of the scope of application, and, on the other hand, in extending the scope of application to contracts on the provision of digital content, pursuant to proposed Article 2(11) Consumer Rights Directive, and to digital service contracts, pursuant to proposed Article 2(18) Consumer Rights Directive, where the consumer 'provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer is exclusively processed by the trader for the purpose of supplying the digital service, or for the trader to comply with legal requirements to which the trader is subject, and the trader does not process this data for any other purpose'.

Thirdly, the remaining question is whether the proposed revisions go far enough in the light of the current discussion on inclusion of software and digital services embedded in connected devices in the framework of the definition of digital content and services in the Digital Content Directive. As seen in the preceding analysis of the existing withdrawal right under the Consumer Rights Directive, the broad concept of a service contract should already today provide a right to withdraw from a service contract where a consumer has entered into a separate licensing or digital services contract, fulfilling the requirements of a distance contract, linked to a connected device. As argued for the Digital Content Directive, the scope of application should however explicitly be broadened to include contracts on the provision of software and digital services for the use of connected devices in cases where the consumer does not pay with money but provides or undertakes to provide personal data.

In addition, special consideration has to be given to the exception made from the withdrawal right under Article 16(m) Consumer Rights Directive. As seen above, this provision already now excludes the right of withdrawal in the case of a contract on the supply of digital content, such as a song, a video or a computer game, from the very moment the performance (download or streaming) begins. The reason for this exclusion lies in the 'one-off nature' of the digital download or a streaming.[520] For this purpose, the definition of a contract on the provision of digital content in a new Article 2(16) Consumer Rights Directive would now require a contract on 'specific' digital content. Hence, the exception would not apply where a consumer concludes a subscription contract for a music or video streaming service. In the latter case the withdrawal right is justified since the provider is continuously involved in the provision of a service and the consumer is therefore in need of making experience with the service for some time before making a final decision on the contract.[521] The Commission proposes further refinements to this exemption. First, by including explicit definitions on 'digital content' in Article 2(11) and on the concept of a 'contract for the supply of digital content which is not supplied on tangible medium' in Article 2(16) Consumer Rights Directive, the Commission aims at clarifying that the exception of Article 16(m) does not apply to contracts on the provision of digital service, although they are understood as sub-categories of digital content under the proposed Digital Content Directive. Secondly, it has to be emphasized that the extension of the definition of such contracts for the supply of digital content to include cases where the consumer only provides personal data, without paying a price in form of monetary remuneration, is also taken into account in the framework of the exception pursuant to Article 16(m) Consumer Rights Directive. This provision only differentiates by restricting the need for consumer's prior express consent to begin the performance as a requirement for the exception to cases where the consumer has actually committed to pay a price. This means that the consumer loses automatically the right to withdraw from the contract for the provision of digital content, even

[520] See Recital 21 Proposal for a Directive on better enforcement and modernisation of EU consumer protection rules (n 462).

[521] Ibid.

without prior consents, where she starts to download the content and where she only provides personal data in return.

Against the backdrop of this analysis, the remaining question is whether and how the exception of Article 16(m) Consumer Rights Directive should apply to software and digital services embedded in, or ancillary to, the use of connected devices. Here, it is to be noted that Article 16(m) already makes a clear statement as regards so-called embedded software.[522] A connected device may well have to be considered a tangible medium, although, in formulating this rule, the European legislature did not consider the specific case of connected devices but rather CDs, DVDs and CD-ROMs as physical carriers of audio, video and computer programs. If this reading is followed, the exception of Article 16(m), only covering 'digital content which is not supplied on tangible medium', would not apply to embedded software. However, this does not mean that the consumer will have a withdrawal right concerning embedded software that can be separated from the contract concerning the connected device as a tangible item. Quite the contrary, the consumer will only be able to rely on the withdrawal right, if the connected device was acquired or used in the framework of a distance sales contract or a distance service contract. If the software is used under a licensing contract with another person than the trader from whom the consumer has acquired the connected device, the software would not be considered as being provided on a tangible medium; indeed, in such cases, technical protection measures will regularly prevent the consumer from using the software before entering into the licensing agreement for the software with the third person, making this third person the provider of the software. In cases where a third person provides software, including updates, or digital services, the exception of Article 16(m) Consumer Rights Directive should not apply, since the contract does not demonstrate a one-off nature. Rather, the consumer should be allowed to test the service during the withdrawal period. It seems that such adequate results could already be attained through a purpose-oriented construction of Article 16(m) Consumer Rights Protection.

Furthermore, problems can arise where a consumer buys a connected device from a retailer while she enters into a contract for the provision of software enabling the use of the device or for the provision of ancillary services with another person such as the manufacturer. In such cases the consumer may be allowed to withdraw from the distance contract with the manufacturer while a withdrawal right might not exist with respect to the sales contract regarding the device as such. In such instances, withdrawal from the former contract will lead to automatic termination also of the contract with the seller of the device according to Article 15 Consumer Rights Directive. The sales contract seems to fulfil the requirements of a so-called ancillary contract under this provision and the definition contained in Article 2(15) Consumer Rights Directive.

In sum, the preceding analysis argues for the applicability of the right to withdraw from a contract on the supply of software or services that are embedded or ancillary to the supply of a connected device where the requirements of a distance contract are fulfilled. It seems that appropriate results can be attained by a purpose-oriented interpretation of the Consumer Rights Directive, whereby the extension of the rules of the Directive to cases where digital content and digital services are provided only against the provision of personal data by the consumer, as now proposed by the Commission, should also apply to software and digital services embedded or ancillary to connected devices.

[522] Yet the question should be asked whether the approach of the Commission to exclude software that is subordinate to the main functions of a device from the application of the Digital Content Directive should also be applied to the interpretation of the definition of digital content in Art 2(11) Consumer Rights Directive. In proposing the reform of the latter Directive, the Commission does not seem to have considered this issue.

h) Coordination of consumer contract law with data protection rules

The right to withdraw from a contract regarding connected devices raises additional issues of coordination of the legal rules on consumer contract law, on the one hand, and the data protection rules of the GDPR, on the other. Many of the data protection rights of GDPR can be exercised, although personal data is provided in the framework of a contractual relationship. The interactions work in both directions. Thus, in the recent 'New Deal for Consumers' Proposal, the Commission points out that the withdrawal from a digital service contract under the revised rules would trigger the rights under the GDPR, including the right to erasure (right to be forgotten) and the right to data portability.[523]

The reverse case has to attract particular attention from a contract law perspective. The right to withdraw consent at any time and the ensuing right to erasure pursuant to Article 17(1)(b) GDPR seem to directly conflict with the binding effect of a contract under which the data subject has in fact entered into an obligation to grant access to or to provide personal data. Article 17 can be read in context with Article 6(1) GDPR. According to Article 6(1)(a) GDPR, consent is a requirement to make the processing of personal data lawful. However, Article 6(1)(b) GDPR also allows for processing without consent where 'processing is necessary for the performance of a contract to which the data subject is party'. This rule could be interpreted in the sense that in the case of a contract for which processing of personal data is necessary the data subject can neither withdraw consent to the data processing nor claim erasure as long as the contract is in force and in need of being performed.

In the case of connected devices, personal data will often be necessary to provide an information service to the data subject. A typical example would be the processing of personal data generated through smart wearables in the framework of providing mobile health care to patients. Against the backdrop of above rules, a clash between contract law and data protection would only arise where the patient has accepted contract clauses that authorise the health care provider to use the data for further purposes, such as to commercialise the data in secondary markets to generate additional income. For such further use, the patient has to give consent under Article 6(1) GDPR consent, which can later be withdrawn according to Article 17(1)(b) GDPR.

To assess the consequences of the withdrawal of consent in such a case, the point of departure is the legal nature of prior consent. The consent has a dual nature. It does not only constitute consent in the sense of data protection law. By expressing consent, the data subject also agrees to license the use of her personal data to the data processor.[524] The latter does not necessarily require recognising personal data as an economic asset 'owned' by the data subject. Already the need to give consent provides the data subject with legal control that can be used for economic purposes. However, the legal consequences of withdrawal of consent according to Article 17(1)(b) on the licensing agreement are not explicitly addressed by the GDPR. A strict contract law approach would lead to the conclusion that, by withdrawing consent, the data subject violates the contract and hence, can be held liable at least for damages. However, this result runs counter to the very objective of Article 17(1)(b) GDPR, according to which the data subject shall have the right to autonomously change her mind. An obligation to pay damages to the other party could easily prevent the data subject to exercise the right to withdraw consent. This interpretation seems to be confirmed by Article 3(8) of the Proposal for a Digital Content Directive, stating that this Directive is without prejudice to rights of individuals regarding to the processing of their personal data. Although this provision still has to come into force, it demonstrates the weight given to data

[523] Commission Proposal for a Directive on better enforcement and modernisation of EU consumer protection rules (n 462) 6.

[524] See also Berger (n 24) 352.

protection rights in the EU legal order.[525] As part of EU law, the data protection rights should therefore be understood to prevail over the applicable national contract law. Thus, withdrawal of consent pursuant to the rules of the GDPR terminates the licensing of the use of the data to the extent that it goes beyond what is required for the performance of the contract. The follow-up question then is whether the rest of the contract can continue to exist. It is for the applicable contract law to decide that matter. The answer will very much depend on the circumstances of the case.

Another question relates to the effect of the withdrawal of consent under Article 17(1)(b) GDPR where data is provided for the purpose of receiving a service (data as a 'counter-performance'). As discussed just before, the instances where a consumer is allowed to use a connected device for free by only providing personal data may only occur rarely but become more frequent in the future. In addition, it is to be noted that the collection of personal data where personal data is needed for providing the data subject with the service that is the major object of the contract, such as the provision of safe driving in the case of connected cars or the provision of health care based on data collected by smart wearables, the personal data collected cannot be considered as a counter-performance or a payment for the service. Rather, such cases should be limited to those where the data is collected for other purposes, such as collecting personal data through a bike-sharing company to be sold to the local authorities for purposes of city planning.[526] The question of the effect of the withdrawal of consent to the data processing on contracts where the consumer provides personal data for the purpose of receiving a service[527] is particularly discussed for the future Digital Content Directive.[528] If ultimately the EU legislature broadened the scope of the Digital Content Directive to also apply to software or digital services embedded in, or ancillary to, connected devices,[529] it should be clear that the rights of the GDPR would prevail for all contracts for which the counter-performance consists in the provision of data.[530] Even authors who think that the withdrawal of consent will not terminate the contract, but still want to make the obligation to provide data unenforceable as a matter of data protection law, opine that this should also lead to the conclusion that the data subject refusing to fulfil her contractual obligations can no longer be entitled to claim the performance of the contract by the other party.[531]

i) Contractual data portability rights under the Digital Content Directive

Contractual data portability rights have been proposed by the Commission for Articles 13(2)(c) and 16(4)(b) Digital Content Directive.[532] In the first case, the right arises when the consumer terminates the contract as a remedy when the digital content delivered by the other party is not in conformity with the contract. In the second case, the right is given after regular termination of a digital content

[525] In reaction to the Commission Proposal, the European Parliament proposes to shift the safeguard clause in favour of the application of EU data protection rules to the very beginning of the Directive as its new Art 1. See Report of the European Parliament of 27 November 2017 on the proposal for a directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, PE 592.444v02-00.

[526] In the same vein Janal (n 156) 28.

[527] As already discussed at d) above.

[528] See Berger (n 24) 353-54.

[529] Report of the Parliament (n 525) Amendment 83 on Art 3(3). See also discussion at e) above.

[530] See also Berger (n 24) 353-54.

[531] Ibid, 354.

[532] Proposal for a Digital Content Directive (n 199).

contract concluded for an indeterminate period (long-term contract).[533] In both cases, the portability right would require the supplier to

> provide the consumer with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent this data has been retained by the supplier. The consumer shall be entitled to retrieve the content [free of charge,] without significant inconvenience, in reasonable time and in a commonly used data format . . .

Hereby, the requirement that the retrieval of the content must be free of charge is only stipulated in Article 13(2)(c) of the Proposal.[534] Hence, the fact that the data portability rule arises from a defect of the digital content for which the supplier is liable justifies that the consumer does not have to pay anything when asserting the right.

These data portability rights would differ from the data portability right of Article 20 GDPR in several regards. The scope of the application is broader in some regards, but also narrower in other regards. Whereas Article 20 GDPR only applies to personal data, the rights of the Digital Content Directive would also cover non-personal data. Conversely, unlike under Article 20 GDPR, the consumer cannot claim data portability prior to the termination of the contract. In this latter regard, it is clear that the Digital Content Directive would not provide for a data access right where the consumer has an interest in data access to the datasets produced by a connected device during the time of the contractual relationship. In addition, the data portability rights of the proposed Digital Content Directive would be more limited than the one of Article 20 GDPR to the extent that the consumer cannot claim transfer of the data to a third person.

The scope of these data portability rights of the Digital Content Directive are also a major point of discussion among EU institutions in the current trilogue.[535] As regards the data portability right in case of liability of the supplier, both the European Parliament and the Council aim at establishing a more coherent approach by excluding portability of personal data from the scope of the rules of the Digital Content Directive. For protecting consumers with regard to personal data, both institutions therefore propose introducing a rule that clarifies that the supplier should exclusively comply with the obligations under the GDPR.[536]

Hence, the most important question relates to the extension of data portability to non-personal data. Here, the European Parliament and the Council propose more limited, yet somewhat diverging approaches. As regards termination in the case of contractual liability of the supplier, both institutions would at least prefer to limit the scope of the right to certain forms of non-personal data. The Council proposes to implement a limitation to non-personal 'digital content ..., which was uploaded or created by the consumer when using the digital content or digital service supplied by the supplier'. Even more specifically, the European Parliament refers to 'user-generated content ..., which was provided or created by the consumer when using the digital content or digital service supplied by the trader'.[537]

In respect of data portability in case of termination of long-term contracts, the Council proposes a most appropriate alignment with the data portability rules in Article 20 GDPR and data portability right in case of the supplier's liability in the Digital Content Directive by making references to the

[533] See also the analysis by Janal (n 156) paras 26-47.

[534] This is criticised by Janal (n 156) 37 (arguing *inter alia* that also in the case of a long-term contract where personal data is involved, data portability could be claimed free of charge pursuant to Article 20 GDPR).

[535] See the comparison of the proposals of the Commission, the Parliament and the Council in Metzger et al (n 464) 102.

[536] In support of this proposal, BEUC (n 493) 6; Metzger et al (n 464) paras 51 and 53 (also after taking into account the differences between the data portability rights under the GDPR and a future Digital Content Directive).

[537] See comparison in Metzger et al (n 464) 102.

respective provisions in Article 16(3) Digital Content Directive,[538] while such reference is surprisingly missing in the Parliament's proposal[539].

On substance, especially the use of the terms 'provided and created by the consumer' as proposed by the Parliament appear more appropriate than the term 'retained by the supplier' in the Commission's Proposal. This formula would guarantee the consumer to get back what she has actually provided to the supplier, irrespective of whether the supplier has still 'retained' the data. This approach would require the supplier to retain any data provided to it. Indeed, the case of user-generated content may well constitute the most important kind of non-personal content in which the consumer has an interest in retrieving it at the time of termination of the contract.[540]

On the other hand, both institutions seem to limit the scope of the data portability right considerably by limiting it to 'digital content' or even 'user-generated content'. It can certainly be argued that consumers may only have a strong interest in retrieving non-personal data that consists in user-generated content, whereas Internet service providers will often seek to acquire the rights, especially the copyright, in such user-generated content on a permanent basis. Whether consumers have a legitimate interest in retrieving yet other non-personal data they may have provided to the supplier is less clear and may even be doubtful. Hence, to better protect suppliers against excess claims of data portability, limiting the scope of data to user-generated content may be considered justified. Yet both institutions propose even further limitations. The Council and the Parliament want to exclude a right to retrieve non-personal digital or user-generate content (the latter in the terminology of the Parliament) in three important cases, namely, where such content 'has utility within the context of using the digital content or the digital service supplied by the supplier, or which relates only to the consumer's activity when using the digital content or digital service supplied by the supplier or which has been aggregated with other data by the supplier and cannot be disaggregated or only with disproportionate efforts'[541]. As other critics have already pointed out, such limitations could seriously weaken consumer protection and prevent consumers from asserting their rights, even in the case of the supplier's liability, and from switching to other suppliers. This could indeed considerably weaken competition in the digital sector.[542] As an alternative, Metzger et al propose that retrieval of the data should already be possible if the consumer sees utility outside the context of the digital content or service provided by the supplier; the other two exceptions could be avoided if the supplier would be required to design its service in a way that allows for extracting the user-generated content easily.[543] In sum, it appears most important that the European legislature fully understands that the interest of consumers in retrieving non-personal user-generated content is not less strong and less legitimate than the interest in retrieving personal data.

From the perspective of this Study, however, the main question is of course whether the data portability rights of the Digital Content Directive in the two cases of termination of the contract should also apply to non-personal data generated by connected devices. This will crucially depend on whether—against the backdrop of the wording proposed by the Commission—the term 'digital

[538] See also Metzger et al (n 464) para 55.

[539] Criticised by Metzger et al (n 464) para 55.

[540] User-generated content may consist in a large variety of content, such as pictures, videos, music, etc. A most important kind of user-generated content for which consumers might have a particularly strong interest to get a data portability right at the point in time they terminate an online service contract are avatars consumers created by playing online computer games. For a discussion of the data portability right concerning avatars under Article 20(1) GDPR, see Van der Auwermeulen (n 114) 70 (arguing against the personal data character of avatars).

[541] Quote from the text proposed by the Council.

[542] See the critique expressed by Metzger et al (n 464) para 54.

[543] Ibid.

content' would also include any 'embedded' or ancillary content. [544] In such case, any 'data produced or generated through the consumer's use of the [embedded] digital content' would indeed coincide with all data collected by the device without any limitation if this data is indeed linked to the consumer's use of the device. In contrast, the proposals of the Council and the Parliament would considerably limit the scope of the data portability rights. In the first place, connected devices will typically not collect non-personal, user-generated content. Nor can data collected by connected devices be easily considered as data 'created' by the consumer. Although the Council's proposal would not limit the kind of data, the Council seems even more restrictive as regards the way the consumer makes the data accessible to the supplier. While the Parliament's proposal would include all cases where the consumer has 'provided' user-generated content, whereby the term 'provided' can be interpreted rather broadly as shown in the context of the discussion of Article 20(1) GDPR[545], the Council's text would only include cases where the consumer has provided data in the form of 'uploading'.

Ultimately, the question of whether the consumer should enjoy a right to retrieve any non-personal data collected by a connected device during the time of using the device in case of termination of the contract has to be answered against the backdrop of the legitimate interests of consumers. Indeed, it has to be taken into account that especially where the consumer has acquired ownership in the device but still uses the device under a long-term service contract with the manufacturer, denial of the portability right may prevent the consumer from switching to an alternative supplier.

Hence, in the context of adopting the Digital Content Directive, the European legislature would have the opportunity to consider introduction of a consumer-oriented data access right that would help consumers to escape a data lock-in where they have acquired connected devices. Yet the current state of the discussion as regards this piece of legislation is rather going in the opposite direction, namely, a more restrictive approach to recognising a data portability right regarding non-personal data. In addition, consumers may be in need of a data portability right including non-personal data collected by connected devices not just in the case of termination of a digital content or digital service contract but also during the time of performance of such contract. Therefore, the discussion of whether such more extended 'data access' rights for consumers should be recommended is postponed to the last part of this Study.[546]

j) Control of standard contract terms, especially concerning personal data

Control of standard contract terms under the Unfair Contract Terms Directive[547] is a classical instrument of European consumer contract law.

In its European Data Economy Communication of January 2017, the Commission has also addressed the question of whether mechanisms of control of unfair contract terms could be used to enhance access to machine-generated data.[548] Yet the Commission clearly understood the challenges of such an approach. First, unfairness control mechanisms require a benchmark in form of default contract rules from which the contract terms deviate. Since such default rules do not exist on the EU level, for the public consultation launched by the European Data Economy Communication in 2017, the Commission addressed the issue of unfairness control of contract terms relating to data within the context of a larger debate on whether there is a need to adopt such default contract

[544] See at sub-section e) above.

[545] See at sub-section b) above.

[546] See at 5.3 below.

[547] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, [1993] OJ L95/29.

[548] European Data Economy Communication (n 9) 12; European Data Economy SWD (n 9) 31-32.

rules.[549] The second challenge relates to the question of whether unfairness control of contract terms should be extended to B2B relations, since contracts relating to data are typically concluded among businesses. By opening a debate on extending the scope of application of the Unfair Contract Terms Directive to B2B contracts, the Commission sought to provide protection to SMEs who seek access to data and may, similar to consumers, suffer from an imbalance of bargaining power.[550] For advancing this idea, the Commission could rely on already existing practice in some Member State to control B2B contracts, although the standard, following good commercial practice as a guidepost, may be more lenient, as well as already existing sector-specific rules on the control of B2B contracts.[551]

In the public consultation, stakeholders were then much divided on whether the creation of default rules for contracts relating to data combined with unfairness control mechanisms in B2B relations would promote access to data.[552] Against this idea, it was especially argued that the risk of unfair contract terms in B2B relations was not new, but that it was adequately dealt with by existing law; that the situation differed widely between sectors and that such legislation could harm innovation and the development of new business models.[553]

Meanwhile, the Commission seems to have given up the idea to extend unfairness control mechanisms to B2B relations. In the 'New Deal for Consumers' package of 11 April 2018, the Commission proposes an amendment of the Unfair Contract Terms Directive.[554] Yet this amendment is limited to the introduction of penalties applicable to infringements of the national provisions adopted for the implementation of the Directive.

Hence, the Unfair Contract Terms Directive will continue to exclusively address B2C relations. As concerns the contractual rights of consumers in the data economy, the two Commission proposals for the Digital Content Directive and the Online Sales Directive will create mandatory contract law for the protection of consumers. Within the framework of this legislation unfairness control of contract law will therefore not be of great importance. Yet it is still to be seen to which extent the scope of application of the Digital Content Directive will be extended to also cover the sale of connected devices with embedded digital content and services.[555]

Against this backdrop, the most important field of application of the Unfair Contract Terms Directive concerning connected devices should relate to contract terms that address the collection and use of personal data collected from the owner or user of the device. Recital 43 of the GDPR confirms the applicability of the Unfair Contract Terms Directive where consent for the data

[549] European Data Economy Communication (n 9) 12.

[550] Ibid. Thereby, the Commission also launched an academic debate that did not exist before. See Friedrich Graf von Westphalen, 'Contracts with Big Data: The End of the Traditional Contract Concept?' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, 2017) 245 (discussing in particular whether Art 86(1)(b) of the Proposal for a Common European Sales Law could serve as a basis for such unfairness control between businesses).

[551] European Data Economy SWD (n 9) 32. As regards sector specific rules, the Commission Staff refered to Art 7 Directive 2011/7/EU of the European Parliament and the Council of 16 February 2011 on combating late payment in commercial transactions, [2011] OJ L48/1.

[552] Commission, Synopsis Report (n 10) 5-6. Among respondents 24.5% agreed, 17.7% said that this would sometime be the case, and 41.1% disagreed. See Annex to the Synopsis Report (n 10) 21.

[553] Commission, Annex to the Synopsis Report (n 10) 21. Equally cautious—and only advocating the adoption of draft model contract rules—Graf von Westphalen (n 550) 269 (in the light of limited knowledge about the suitability of any default rules for new business models that are constantly evolving).

[554] Art 3 of the Proposal for a Directive as regards better enforcement and modernisation of EU consumer protection rules (n 462).

[555] See at n e) above.

processing is included in a written, pre-formulated declaration on another matter.[556] Yet the question remains whether unfairness control is at all needed to ensure the respect of data protection rights, since the GDPR recognises mandatory rights that can be relied upon even against any conflicting agreement. This is confirmed by Article 7(2), 2nd sentence, GDPR, which explicitly states that, where consent to the data processing of personal data is given in a declaration that also concerns other matters, a violation of the GDPR by any other part of such declaration will make such part non-binding.

Yet the relationship between the data protection rules of the GDPR and contract law is complex.[557] In general, the GDPR does not prevent the data subject from entering into a contract that entitles the other party to collect and use personal data, provided that the data processing is lawful under the provisions of the Regulation. Where the processing of personal data is necessary for the performance of a contract to which the data subject is a party, Article 6(1)(b) GDPR even dispenses the other party from getting consent according to Article 6(1)(a) GDPR. This provision has been criticised for enabling businesses to circumvent the rights of the data subject.[558] This is so because consumers nowadays often conclude a series of additional contracts—typically with the manufacturer—when they turn on a digital (connected) device. These contracts provide consumers with additional services. In such instances the consumer will not necessarily have to pay a separate price, but the terms and conditions that consumers accept by clicking a box with the objective to finally use the device may entitle the other party to collect and process valuable personal data.[559] Article 6(1)(b) GDPR can make data processing lawful, although the data subject will not necessarily be fully aware of the data processing. Conclusions of such contracts are also, and even more, problematic, because Article 6(1)(b) leads to the loss of rights that the data subject would otherwise have where consent is needed pursuant to Article 6(1)(a) GDPR. This includes in particular the right to withdraw consent according to Article 17(1)(b) GDPR.[560] For this reason, Wendehorst and Graf von Westphalen argue that there is a particular need to exercise unfairness control over the description of the performances of the other party, since such description will trigger the loss of important rights of the data subject under the GDPR.[561]

Before looking at the application of the Unfair Contract Terms Directive in such instances, it is important to get a correct understanding of the scope of Article 6(1)(b) GDPR. The question is how the fact that the processing of data is necessary for the performance of the data has to be characterised in a contract law framework. If provision of such data could also constitute a counter-performance in the sense of contract law, unfairness control could be excluded by Article 4(2) Unfair Contract Term Directive according to which the assessment of the unfair nature of contract terms 'shall relate neither to the definition of the main subject matter of the contract nor to the adequacy of the price and remuneration'.

In the light of the problem that Article 6(1)(b) GDPR dispenses from the requirement of consent by the data subject in Article 6(1)(a) GDPR, the wording of Article 6(1)(b) GDPR should be interpreted

[556] Recital 43, 3rd sentence, GDPR.

[557] This relationship is reviewed by Maximilian Becker, 'Reconciling Data Privacy and Trade in Data—A Right to Data-avoiding Products' (2017) 9 *Zeitschrift für Geistiges Eigentum* 371, 378-82; Moritz Hennemann, 'Personalisierte Medienangebote im Datenschutz- und Vertragsrecht' (2017) *Zeitschrift für Urheber- und Medienrecht* 544; Christiane Wendehorst and Friedrich Graf von Westphalen, 'Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht' (2016) *Neue Juristische Wochenschrift* 3745.

[558] Wendehorst and Graf von Westphalen (n 557) 3747. Others call Art 6(1)(b) GDPR the 'Trojan horse' of data protection. See Hennemann (n 557) 546.

[559] Wendehorst and Graf von Wesphalen (n 557) 3746. Critical on the weakness of the consent principle, Becker (n 557) 378-79 and 381 (specifically referring to take-it-or-leave-it situations, nevertheless, now addressed by Art 7(4) GDPR prohibiting a tying of standard contract terms to consent).

[560] Ibid, 3747.

[561] Ibid, 3749.

strictly, excluding cases where data is provided as a counter-performances of the data.[562] The purpose of the provision is best explained for an off-line world. For many service contracts the service can only be provided if the other party provides relevant information. An attorney at law cannot give advice to a client if the latter does not provide all relevant facts; a doctor typically has to ask the patient about his symptoms to make a diagnosis. In such instances, the client and patient provide the relevant information in their own interest for enabling the attorney and the doctor to provide best service. In such cases the provision of information cannot be regarded a counter-performance with which the client or patient pays the service provider. Still provision of such information is needed to enable the other party to perform the contract properly.

Accordingly, personal data collected by connected devices should be considered to fall under Article 6(1)(b) GDPR only to the extent that they are needed to enable the manufacturer to provide a service to the consumer, especially to guarantee the safe and proper functioning of the device. On the other side of the spectrum, there are personal data which are collected exclusively in the interest of the other party to commercially exploit these data in secondary markets. Where such data collection takes place, the other contracting party should be considered to be in need of consent according to Article 6(1)(a) GDPR.

Yet there are more complex cases, which are characterised by the fact that there is a link of the use of the data with the performance of a contract, and still the conclusion should be that Article 6(1)(b) GDPR does not apply. A first group of cases relates to secondary uses. Where data collection is in principle necessary to perform the contract in the abovementioned sense, Article 6(1)(b) GDPR will not cover the subsequent commercialisation of the data by the manufacturer in its own interest. In the framework of the latter activity, the data is used as an asset for the provision of services in another 'secondary' market without the data subject being a recipient of the service. For such subsequent commercialisation, the manufacturer of a connected device should be required to seek consent according to Article 6(1)(a) GDPR.

A second, and more difficult, borderline case relates to platform service providers where the data subject on one side of the market benefits from indirect network effects. An example would be search engines and social platforms. If Google and Facebook register the activities of users to better select information provided to the users through the algorithms the operators use, under the principles just identified, such data processing would still fall under Article 6(1)(b) GDPR, since the quality of the service will depend on the provision of personal data. However, if the same data is also used to better target advertising at the users in the interest of advertising customers and the platform operators charge a price to these customers, Article 6(1)(b) GDPR should no longer apply. The fact that the data subject may indirectly benefit from the commercialisation of the data on the other side of the platform market, since the advertising customers also, but indirectly finance the service provided to the user 'for free' should not be accepted as a counter-argument. The question of what a specific customer group—the users or the advertising customers—will be charged for running the platform will be decided by the platform operator based on efficiency considerations.[563] Hence, also in such cases, the provision of personal data by users should be considered a counter-performance, as much as the price paid by the advertising customers. Such processing of personal data should require consent pursuant to Article 6(1)(a) GDPR to be legal.

According to these principles, Article 6(1)(b) GDPR would remain limited in scope. As a result, consent would always be required where the provision of data serves a separate commercial interest of the supplier or service provider. Where, hence, consent is required pursuant to Article 6(1)(a) GDPR, there seems to be less need for the assessment of the unfairness of the contract terms. In

[562] In the same sense Wendehorst and Graf von Westphalen (n 557) 3747.

[563] According to the economic model of attention markets, the fact that social platforms such a Facebook only charge a price to advertising customers and offer users access to the platform to for free, is considered to be efficient. See Evans (n 145).

principle, the GDPR itself will sufficiently protect the privacy concerns of the data subject.[564] Still Recital 42 GDPR seems to argue in favour of general availability of fairness control. This may make it possible to consider certain contract terms as unfair in pre-formulated contracts although they do not conflict with the GDPR and therefore would be accepted in negotiated contracts.[565]

Conversely, strict interpretation of Article 6(1)(b) GDPR will make it less likely that, where this provision applies, the terms on the use of data will turn out to be unfair under Article 4(1) Unfair Contract Terms Directive. Yet, also in this case, the issue is whether control is excluded, because the description of the interdependent performances of the service provider and the provision of personal data relates to the main subject-matter of the contract in the sense of Article 4(2) Unfair Contract Terms Directive. Wendehorst and Graf von Westphalen argue that control is nevertheless possible and hint at the narrow interpretation of Article 4(2) Unfair Contract Terms Directive by the CJEU.[566] According to the Court, Article 4(2) only excludes those terms from control that 'lay down the essential obligations of the contract and, as such, characterise it',[567] whereas clauses that are only ancillary to the essential clauses need to be controlled.[568] Wendehorst and Graf von Westphalen argue that the description of the performances should be considered unfair where the principles of privacy of design and privacy by default as enacted in Article 25 GDPR are not respected or where the consequences of a certain element of the performances for the processing of personal data is not transparent.[569] The latter is particularly important: contract terms in the sense of Article 4(2) Unfair Contract Terms Directive will only be exempted from control 'in so far as they are in plain and intelligible language'. This transparency test will most likely become the most important basis for controlling the fairness of data-related contract terms.

This analysis shows, that the application of the GDPR and the Unfair Contract Terms Directive can be applied in a mutually supportive way, which both strengthens the data protection rights of the consumers as recipients of digital services and allow for the development of new markets for digital services, including those that are provided through connected devices.

k) Conclusion

The analysis shows that the data protection rules of the GDPR have meanwhile become the most important system of protection with regard to data generated by connected devices. At the centre of this protection is the principle of autonomy, which, with certain exceptions, makes data processing dependent on consent by the data subject. The GDPR protects the privacy concerns of the individual. With the data portability right of Article 20 GDPR, the European legislature has created a new type of right which goes beyond mere protection of privacy concerns with the objective of enhancing access of the individual to data also for the purpose to overcome economic lock-in situations and to enhance competition. Yet all these rights remain limited to personal data. Based on national law, tort protection of the integrity of the data stored in connected devices may create a second layer of protection where consumers own connected devices. Apart from this, consumers do not hold ownership rights in data.

---

[564] Yet authors argue that fairness control is especially needed where the provision of data has to be considered a counter-performance. See Hennemann (n 557) 548. However, this author does not take into account the possibility of strict interpretation of Art 6(1)(b) GDPR. He also confirms that, under former data protection rules, German case-law did not consider contract terms on data processing as unfair where the data protection rules were respected.

[565] See Hennemann (n 557) 549 (mentioning the potential case of consent to the use of particular forms of data processing).

[566] Wendehorst and Graf von Westphalen (n 557) 3749.

[567] See especially Case C-26/13 *Kásler* ECLI:EU:C:2014, 282, para 49.

[568] Ibid, para 50.

[569] Wendehorst and Graf von Westphalen (n 557) 3749.

Rights of consumers in respect of data generated by connected devices also arise from consumer contract law, including the rights to be informed and to withdraw from a contract. The European legislature is currently working on the implementation of a 'digital update' of European consumer law. However, it is not that clear where contractual liability concerning connected devices should be dealt with in a bifurcated system of the Consumer Sales Directive and a new Online Sales Directive, on the one hand, and a new Digital Content Directive, on the other hand. The commercialisation of connected devices involves much more complex B2C transactions than the sale of non-connected goods. In such transactions, elements of sales contracts and contracts on digital services ancillary to these devices become increasingly inseparable. In its Proposal for a Digital Content Directive, the Commission excluded application of its rules to embedded digital content and services that is subordinate to the functioning of a physical device. This limitation would exclude consumers from protection against the failure of such content and services where to comply with the contract especially in the case where the other contract party is the manufacturer and not the trader from whom the connected device was directly purchased. In addition, this limitation would also exclude the purchasers and users of connected devices from potential future data portability rights of that Directive which are granted both as an additional remedy to termination of the contract for non-conformity of the content or service with the contract and as a right in case of the termination of a long-term contract. Such data portability rights are specifically important for non-personal data, including user-generated content, where the consumer has a particular interest in retrieve them, at the time of termination of the contract. Legislation on this point would even provide the opportunity to create a generally applicable access regime for unlocking data collected by connected devices beyond the data portability right of the GDPR. Yet such a regime would be limited to both B2C relations and the case of termination of the contract. Yet it is still to be seen whether the European legislature will use this opportunity to create more extended data portability rights in the context of the Digital Content Directive. In sum, this legislation cannot replace a more general analysis of the pros and cons of recognising data access rights of the users of connected devices.

All data portability rights suffer from technical limitations of data interoperability. Data can be stored in very different formats. At least, in the framework of Article 20 GDPR the legislature has taken this problem into account. There, although this data portability right also includes the right to make the data available to third persons, in particular for the purpose of switching suppliers, data portability may fail in practice because the new supplier will not be able or willing to accept the data.

The Commission's 'free-flow-of-data' initiative has also launched a debate on creating default rules for contracts relating to data as a benchmark for controlling the unfairness of contract clauses. However, this debate has very much focused on B2B contracts concerning data sharing and, due to lack of support by stakeholders, has not led to any further legislative action. As part of the 'New Deal for Consumers' package of April 2018, the Commission has however proposed the introduction of penalties for violations of the Unfair Contract Terms Directive. This Directive also applies in principle within the scope of application of the GDPR. Unfairness control may be less needed where data subjects can directly rely on the rights of the GDPR. But Article 6(1)(b) GDPR, the Trojan horse of data protection, dispenses of the need to seek consent of the data subject where the processing of personal data is necessary for the performance of a contract. This may well invite businesses to try to circumvent the requirement of consent by contractual arrangements. In this regard, the analysis recommends a two-pronged strategy: on the one hand, the provision should be interpreted strictly, delegating cases where the data is provided as a counter-performance to the data processor and for making use of the data for a separable commercial purpose to Article 6(1)(a) GDPR, with the result that processing can only take place with the consent of the data subject. On the other hand, the rules of the Unfair Contract Terms Directive should be applied to protect consumers against unjustified denial of data protection rights and non-transparent contract terms regarding the use of data where data is arguably necessary to perform a contract.

5 Assessing the potentials of different access regimes

This last Part of the Study will focus on the future framework of the regulation of control and access to data generated by connected devices. Thereby, the reminder and larger part of the questions listed in the introduction (at 1 above) will be answered. In order to do so, this Part takes the form of assessing the 'benefits and disadvantages' of three different regimes that have either been created or are discussed from the perspective of consumers as regards access to data generated by connected devices. These three regimes are: (1) a potential data producer's right as discussed by the Commission in its European Data Economy Communication of 10 January 2017[570]; (2) access rights recognised by the GDPR[571]; and (3) additional access rights in the interests of the owners or long-term users of connected devices[572].

5.1 The potential data producer's right

To assess the benefits and disadvantages of a potential rights system is not an easy task. In the European Data Economy Communication of 2017 and the accompanying Staff Working Document, the Commission has given little, and even contradictory, information on how such a new right's systems should be framed legally. More importantly, before entering an analysis of the design of such a new right, the preliminary question to be answered regards the need and justification as well as the functions of such a right. As Kerber rightly points out, the Commission is raising policy questions that first require an economic analysis of the market failures, and only after having identified these failures, the question can be answered on how these failures can be best remedied by legal rules.[573] In fact, the Commission advocates specific objectives when discussing a potential data producer's right. But this does not automatically mean that these objectives are convincing and that the Commission has not overlooked other objectives that would deserve consideration. The following analysis will therefore take a more open and legal approach. For the assessment of the benefits and disadvantages of a potential data producer's right, it is most important to discuss the potential objectives of such legislation by also looking beyond the goals advocated by the Commission. Then, from a legal perspective, the question will be discussed whether and how a data producer's right can be designed to reach these goals. The analysis thereby builds on the policy considerations of Parts 2 and 3 of this Study. The analysis of the existing legal situation in Part 4 is important to the extent the assessment of new legislation has to take into account the interaction with already existing rules. In this regard, a major question concerns the role of data protection rules.[574]

a) The objectives of a data producer's right

In the European Data Economy Communication, the Commission puts forward the idea of a data producer's right as a new property right of the owner or long-term user of non-personal machine-generated data.[575] In contrast, the Commission in the Staff Working Document (SWD) considers other options of attributing this right, namely, to the manufacturer of the connected device or to

[570] Hereby answering Questions 3 and 4 listed in Part 1 above.

[571] Hereby answering Question 5 listed in Part 1 above.

[572] Hereby answering Questions 6, 7 and 8 listed in Part 1 above.

[573] Kerber (n 51) 109, 111.

[574] Answering Question 4 listed in Part 1 above.

[575] European Data Economy Communication (n 9) 13.

this manufacturer and the user of the device as co-owners, yet, with the important limitation to users as economic operators.[576]

The reason for this is that, in the Communication and the SWD, the Commission seems to adopt diverging views about the functions of the right. In the SWD, the Commission Staff follows a more classical approach based on an incentive theory. The right should be allocated to the person that has invested the major resources in the creation of the data.[577] In contrast, in its Communication, the Commission states that such right would aim 'at clarifying the legal situation and giving more choice to the data producer, by opening up the possibility for users to utilise their data and thereby contribute to unlocking machine-generated data'.[578]

Following this latter approach, the objectives of this right can be described as two-fold: first, the Commission intends to increase legal certainty. In this regard, the Commission seems to share the general assumption according to which property rights can promote transactions by increasing the certainty about how economic assets are allocated among market participants. Second, the data producer's right is conceived as legislation to serve the interest of data user's in getting access to data.

The motivation of the Commission to argue in favour of a data producer's right of the owner or long-term user of a connected device seems to be based on a very specific market failure, according to which the owners or users depend on access to data but are confronted with resistance by the manufacturer who is unwilling to provide access for free. Hence, from a market-failure perspective, the Commission does not simply seek to serve the individual interests of the purchasers and long-term users of such devices. The proposal for a data producer's right has to be read and understood against the backdrop of the general goals of the free-flow-of-data initiative and the problems to which it is meant to respond more globally. In this general perspective, the Commission assumes that, on the one hand, to generate maximum benefit from the large diversity of machine-generated data, market players are in need of access to the datasets in which such data is included and, on the other hand, that those who control these datasets will often keep the data to themselves and analyse them 'in silos'. Accordingly, the Commission concludes that access and transfer of machine-generated raw data is central for the emergence of the data economy.[579] The Commission sees the data producer's right not only as a means to create access of the owner or long-term user of a device to the data, but also as a means to facilitate access of third parties to the data. The Commission explicitly argues that *de facto* control over the data allows manufacturers and service providers to prevent the user of a device to license the use of the data to a third party.[580] Thus, the data producer's right appears as an important element of a broader legal framework of promoting access do machine-generated data for the purpose of allowing big data analyses.

Yet enhancing access to data is only a means to another end, namely, of promoting new, innovative services, improving products and production and supporting decision-making by using data.[581] To attain these final goals the Commission formulated a series of sub-objectives that are not without tensions.[582] Improving access to machine-generated data and facilitating data sharing are only the first two of these objectives. The objective of protecting the investment of market players to create the necessary incentives for investment in new, innovative products and services counts more, in

[576] European Data Economy SWD (n 9) 35.

[577] Ibid.

[578] Ibid.

[579] Ibid, 8.

[580] Ibid, 10.

[581] As formulated by the Commission in the first paragraph of Part 3 of the Communication on data access and transfer. Id, 8.

[582] Id, 11-12.

line with the Commission SWD, for protecting the interests of the manufacturers of the connected devices. In the same vein, the Commission confirms the need to protect against the disclosure of confidential data especially to competitors. As a third category of objective, the Commission also argues to take unequal bargaining power of companies and private individuals into account, especially where SMEs and consumers have to face lock-in situations.

But, for the purpose of assessing the pros and cons of a data producer's right, the Commission's analysis still remains incomplete since it does not take into account the objectives that should generally be considered in the field of intellectual property. In particular, recognition of a new intellectual property right as a right *in rem* will necessarily create new exclusivity and allow the rightholder to exclude others from using the subject-matter of protection.[583] Such exclusion produces social costs and is in need of a justification to guarantee that the trade-off for society will at the end be positive. Especially, a data producer's right must not be discussed without taking into account the potential costs arising from creating potential impediments to free flow of information.

Indeed, the classical justification for the creation of an intellectual property right would be to create incentives for the rightholder to invest in the production and commercialisation of the subject-matter of protection, to stabilise transactions and to increase legal certainty on the allocation of rights among market participants. Promoting access to the subject-matter of protection is normally not part of the objectives for vesting a new intellectual property right in the person seeking access to the subject-matter. Rather, access is typically regarded as a countervailing interest of third persons, which is therefore taken into account in the framework of exceptions and limitations of an intellectual property rights system.[584] In sum, traditional intellectual property would in fact argue in favour of allocating the right to the 'investor' and take care of the interest of others in access to the data in the framework of the exceptions and limitations. Hence, an alternative approach would consist in vesting the data producer's right in the manufacturer of a connected device and provide for an access regime in favour of the purchaser or long-term user of the device as part of this legislation. Respective exceptions and limitations could also be integrated as mandatory contract rules governing the rights and obligations between the manufacturer, on the one hand, and the purchaser or long-term user (lessee) of the device, on the other. Mandatory exceptions and limitations could also be used as a benchmark for assessing the unfairness of contract terms on the use of data and thereby make it more difficult for the manufacturer as the data producer to restrict the legitimate interests of other persons in access to data.[585]

The idea of the Commission to promote access to data by recognising an intellectual property right for the owner or long-term user of the device based on the particular interest this person has in access to the data breaks with classical approaches to intellectual property legislation. Whether this is a viable innovation in intellectual property law or simply a flawed approach based on fundamental misunderstandings of intellectual property law, will depend on how such data producer's right can be designed more concretely.

While above-mentioned justifications are of an economic nature, it is also possible to categorise the 'functions' of any intellectual property rights system from a more legal perspective. More recently, Specht discussed the relationship between data ownership rights in personal data and data protection. She thereby identified three reasons why the existing data protection rules collide with the requirement for a functioning data ownership system.[586] By relying on this analysis, three general requirements can be formulated that an intellectual property should meet in order to be

[583] See also Kim (n 8) 705 (pointing at the character of data as non-rivalrous goods and concluding that restrictions on the consumption of such goods with therefore be inefficient in principle).

[584] As also emphasised by Denga (n 94) 1372.

[585] On these justifications see already Drexl (n 51) paras 73-102.

[586] Specht (n 192) 1040.

adopted. These three requirements relate to (1) attribution, (2) participation and (3) dissemination in the following sense: first, intellectual property rights have to clearly identify the object of protection and to attribute the right in this subject-matter to an individual person with legal certainty. Second, legislation has to guarantee that the rightholder can realise participation in the income generated from the economic exploitation of the subject-matter of protection. Third, legislation has to enable unrestricted use of the rights not only for the rightholder, but also third persons.[587] The latter requires that contracts on the transfer and licensing of the use of the subject-matter be in principle allowed and enforced. It has to be emphasised that this framework, does not make the economic justification of a new intellectual property right dispensable. Rather, this standard should be used as a complement to test the quality of legislation. It will dispense neither from the need to show that there is a market failure as a justification for the introduction of a new data producer's right nor that the concrete legal rules adequately remedy this market failure, striking a proper balance in terms of a positive trade-off for society.

In the following, the analysis will turn to the legal design of a potential data producer's right and assess whether the individual elements of such a rights system meet the abovementioned requirements.

b) Limitation to non-personal machine-generated raw-data

The Commission discusses a data producer's right only for non-personal machine-generated raw-data as the subject-matter of protection. In this regard, there are two fundamentally different dimensions that need to be considered. The first one is whether there is an economic justification for data ownership in machine-generated data in the first place and, on the other hand, whether it actually makes sense to limit protection to non-personal raw data.

With respect to the economic justification of a data ownership right, it is doubtful whether the traditional incentive theory of intellectual property can be relied upon in the first place. The new data economy is not characterised by a problem of under-production of data.[588] Rather, the growing perception that, in a world of big data analytics, any data could prove valuable seems to work as an additional driver for collecting and storing more data than ever. In the specific case of connected devices, machine-generated data, which can also be used for secondary purposes, is just a by-product of the main business of the manufacturer to provide customers with better products and more utility.[589] Especially for connected devices, the major incentive is strongly linked with the main business of the manufacturer. The major driver in many industries where firms nowadays invest heavily in 'digitising' their products is competitive pressure. Firms that do not take part in the digital transition may soon the risk of having to leave the market. In addition, the investment made into the development and design of the connected device, including the sensors and the software that collect and process data, can be recouped by charging a price for the sale and use of the device. Additional intellectual property rights to recoup the investment in the development of the device and the collection of the data are therefore not needed. The situation may be slightly different as regards the incentives for manufacturers to license the use of 'their' data in secondary markets. For that purpose, the manufacturer may need to further invest in the data, for instance by guaranteeing

[587] Zech (n 44) 141, prior to the adoption of the GDPR, even seemed to go a step further by arguing that data protection does not equal data ownership since the data protection rights cannot be transferred to the data controller.

[588] Authors typically argue against sufficient evidence of suboptimal production of data: Kerber (n 2) 992-93; in the same vein Heymann (n 26) 653; Mezzanotte (n 45) 171-72; Florant Thouvenin, Rolf H Weber and Alfred Früh, 'Data ownership: Taking stock and mapping the issues' in Matthias Dehmer and Frank Emmert-Streib (eds), *Frontiers in Data Science* (Boca Raton, FL: CRC Press 2017) 111, 116; Weber and Thouvenin (n 44) 53 and 63.

[589] The existence of an incentive problem of the manufacturers of connected devices is also denied by Kim (n 8) 703-704.

the quality of the data, getting consent to using personal data or for anonymising personal data[590], not to mention the costs of guaranteeing data security and secrecy. But *de facto* control will in principle allow the manufacturer to also recoup such costs by charging a price for the use of data in such secondary markets.

The other question is whether a data ownership right is needed to stabilise data markets in which data is traded.[591] However, the potential market failures that could negatively affect and prevent trading of machine-generated data are not so clear.[592] Authors doubt that the reasons have to be found in a lack of ownership.[593] It is much more likely that markets for trading data are mostly affected by information asymmetries concerning the quality, provenance and value of data. Intellectual property could perhaps help overcome the problem of the so-called information paradox.[594] This paradox describes the problem that the person seeking access to information cannot assess the value of the information without getting access to it. Once this person has access to the information, it will however no longer be willing to pay a price for access. Yet, whether data ownership is the only way to solve the information paradox, is questionable.[595] A simple alternative consist in appointing a data analytics trustee that runs sample tests on the quality and utility of the dataset without providing access to the potential customer to the concrete information. The quality and utility of datasets could also be tested by the data holder and described in general terms.

Hence, the question is what data ownership can add to stabilise transactions beyond exclusivity based on *de facto* control. A similar and well-known example for this problem relates to the licensing of know-how, which is only protected as a trade secret. Know-how licensing is typically more fragile since the licensing agreement can only impose *inter partes* confidentiality obligations on the licensee without absolute legal guarantees that the licensor can also sue a third person that uses the know-how after undue disclosure of the know-how.[596] Whether transactions relating to trade in data are equally affected by such instability, is not that clear. Without additional protection there is at least a risk that the first buyer could immediately resell the data, without any possibility of the initial *de facto* holder to bring an action against the third-party buyer.[597]

Whether data ownership is recognised or not, the fundamental problem will always be one of monitoring. Without data ownership the *de facto* holder who grants a licence for the use of data will be in need of monitoring the conduct of the licensee in order to make sure that the licensee does not break any confidentiality obligations. Where violations of the licensing contract can be detected, the licensor can sue the licensee for damages based on contract law. Trade secrets protection may add another layer of protection on top of contract law claims against the direct buyer and, under certain conditions, it can also provide the data licensor with direct claims against third persons.[598] Conversely, where such monitoring is not possible, it is hard to imagine that data

[590] On these costs see Kerber (n 51) 117.

[591] See also Kerber (n 2) 593-95; id (n 51) 120-23.

[592] See in particular Duch-Brown, Martens and Mueller-Langer (n 36) 36-41.

[593] Kerber (n 51) 121.

[594] As coined by Kenneth J Arrow, 'Economic welfare and the allocation of resources for invention' in National Bureau of Economic Research (NBER) (ed), The Rate and Direction of Inventive Activity (Princeton University Press, 1962) 609. The information paradox as a basis for a data producer's right is relied upon by Zech (n 44) 145.

[595] On the current economic literature see Duch-Brown, Martens and Mueller-Langer (n 36) 36. Kerber (n 2) 994 assumes that the information paradox is not a huge problem in this context, since the relevant data could be sufficiently circumscribed by the data holder to inform a buyer.

[596] On the application of Trade Secrets Directive in such a case, see above.

[597] This is identified as the major issue by Kerber (n 2) 994.

[598] This is also noted by Kerber (n 2) 994 (in addition trusting technical protection measures as a means to prevent proliferation of data in violation of the licensing agreement). On trade secrets protection, see the comprehensive analysis at 4.4 below.

ownership will help. In such instances, the monitoring problem does not only regard the conduct of the licensee, but of all market participants as potential infringers.[599] In a world of big data analyses where it will become increasingly difficult to trace back accessible information on business conduct of a firm in the market to the use of specific data, originating from an individual data producer, especially where data analytics is used to enhance internal decision-making. The expectation that data ownership rights could be used against third persons becomes even more an illusion where computer programs based on machine learning make decisions and where it is no longer possible for programmers to understand which data was used for making a particular decision. In sum, it is very unlikely that data ownership could create a sufficiently strong backbone for protection against misappropriation of data by third persons.[600]

The argument according to which recognition of data ownership rights can produce more transparency and legal certainty in the market by clear allocation of the rights in the market, also has to be rejected. As compared to the alternative of leaving the situation as it is, the introduction of a new property right will force other market participants to monitor and clear rights to do business in the digital economy. In the case of recognition of a data producer's right for the owner or long-term user of a connected device, companies and other entities taking a licence for the use of data from a manufacturer of connected devices would have to make sure that they do not violate the data producer's right of third persons. This appears as a most burdensome task since the licensee in such a case may be completely unable to identify the numerous data producers who will eventually claim rights. Hence, introduction of a data producer's right would create considerable costs of monitoring and managing the licensing of rights as well as litigation costs arising from disputes concerning the infringement of such rights.

The problems of legal uncertainty caused by a potential data producer's rights would be even more severe, if the data producer's right will only applied to non-personal machine-generated raw-data. With both limitations the Commission tries to counter arguments against data ownership, namely, that ownership should not exist in information, i.e., on the semantic level of data, and that the data protection rules should be guaranteed.[601] But defining the subject-matter of protection in this way fails to meet the requirement of attributability of the right to an individual person. The problem arises both from the attempt to protect raw data on the mere syntactic level and from the exclusion of personal data.

In general, property law requires that the object of ownership is clearly identifiable. In some instances, intellectual property law uses registration systems to increase transparency in this regard. Property in raw data, however, will only be protected in form of bits and bytes, whatever information can be taken from it. In the case of data generated by connected devices, if owned by the owners or long-term users of the device, these data may well end up as aggregated data in larger datasets of the manufacturers. If the manufacturer makes available such data to another person, attributability would still require that the data used remains identifiable for the matter of rights-clearing and monitoring of infringements. By simply looking at the semantic level of the encoding, this will not be guaranteed. At best, it will be possible to allocate ownership in specific raw data by

[599] This may be overlooked by Kerber (n 2) 994; id (n 51) 122 (arguing that property rights reappear as an 'interesting policy option' where the data holder cannot monitor the conduct of the licensee).

[600] Ultimately, Kerber also refrains from claiming introduction of a data ownership right, yet based on the lack of empirical evidence that the major problem for the working of data markets is the absence of such data ownership. See Kerber (n 2) 994-95. While the existence of the market failure which the data ownership right could remedy has not yet been proven—especially Kerber does not see any evidence that data licensees break their contractual confidentiality obligations on a systematic basis—Kerber argues, that the ownership right could not remedy any of the other market failures, such as the low quality of data or insufficient data interoperability). See Kerber (n 51) 122-23.

[601] See also the analysis at 2.4 c) above.

looking at the information that they encode.[602] In addition, this will only work if the information can be traced back to a single source. But exactly where this is possible ownership rights in raw-data runs the risk of undermining the free-flow of information, because the information encoded in the raw data cannot be accessed anywhere else.

Attributability would also be undermined by the difficulties to distinguish between personal and non-personal data. The exclusion of raw data encoding personal data from the subject-matter of protection would require a judge to assess ownership of the data on the syntactic level by distinguishing the information it contains on the semantic level. Apart from this burdensome task, the lack of attributability arises from difficulties to clearly distinguish between personal and non-personal data. This is why Specht argues against ownership of the data subject in personal data.[603] The problem is not only the breadth of the concept of personal data in Article 4(1) GDPR, which also covers information on a merely 'identifiable' person. It is more problematic that non-personal data can become personal data if the information is read in the context with other non-personal data that suddenly makes it possible to identify a person. Hence, even where personal data got anonymised, big data analytics may manage to retrieve the person.[604] Hence, in a world of big data analytics a lot of non-personal information is potentially personal data. This practically excludes the criterion of personal data both as a positive requirement for data ownership in personal data[605] and as a negative requirement to exclude data ownership in personal data.

To solve this last problem of attributability, the data producer's right would need to be extended to also cover personal data. This is legally not excluded as such. Rather, this solution would create a cumulation of rights of potentially different persons protecting slightly different subject-matter. In fact, the Commission also confirms that machine-generated data can be personal or non-personal and that in the former case the GDPR needs to be applied.[606] But this would also mean that the licensing of personal data is heavily burdened with the risk that the data subject can withdraw consent at any moment[607] and thereby torpedo the licensing of the data by the data producer.[608] This would even apply in a case where the data producer has successfully requested consent to enable licensing. The Commission additionally argues that the licensing could be facilitated by the anonymisation of the data. As just argued, however, reference to anonymisation wrongly pretends to be able to draw a clear line between anonymised data as non-personal data, on the one hand, and personal data, on the other. More importantly, the Commission fails to explain why anonymised data can still be considered machine-generated data. At best, this can only be argued where personal data is deleted from the dataset leaving the other data intact. In contrast, where anonymisation consists in the statistical aggregation of personal data of a large group of data subjects, such aggregation could well be perceived as a data processing which leads to new data.

---

[602] This is also noted by Wiebe (n 102) 882 (therefore, arguing that ownership in raw-data tends to shift back to the semantic level).

[603] Specht (n 192) 1042.

[604] Weber (n 87) 144. It is therefore not guaranteed that anonymisation will make the person 'non-identifiable'. This is why Oostveen 305-306 neatly distinguishes between anonymous and de-identified data. Only, in the latter case the data will be 'non-identifiable' and, hence, not be covered by the rules of the GDPR. Oostveen (n 122) 305-306 and, in particular, n 70. In a similar vein, Mark Elliot, Kieron O'Hara, Charles Raab, Chrstine M. O'Keefe, Elaine Mackey, Christ Dibben, Heather Gowans, Kingsley Purdam and Karen McCullagh, 'Functional anonymisation: Personal data and the data environment' (2018) 34 *Computer Law & Security Review* 204 argue in favour of the concept of 'functional anonymisation', that takes into account the 'environment' to make sure that there is no available additional information that can make the person identifiable.

[605] Against the use of the criterion of personal data for the framing of a data ownership right, see also Specht (n 192) 1047.

[606] European Data Economy Communication (n 9) 9.

[607] Ibid, 13.

[608] Specht (n 192).

The latter obviously has to be argued since the aggregated data will be encoded in form of new raw data that was not created by the connected device.

Finally, the fact that machine-generated data may be processed, and often needs to be processed before being licensed, raises yet additional problems of attributability. It will be extremely difficult to distinguish between protected original machine-generated raw data and unprotected processed data in the same dataset.

c) Identifying the data producer

As mentioned, the objectives of the data producer's rights would also have to define in whom those rights should be vested. From an economics perspective, clear allocation of the data producer's right creates major problems, since many different persons may contribute to the generation and subsequent processing of data within networks of value-generation.[609] In addition, economic justification of a specific allocation of the right also remains insecure, because the debate has so far not yet conclusively answered what kind of economic objectives the data producer's right is supposed to achieve. Both problems explain why the Commission's discussion of who should be recognised as the data producer is largely characterised by internal contradictions and inconsistencies.

As regards the Commission's idea to recognise a data producer's right of the owner or long-term user of a connected device, the economic justification of such choice is particularly questionable. To call this person the 'data producer' seems to go back to the earlier proposal by Zech, to grant the right to the 'economically responsible data producer'.[610] But Zech also notes that such allocation would not necessarily respond to the interests of the parties concerned.[611] What he seems to aim at is allocating the original data ownership with sufficient legal certainty irrespective of who is in *de facto* control of the data.[612] In a second step, Zech leaves it to contract law to achieve an interest-based allocation of rights even in form of an *ex ante* assignment of the rights.[613] Accordingly, in the case of data collected by farming machines, the data producer's right would go to the economically responsible operator of the farming machine. If this is an independent service provider, it would be for the farmer to secure these rights based on contract law when hiring the service provider to get access to the data the farming machine is collecting by being used on its land.[614]

---

[609] From an economic perspective, see Kerber (n 2) 995-96.

[610] Zech (n 44) 145 (using the term '*wirtschaftlich verantwortlicher Datenerzeuger*'). To identify the act of 'producing' data, Zech relies on the so-called 'script act' as the act that ultimately leads to the digital encoding of information. See also Becker (n 25) 256. This would typically be the act of the user of a connected device, since it is this use the leads to the generation of data.

[611] This is also criticised by Wiebe (n 102) 883.

[612] In a later publication, Zech relies on two additional reasons; see Zech (n 90) 324-25. The first one is the analogy to certain related rights where the right is also vested in the 'producer', such as in the case of the sui generis database right, the phonogram producer's right or the German press publisher's right. While this is only a systematic reason, the second reason is more policy-oriented. Zech argues that allocation of the right to the data producer would lead to parallelism with the allocation of economic risks and benefits. Yet Zech also admits that allocating the economic risk and benefits in cases where connected devices are used in rather complex network structures may be a most difficult task.

[613] Zech (n 44) 145.

[614] Ibid. Hereby, Zech trusts the working of contract law, but simultaneously overlooks that the manufacturer can secure ownership of the data through *ex ante* assignment when selling the machine. According to the principle of priority, the first *ex ante* assignment would prevail. Under the second contract with the farmer, the operator of the machine (data producer) would no longer be able to transfer any rights. This shows that allocation of data ownership rights to another person than the manufacturer will not work, if the manufacturer has sufficient bargaining power to claim the rights. On the insight that ownership allocation cannot overcome the unequal distribution of bargaining power where the right is

In contrast to Zech, the Commission, at least in its European Data Economy Communication, seems to prefer allocation of the data producer's right to the owner or long-term user for a functional reason, namely, to use the interests of this person in licensing the use of the data to third persons as a means to promote access to data. One way of justifying such choice, would be to consider the owner or long-term user of the device, because this person can make the most efficient use of the data, including enabling others to use the data based on licensing. Such initial allocation would at least reduce transaction costs.[615] Yet such justification does not appear fully convincing, since also the manufacturer could make very efficient use of the data by licensing the aggregated data collected and processed by all the devices he has initially manufactured.

If applicable at all, the incentive theory of intellectual property right would argue in favour of recognising an intellectual property right for the manufacturer rather than for the owner or user of the connected device. The investment in the development of both the connected device and new and innovative data services linked to the use of the device is made by manufacturer.

In sharp contrast to the text of the Communication, the Commission Staff Working Document adopts a classical incentive theory.[616] By relying on the investment done and the resources invested in the creation of the data,[617] the Commission Staff focuses on the contribution of the manufacturer of the connected device for allocation the data producer's right, but still tends to consider at least the economic operators using connected devices as co-producers of the data. In sum, the Commission Staff describes both parties as holders of 'joint rights'.[618]

However, also the idea of considering an economic owner or user a 'co-producer' is to be criticised.[619] The Commission Staff is not very convincing in arguing that, by paying a price for the device, the purchaser or user of a connected device is making an investment in the production of the data. This applies equally to economic operators and consumers as owners or users of the device. The mere fact that the device produces data when it is used does not make the payment for the device an investment in the generation of data. The investment argument requires that the investor first incurs the costs with the expectation that, based on the exclusive property right, it will later be able to recoup these costs. In contrast, also in the case of an economic operator buying a connected device, the investment is not made for the purpose of producing data that can be commercialised by licensing to third parties, but as part of the purchaser's main business. A farmer is buying a smart farming machine in recognition of the higher utility of this machine and the expectation to increase yield. Neither from a technical, financial nor an organisational perspective, the owner or long-term users is 'producing' data as part of its business. The only connecting point with the generation of data consists in the fact that without using the device, data would not be generated. Such use, which is the very motivation of the user for the decision to purchase a connected device, cannot be regarded a sufficient justification to allocate property rights to the user.[620] Use of the device, including the man power for using the farming machine, is not an

freely transferrable, see at 2.3 f) above. See also Kerber (n 2) 996 (arguing that vesting smaller firms with alienable property rights cannot solve the market failure of unequal distribution of bargaining power).

[615] See Wiebe (n 102) 883.

[616] Which is doubtful since there is no evidence for the need of additional incentives for the generation of machine-generated data; see a) and b) above.

[617] European Data Economy SWD (n 9) 35.

[618] Ibid.

[619] See also the criticism expressed by Kim (n 8) 703-704 (arguing that this would lead to a 'standstill' situation failing to achieve the goal of unlocking data).

[620] See also Heymann (n 26) 654 (for similar reasons criticising the idea that the data producer's right should be allocated to the person using a farming machine based on the mere fact that this person is using the device and thereby influencing which data will be generated); against Zech (n 44) 143.

investment in the future, but rather the benefit that the farmer seeks and gets from the connected machine.

In particular, the arguments of the Commission do not justify making a distinction between economic operators and consumers as users of connected devices with the result of excluding consumers as co-producers of data. Quiet on the contrary, in the case of consumers, there is no other business in which they could invest than the production of data. But especially the investment made by a consumer buying a connected car because she appreciates the higher level of convenience and safety should not be considered sufficient to redefine the consumer as a person operating a data production business, with all the implications such conclusion could have in other fields of the law, such as tax law in particular. The consumer is still using the car for private purposes; the data that the car is producing, will largely be needed to operate the device in the first place. The mere possibility that such data can also be commercialised in secondary markets should not change this perspective.

The reason why the Commission wants to allocate such a right to the owner and long-term user is not based on an intellectual property consideration but, quite on the contrary, on the fact that the owner or long-term user of the device may have a legitimate interest in access to the data, whereas the manufacturer may abuse its position as a *de facto* data holder to prevent access for strategic reasons. This shows that, in terms of intellectual property protection, the owner or long-term user—whether this is a business operator or a consumer—is much more in the situation of somebody who seeks a compulsory license to use the data.

d) The exclusive right to use the data

The Commission is rather silent on the scope of protection. In its European Data Economy Communication, the Commission describes the data producer's right as 'a right to use and authorise the use of non-personal data'[621] and argues that otherwise the user would often be 'prevented by the manufacturer from authorising usage of the data by another party'.[622]

Although the data producer's right is primarily advocated by the Commission as a means to access data, the possibility to enhance access by licensing the right to third persons seems to lead the Commission to the conclusion that this right should encompass the right to exclude others from the use of the data.[623] This is further confirmed by the accompanying Staff Working Document, which describes the data producer's right as a right *in rem*, hence, as a right that can be enforced against any third party with the effect of excluding such party from further use of protected data.[624]

Even in the Staff Working Document, the Commission is not elaborating on how a right to exclude others from the use of data could in fact enhance data access. The problem is that a licensing agreement under which the owner or long-term user of a connected device authorises the use of the data by another party by itself does not provide the licensee with access to the data held and controlled by the manufacturer. If the manufacturer still refuses access to the data, the licensor could be held liable for non-performance of the contract. This shows, that the right to exclude others may be too limited to facilitate access. Upfront, it only adds a layer of legal exclusivity—a right to exclude—of the owner or long-term user of the device to the already existing *de fact* exclusivity of the manufacturer. This shows that the recognition of an exclusive data producer's

[621] European Data Economy Communication (n 9) 13.

[622] Ibid, 10.

[623] Exclusivity of use, including the use of data for the purpose of data analysis, is also listed as part of the data ownership concept presented by Zech (n 44) 139.

[624] European Data Economy SWD (n 9) 33.

right cannot work as a substitute to data access rights. Rather, a new data producer's right of the owner or long-term users of a connected device will only manage to achieve its given goal of promoting access to data if legislation on the data producer's right would be accompanied with a data access right of the owner and long-term user of the device.

Of course, if the owner or long-term user of a device was recognised as the sole holder of the data producer's right, based on the threat of claiming injunctive relief, the exclusive right could be used as a leverage against the manufacturer to get access to the data. In other words, the owner or long-term user could offer the manufacturer to license the use of the data for getting access to the data. However, this argument overlooks that the owner or long-term user of the device has a personal interest in continued use of the data by the manufacturer, since this is a condition for undistorted use of the device. In substance, this is also noted by the Commission Staff hinting at the fact that surveillance of the working of connected devices is in the legitimate interest of the manufacturer and that the manufacturer, as a matter of product liability law, may even be under a legal obligation to monitor the working of the device.[625] Therefore, the Commission Staff argues for a respective exception in favour of the manufacturer of the device.[626] Still the owner or long-term user of the device could rely on injunctive relief against the commercialisation of the aggregated data by manufacturers, in which the data originating from the individual user has been integrated, in order to enforce access. Yet such injunctive relief runs counter to the very idea of promoting access to data, since licensing of access to the large aggregated datasets of manufacturers is not less likely to produce benefits to society than separate licensing of access to the data generated by single connected devices.[627] Granting an injunction against the licensing of the aggregated datasets of manufacturers in the interest of a single owner or long-term user of a connected device may also run counter to the principle of proportionality.[628]

Moreover, given the need to use the data generated by the device to operate the device and to be able to license the use of the data to third parties, the manufacturer would typically have to secure any exclusive rights in the data originally attributed to the owner or long-term user of the device when the connected device gets sold or leased to the end users. From an intellectual property perspective, there is nothing wrong with assigning or licensing the exclusive right. The Commission Staff Working Document seems to argue that it would be possible that, depending on the market conditions and the bargaining position of the rightholder, the data producer's right would be 'traded away to the actor(s) who most benefit from its use'.[629] Assignability clearly corresponds to the requirement of dissemination of intellectual property systems and the goal of free flow of data. Even where the legislature attributes an intellectual property right to a specific person, assignability and the possibility to grant licences should allow the market to maximise use of the subject-matter of protection.

As indicated by the Commission, the situation however changes fundamentally where bargaining power is distributed unequally. Indeed, unequal distribution of bargaining power between the manufacturer and the purchaser or the user of the connected device is much more a problem than lack of intellectual property protection. Although the manufacturer will not necessarily always hold superior bargaining power—especially in case of the supply of a connected device by an SME to a large industrial customer, the situation may even be the other way around—, it will typically be the manufacturer who decides how and at what terms a connected device is sold to consumers and other customers. Hence, for cases in which the manufacturer holds superior marketing power, it is

[625] Ibid, 35.

[626] Ibid.

[627] On the need to guarantee to the aggregated data of manufacturers see also Drexl (n 9) 235.

[628] According to Art 3(1) IP Enforcement Directive (n 120) remedies for the infringement of intellectual property rights need to be proportionate.

[629] European Data Economy SWD (n 9) 36.

important to understand that the data producer's right vested in the purchaser or long-term user of the device would fail to achieve the goals for which the Commission considers its introduction.[630] A way to address this issue could consist in limiting the possibilities of the data producer to assign and licence the right, especially by only allowing non-exclusive licences. However, this could still considerably reduce the capability and the incentives of the manufacturer of the connected devices to open up access to its larger sets of aggregated data, since, under such a regime, the manufacturer would be unable to grant exclusive (sub-)licences to its licensees.

In sum, an exclusive data producer's right for the owners or long-term users cannot be expected to produce any significant benefits. It will not necessarily enable the rightholder to grant licences for the use of the data to third parties, if it is not accompanied by a right of access to the data which is still under the *de facto* control of the manufacturer. Quite the contrary, the rightholder will in most cases assign the right in the data at the time of purchasing or leasing the device.

e) The right to participate in the economic income from the exploitation of the data

Another question regards the allocation of the economic value of data. Intellectual property law has the function to allocate the income generated through the commercialisation of the subject-matter of protections to the rightholder. The following analysis questions whether a data producer's right will be capable of fulfilling this function.

First, if the data producer's right were attributed to the owner or long-term user of the device, but under the given market situation the manufacturer holds a position of superior bargaining power, the data producer's right would still allocate the economic value of the data to the manufacturer, since the latter would have the power to require the rightholder to assign the right or grant an exclusive licence without adequate remuneration. To remedy this problem, the legislature would have to adopt additional mandatory contract rules guaranteeing fair remuneration for the rightholder. Such rules exist as part of copyright legislation in some jurisdictions; but the lesson to be learned from copyright law is that such legislation for being effective faces huge obstacles, not least by requiring a system of price-control. In the context of a data producer's right of the owner or long-term user of a connected device, this would not be any different. The 'data producer' already has to pay a price for acquiring or using the connected device. Therefore, in a market economy, the manufacturer could easily react to the introduction of a system guaranteeing fair remuneration for the use of the data by increasing the price charged for the device. Indeed, from an economic perspective, the transaction concerning a connected device should not be split into separate contracts on the sale of a connected device, on the one hand, and the licensing of the data producer's right to the manufacturer, on the other hand. The customer does not just buy a whatever device but a 'connected' device that comes with the capacity to produce data that is typically needed to generate higher utility by using this device. Therefore, from an economic perspective, it is correct that the manufacturer charges one price for the connected device and its use, and no re-payment seems justified for the use of the data by the manufacturer. It should remain the task of the market to identify the appropriate price.

Secondly, whoever is chosen as the data producer, the question of the status of 'derivative data' needs to be addressed.[631] From an economic perspective, the question is whether the data producer's right should also produce streams of income for the producer of the original data, where data is processed and the processed ('derivative') data is then commercialised. This is a most important question since most value from machine-generated data will typically be generated

[630] See also Kerber (n 2) 996.

[631] This issue is ignored by Zech (n 44) sketching the need for and design of a future data producer's right.

through additional data analyses. Yet whether intellectual property rights extend protection to such 'derivative' markets, depends on the decision of the legislature.[632]

In copyright law, a derivative work—such as a translation of a novel—that is characterised by creative input coming from its author is considered a work that is separately protected under copyright law (the copyright held by the translator). Yet, to the extent that it still reproduces recognisable creative parts of the work, commercialisation of the derivative work also amounts to commercialisation of the original work. Hence, under copyright law, a translation of a novel cannot be reproduced and sold without the consent of both the author of the original work and the translator. The question of whether such a system should also be implemented with respect to a data producer's right, is not at all addressed by the Commission.[633] The Commission only mentions that there is a need for taking technical measures, such as watermarking, to make data traceable.[634] This may suffice to protect the data producer against integration of 'her' data in the datasets of third parties. Yet the more difficult—and economically more important—question regards derivative data, namely, as raw data that encodes derivative information gained through the analysis of data originally generated through the use of connected devices. This is of extreme importance, since, as seen further above,[635] machine-generated data will typically be treated and analysed to gain additional information for enabling quick, almost immediate, decision-making. In secondary data markets, data may be analysed for getting new information. Watermarking will not help in such cases, since the new information will be different and will be encoded in different raw data. Still, the fact that the generation of derivative data is dependent on access and use of pre-existing data could be taken as an argument to extend protection of the producer of the pre-existing data against generation and commercialisation of derivative data to prevent economic free-riding.

Yet such protection has to be rejected for the several reasons: (1) the right to participate in such secondary data exploitation does not create any benefits in terms of access. Quite the contrary, the secondary user would have to share income with the original data producer, with the potential effect of reducing incentives of this secondary user, especially the manufacturer of the device, to invest in the commercialisation of its larger and more valuable datasets. (2) Secondary use will be extremely difficult to detect, especially in a world where data are analysed by computer programs based on artificial intelligence. (3) Protection against secondary use will collide with the public interest in free flow of information. The negative effects on free flow of information through direct protection of the underlying raw data would be extended to all information that is derived from data originally generated by connected devices. In addition, the exclusionary effects would even be multiplied if one took into account that, based on big data analytics, new information is typically generated through correlations between different pre-existing pieces of information. If the raw data in which such the different pieces of information are encoded belonged to different 'data producers', extension of such ownership to derivative data would lead to the question of whether these original data producers now have to be considered co-owners of the new data. The number of 'data producers' would constantly increase by each and every step of data analysis. (4) The question is not only whether the original data producers hold data ownership rights in the derivative data. The question is also whether a legally separable data ownership right should be recognised for the producer of derivative data—similar to the copyright of the translator in a translated novel. In German legal writing, based on the rules of the Civil Code concerning property in movable tangible objects, it has been argued that only the person who creates new data through the analysis of pre-existing raw data should be considered having a property right in the new data, whereas the owners

[632] See also Denga (n 94) 1373 (arguing that such protection is not mandatory for an intellectual property system).

[633] But it is argued by Fezer (n 31) 65, according to whom his more recently recommended representative data ownership right should extend to derivative data even in the case where personal data gets anonymised, irrespective of additional data ownership rights of the data processor.

[634] European Data Economy SWD (n 9) 36.

[635] See at 2.4. a) above.

of the pre-existing data should have no rights in the new data.[636] This analogy can be criticised in some regards.[637] Yet it puts the finger on a key problem. If, as suggested by the Commission, the data producer's right in the raw data generated by a connected device were vested in the owner or long-term user of the device, the legislator should also answer the additional question of how to balance the interests of this data producer with the interest of other persons who will further process the data. To guarantee equal treatment of all persons investing in the data generation and processing, it can hardly be argued that the owner or long-term user should have property rights in the raw data, maybe even extending to derivative data, while those who make an investment in the creation of derivative data, namely, the data analysts—a concept that would also need be further defined[638]—would be excluded from protection. Yet such cumulation of property rights would considerably increase the exclusionary effects of data ownership on access to information, while the positive effects in terms of additional incentives for investment in data production and processing remain questionable and even insignificant.

Thirdly, even a more moderate, less exclusionary regime of economic participation of the data producers in the income generated from secondary uses based on statutory remuneration rights has to be rejected. It is true that exceptions and limitations could remedy the exclusionary effects arising from multiple data producer rights, especially if original data producer rights would also be recognised for derivative data. Following the example of copyright law, statutory remuneration rights could be introduced as a means to guarantee participation of the data producers, including the owners or long-term users of connected devices, in the income generated through the commercialisation of data. This necessarily leads to the question of whether the model of collective rights management can be used for administering such rights.[639] In fact, collective rights management has been referred to as a way to guarantee economic participation of citizens in the economic exploitation of 'their' data.[640] Yet this idea has to be considered an illusion. Collective rights management organisations (CMOs) do not only have to negotiate tariffs with the users and collect remuneration, which is difficult enough. They would also be under an obligation to distribute the income to the data-producers in proportion to the use of the individual data. This requires, first, to identify the relevant individual rights and, hence, the specific raw data, and, secondly, assess the intensity of the use of these data. CMOs in the field of copyright law require rightholders notify their works to the CMOs as a starting point for administering the exploitation of the rights in such works. Yet it is hard to imagine how the myriads of raw data that connected devices generate can be identified, how such data can be reliably allocated to individual right holders and how the use of such data can be monitored. This problem would appear even less manageable, if protection were

[636] The relevant rule is Sec 950 Civil Code. According to this rule, a person who, through processing or transformation of one or more substances, creates a new movable item, will acquire the ownership in the new item. The owner of the pre-existing substances will not hold any property right in the new item, even where the original owner did not agree with the processing or transformation. According to Sec 951 Civil Code, the latter will only have a claim to be compensated according to the rules of unjust enrichment. The classical law school example is the case of a painter who uses canvas and colours owned by another person to create a painting. Even if the canvas and colours were stolen, the painter would acquire property in the painting. See Jürgen Ensthaler, 'Industrie 4.0 und die Berechtigung an Daten' (2016) *Neue Juristische Wochenschrift* 3473.

[637] See Josef Drexl, 'Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz' (2017) *Neue Zeitschrift für Kartellrecht* 339, 341.

[638] Possible candidates for becoming rightholders would be the software programmer, the person applying the software or the person in whose interest the data analysis is done (in many instances the manufacturer of the device as the *de facto* holder of the original data).

[639] It is to be noted that collective rights management would also be the only way to mitigate the exclusionary effects of a data producer's right as a *right in rem* concerning derivative data. The legislature could even decide to provide for mandatory collective rights management in the sense that only collective rights management organisations are empowered to claim exclusive data producer's rights.

[640] Fezer (n 4) 366-67; *id* (n 26) 5; Wandtke (n 205) 12.

to be extended to derivative data.[641] In addition, such a CMO would have to represent all citizens of a given jurisdiction—not to mention the challenges of cross-border management, which is of essence in a digital economy that increasingly relies on cloud-computing without borders. To identify all the data that all citizens produce would require the CMO to constantly monitor the private and professional life of all members of society. It is quite clear that such a task would go beyond what any membership-driven private organisation in the style of copyright collective rights management organisations can possibly accomplish. A public authority doing the same[642] would however create a mega digital intelligence agency constantly spying on the life of all citizens with the justification of taking care of the citizens' ownership rights. Hence, from a constitutional perspective, the very idea of such a system must be rejected. This idea meanders between an illusion, since the implementation of this proposal appears unrealistic, and a true nightmare for any democratic society.

This may be a reason why Fezer, the strongest supporter of data ownership rights of all citizens in the Germany so far, has recently become more cautious regarding individual property rights of the citizens in machine-generated data. He now advocates 'representative data ownership' (*repräsentatives Dateneigentum*) as explained in his study for the Konrad Adenauer Foundation.[643] There, he still maintains the concept of individual ownership of data of the citizens—yet adding another layer of representative ownership—for creating a legal basis for participation of all citizens in the economic value generated through the use of 'their' data.[644] But now he argues that individual participation in the income of the commercialisation of data has to be replaced by remuneration of the collective of all rightholders where individual remuneration is not possible or would run counter to the principle of proportionality.[645] For implementing and enforcing both individual and collective participation, he mentions alternative systems, including collective rights management.[646] He finally recommends managing such participation, in both the individual and collective form, through the creation of a separate collective data rights estate (*Datensondervermögen*) that would be utilised in the interest of the citizens as the rightholders.[647]

The most interesting question is whether the individual rightholders would still participate in the income. Fezer answers this question in the negative, which is surprising since he has offered the creation of the collective data rights estate as a means to also implement a system of individual economic participation. The data rights estate, however, is only meant to be employed, as it seems, in the collective interest of the citizens as data owners, namely, to support their interest in the digitisation of the environment in which they live and to finance certified institutions active in the field of digital education and training, data security and development of the digital infrastructure.[648] This shows that the focus of Fezer's writing on data ownership of the citizens has shifted from subjective rights to regulation of digital business models through a new 'data agency' (*Datenagentur*), which, in turn, is under democratic control of the rightholders[649], and a new system of financing of measures and programs in the public interest. Yet the question is why such additional regulation based on ownership rights in data is needed, and what it can contribute, in addition to the legal frameworks created by competition law and data protection rules. As regards the interest

[641] As Fezer (n 31) 65 nevertheless recommends.

[642] A public authority is also considered as an alternative by Fezer (n 4) 367.

[643] Fezer (n 31) 78-79.

[644] Ibid, 64-65.

[645] Ibid, 66.

[646] Ibid.

[647] Ibid, 84-85.

[648] Ibid, 85.

[649] Ibid, 72-73.

in generating income for society that can be spent as described by Fezer, the question is whether a tax law reform that makes sure that especially multinational firms active in the data economy do not evade paying national taxes would be the more appropriate and less complicated means of generating funds that could be spent for said purposes.[650] Yet Fezer's preference for 'representative data ownership' confirms the general conclusion of the analysis of this sub-section of the Study that economic participation of the individual citizen in the additional wealth generated by the use of machine-generated data cannot be implemented by a classical intellectual property rights system.[651] Rather, any attempt to do so would create enormous transaction costs, grounds for litigation and impediments to free flow of data rather than unlocking data where the *de facto* holders are unwilling to grant access.

f) Exceptions and limitations

As mentioned before, in the framework of intellectual property systems, the interest in access is typically taken care of by the exceptions and limitations.[652] As nowadays discussed for a potential reform of the Database Directive[653], access could especially be promoted by the adoption of a compulsory licensing system. Hence, the idea would be to, first, recognise a data-producers right in substance and, then, promote access to the data based on exceptions and limitations, including a compulsory licensing system. Recognition of the data producer's right would thereby work as a means to make an intellectual property-type access regime applicable in a situation where data access would otherwise be excluded by *de facto* control of data.

The need to provide for exceptions and limitations is mentioned both in the European Data Economy Communication[654] and the accompanying Staff Working Document[655]. The question of whose interests in access need to be taken into account in formulating exceptions and limitations depends to a large extent on who is identified as the rightholder. Since the Commission is clear in the text of the Communication in this latter regard, considering a potential data producer's right of the owner or long-term user of a connected device, the Commission can also conclude that the manufacturer should get non-exclusive access to the data under the exceptions provided for in legislation on the data producer's right.[656] According to the Commission, the same should apply where public authorities are in need of access, for instance, for traffic management or environmental reasons.[657]

Although the Commission SWD is more open-ended as regards the question of who should be the rightholder, it places the consideration to implement obligations to share data at the centre of its

[650] More in favour of a tax law solution than intellectual property rights in data that extend to the control of secondary markets, Denga (n 94) 1375.

[651] Fezer still argues in the sense of a sui generis intellectual property right. But he only seems in need for such a right to justify a representative system of regulating data-driven business models through a new data agency. Fezer (n 31) 57.

[652] For some exceptions and limitations that would need to be discussed see Zech (n 90) 325-27.

[653] See at 4.2. i) below.

[654] European Data Economy Communication (n 9) 13.

[655] European Data Economy SWD (n 9) 35-36.

[656] In addition, the European Data Economy SWD explains the legitimate interest of manufacturers by the need to further improve the device and legal obligations to monitor the functioning of the device especially based on product liability rules. European Data Economy SWD (n 9) 35.

[657] European Data Economy Communication (n 9) 13. The European Data Economy SWD adds other grounds for promoting access of public sector bodies to privately-held data, namely, to collect statistical information and for purposes of urban planning and civil protection. European Data Economy SWD (n 9) 36.

analysis on exceptions and adds two other scenarios in which exceptions will be needed.[658] The first one addresses the need of scientists to access to privately-held data for the purpose of conducting research entirely or predominantly funded by public resources.[659] The second one is of more interest in the context of this Study. Access may also be needed where there is a public interest in enabling private parties to get access to privately-held data, such as to enable smart homing.[660]

But the Commission does not make any further steps, nor does it seem to be aware of the possibility, to implement a system that would be more in line with traditional intellectual property legislation. The data producer's right could also be allocated to the device manufacturer and, at the same time, exceptions could take care of the private interest of the owner or long-term user of the device to get access to the data generated by the device.

Yet this latter approach has its own shortcomings and, ultimately, is based on a wrong assumption. The shortcomings relate to the fact that recognition of a property right especially for the device manufacturer would strengthen the already existing *de facto* control by adding an exclusive data ownership right *in rem*. Full exclusivity would be accepted as a side effect of the need to overcome *de facto* control within the limited scope of application of the exceptions and limitations. There is even the risk that the legislature would at the beginning overlook specific interests in access, thereby creating a negative impact on the market in form of restricting free flow of data until the legislature manages to add new exceptions.

In more generally terms, it is wrong to assume that access regimes can only be implemented in the framework of intellectual property rights systems. There is the alternative to adopt self-standing access rights to overcome *de facto* exclusivity.[661] Already today, such legislation is known from sector-specific regulation. The Commission itself is confirming this fact by hinting at some EU legal instruments that provide for independent data access regimes as sector-specific obligations to license,[662] such as regulation of access of independent repairers to on-board data of motor vehicles[663], the obligation of banks to provide account information to facilitate market access for digital payment services providers[664] and the so-called REACH regulation on the avoidance of repeated animal testing on chemical substances by an obligation to share existing test results with other companies[665].

The Commission argues that there is a need for further examination of whether adoption of such access regimes could be considered for a wider range of types of data, economic operators or

[658] European Data Economy SWD (n 9), 35.

[659] Ibid, 36.

[660] Ibid. The SWD also mentions the following examples: access to smart metering information relevant for balancing the grid or to enable smart living environments and care institutions.

[661] This seems to be shared by Mezzanotte (n 45) 183-86 with his proposal of a general access system to counterbalance the position of *de facto* data holder.

[662] Ibid, 37-38.

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

[664] Arts 35 and 36 Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L337/35.

[665] Arts 27 and 30 Regulation 1907/2006 of 18 December 2006 concerning the registration, evaluation, authorisation and restriction of chemicals (REACH), [2006] OJ L396/1. This Regulation has been amended several times. Consolidated text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02006R1907-20140410&from=EN (accessed 31 July 2018).

business sectors.[666] In this context, the Commission also refers to the compulsory licensing system that was originally proposed for the EU sui generis database right.[667] The latter shows that implementation of access regimes can become a necessity to balance otherwise excessive exclusivity caused within the realm of a new intellectual property right. But access regimes may also be needed for unlocking data where *de facto* control over data exists. As demonstrated by the abovementioned sector-specific data regimes, there is no need for the legislature to recognise an exclusive intellectual property right in data as a stepping stone for the adoption of an access regime for data.

g) Conclusion

To summarise, the assessment of the benefits and shortcomings of a potential data producer's right clearly argues against its adoption. Such new intellectual property system would fail to fulfil any of the three requirements for supporting its introduction.

First, there is no convincing economic justification for the introduction of a data producer's right based on a market-failure analysis. In particular, neither the owners or long-term users nor the manufacturers have to rely on exclusive control over the use of the data generated by the device in order to make their investment. Manufacturers are sufficiently protected by *de facto* control over the data, the availability of technical protection measures and potential protection under trade secrets rules.

Secondly, a data producer's right cannot be implemented in a way that fulfils the quality standards of intellectual property concerning attribution of the right, participation in the economic returns and dissemination of the subject-matter of protection. It is extremely difficult to clearly identify what kind of raw data is protected and who the rightholder is, especially if protection were to be limited to non-personal data. This problem of attribution would become even more serious where a data producer's right would extend to any 'derivative' data encoding new information generated through analysis of protected machine-generated data. As regards the requirement of participation, it is not possible to create a data ownership system that guarantees the rightholder at the beginning of the value chain to participate in the added value generated at subsequent stages of the exploitation of the data. Especially extension of the rights of the data producer to derivative data would increase transaction costs, give rise to legal uncertainty and, thereby, create impediments to free flow of data. Even if the legislature only decided to implement statutory remuneration rights, it is not possible to imagine a workable system of collective rights management that would appropriately remunerate data producers for secondary use of their data. Finally, to respond to the requirement of dissemination, a system of data producer's rights would have to rely on free transferability and licensing of the use of data. This, however, collides with the other objective of using the owner or long-term user of a device to unlock data by licensing to third parties.

Third, the strongest argument against a data producer's right would be its negative effect on free flow of information and even freedom of information. The data producer's right would circumvent the limitations which are part of other intellectual property regimes, such as copyright law, patent law and the sui generis database right and lead to the recognition of a non-meritorious right of exclusive use of data. In the light of the lack of an economic justification for such a right and the costs in terms of restricting freedom of information, the trade-off is negative. As argued before, the

[666] European Data Economy SWD (n 9) 38.

[667] Ibid.

European legislature should better reform the sui generis database right in a way to make sure that it will not collide with access rules in other parts of the law.[668]

Yet this does not mean that the Commission is wrong in arguing for the need of enabling the owner or long-term users of connected devices to claim access to the data generated by these devices either for themselves or third persons. For attaining this goal, however, a data producer's right does not appear as the appropriate means. Rather, the Commission would be better advised to address the need of access through access rights.

Data protection rules support this analysis. An assignable data producer's right would collide with the far-reaching right of the data subject to withdraw consent at any time as regards personal data, while a data producer's right as a new intellectual property system would have to allow for stable and reliable transactions.

5.2 The GDPR as a basis for rights to access machine-generated data

According to the preceding analysis, access rights should be preferred to the introduction of a data producer's right. The question to be considered in this in the following analysis is whether access rights under the General Data Protection Regulation[669] can also be applied to machine-generated data and what the benefits of such rights are from a consumer perspective.[670]

a) Personal data as machine-generated data

It has already been explained further above[671] that the data protection rules of the GDPR protect data on the semantic level, namely, as information on an identified or identifiable person. For data protection, it is not relevant in what form and in what kind of raw data this information is encoded. Hence, if personal data as protected by the GDPR is collected by a connected device, the data protection rights do not vest any rights of the data subject in the raw data on the syntactic level.

Yet also from the perspective of access, the link between control of the machine-generated data and the personal information that is encoded in that data is important. Whenever connected devices collect personal data, exercise of the right to erasure after withdrawal of consent according to Article 17(1)(b) GDPR will require the data processor to delete the underlying machine-generated raw data.[672]

b) The right of access to data under Article 15 GDPR and access to machine-generated data

Yet erasure of data has to be distinguished from data access. A data access right is enacted in Article 15 GDPR. The right provides for access to personal data and additional information.[673]

---

[668] See at 4.2 k) above.

[669] GDPR (n 22).

[670] Answering Question 5 listed in the introductory Part 1 above.

[671] See at 4.1 a) above.

[672] At 4.1 b) above, it is also argued that this mechanism would even apply if the legislature recognised a data producer's right in favour of the manufacturer as the data processor.

[673] Art 15(1) GDPR.

As in the case of the right to erasure, the right to data access refers to the semantic level of information. Article 15(1) GDPR explicitly defines this right as a right to receive 'the personal data concerning him or her'. However, whereas exercise of the right to erasure will affect the raw data in which the personal information was encoded, the data processor does not have to provide access to the raw data in which the connected device originally encoded the personal information in the sense of Article 15 GDPR. Rather, pursuant to Article 15(3) GDPR, the controller only has to provide a 'copy' of the personal data undergoing processing. Still pursuant to Article 15(3) GDPR, this copy has to be provided in a 'commonly used electronic form' where the data subject makes the request by electronic means, unless requested otherwise by the data subject. In the recitals, it is even stated that, '[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data'.[674]

A particular advantage of this right for consumers arises from the broad application of the right as regards the kind of data. The right applies to any personal data that the controller is processing, irrespective of how, legally or illegally, the controller has obtained the data. The right even extends to data, that the data processer may have inferred or derived from the data subject based on data analyses. In the case of data not directly obtained from the data subject, the data processor has to inform the data subject on the source of the data.[675]

Yet the right does not include the right to claim provision of the data in an interoperable format. Quite the contrary, the right to receive a 'copy', as well as the fact that the data subject may be charged for the administrative costs for providing any additional copy[676], underline that the purpose of the right is limited to protect the autonomy of the data subject by informing the data subject about the personal data that is processed and, thereby, to enable the data subject to exercise other data protection rights such as the right to erasure according to Article 17 GDPR. This also explains why the right to data access does not include a right to provide data access directly for third persons. The data access right of Article 15, unlike the right to data portability under Article 20 GDPR, which will be discussed in the following, does not aim to enable the data subject to switch suppliers and, thereby, to enhance competition in the market.

c) The data portability right under Article 20 GDPR and access to machine-generated data

Article 20 GDPR can be considered a special form of data access right.[677] Just as in the case of the other data protection rights, the right to data portability refers to the semantic level of information. Article 20(1) GDPR explicitly defines this right as a right to receive 'the personal data concerning him or her' with the important limitation to data that the data subject has 'provided' to a controller. Similar to the right to access data under Article 15 GDPR, Article 20 GDPR does not require the data processor to provide access to the raw data in which the connected device originally encoded the personal information. Nor does exercise of the data portability right automatically trigger erasure of the data from the data controller's system.[678]

Article 20(1) GDPR specifies the 'format' in which access has to be provided. The requirement that the data format be 'structured, commonly used and machine-readable' will oftentimes require a

[674] Recital 63, 4th sentence, GDPR.

[675] Art 15(1)(g) GDPR.

[676] Art 15(3), 2nd sentence, GDPR.

[677] See at 4.2 b) above. In contrast, Weber (n 87) 154 distinguishes data portability rights from data access rights and compulsory licensing. According to him, the data portability right is a right to get data transmitted.

[678] Article 29 Data Protection Working Party, Guidelines on the Right to data portability (n 156) 7.

reformatting of the data. This shows that the data portability right of Article 20(1) GDPR cannot be perceived as a right to access original machine-generated data as raw data.

From a consumer perspective, this approach needs to be welcomed. Article 20 GDPR takes the appropriate approach by focusing on the semantic level of information. In the case of a consumer who has acquired or otherwise used a connected device and from whom the device has collected personal data, the specific interest protected by the GDPR only relates to the semantic level of the machine-generated data.

In contrast, a rule that obligates the manufacturer to generally grant access to the machine-generated data collected by a connected device would not sufficiently protect the interest of the data subject, and, at the same time, would disrespect the legitimate interest of the manufacturer as the data processor in retaining non-personal data. From the perspective of the consumer, such general right of access to the raw data generated by a connected device would not go far enough, since the data subject would still have to analyse the machine-generated raw data to discover the personal information. From the perspective of the manufacturer, this obligation could go too far, since it would require granting access to raw data that does not include any or not only personal data.

From a consumer perspective, this rule has advantages and shortcomings. Technically, by not just granting a right to access the original encoding but requiring access in a format that is commonly used and machine-readable, Article 20 GDPR aims to promote data interoperability and, thereby, enhances free flow of data. The data portability right also goes beyond the data access right of Article 15 GDPR by including a right to have the data directly transmitted to another data processor, where this is technically feasible.[679] This identifies the data portability right as a right that is designed to help consumers switch suppliers.

Yet, as compared to the data access right of Article 15 GDPR, the right to data portability under Article 20(1) GDPR is more limited in scope as regards the data to which it applies. The data portability right can only be claimed to get access to data the data subject has 'provided' to the data controller.[680] This requirement should be read in the sense of also including 'observed' data, including data collected from the data subject as part of the provision of a service, such as search data, or based on the use of a device, such as a location data collected through a smartphone or a connected vehicle or data on the bodily functions of a person collected by connected wearables.[681] But unlike Article 15 GDPR, the data portability does not apply to 'inferred' or 'derived' data that the data controller generated by analysing the data provided by the data subject. For instance, based on Article 20(1) GDPR, a data subject can claim transfer of her location record, but she cannot claim data portability regarding the information on the personal profiling, which the supplier of a connected device may have established through data analyses.[682]

In other regards, the argument was made that the data portability right should be read strictly, namely, in the light of the proportionality principle, to only apply to data where the data subject can legitimately expect that data will be available over time.[683]

In addition, according to its lit. a), Article 20(1) GDPR only applies where the data is being processed automatically and based on the consent of the data subject or for the performance of the contract. It is not meant to apply where the data processing is based on a legal ground other than consent or

[679] Art 20(2) GDPR.

[680] See Article 29 Data Protection Working Party, Guidelines on the Right to data portability (n 156) 9-10, and the analysis at 4.5 b) above.

[681] Ibid. In the same sense, Janal (n 156) paras 7-9.

[682] Article 29 Data Protection Working Party, Guidelines on the Right to data portability (n 156) 10.

[683] Janal (n 156) para 10.

contract.[684] Quite strangely, the provision would exclude data portability where the data controller is acting unlawfully.[685] Such literal reading would run counter to the underlying policy of the provision to only relieve the data processor from the obligation to provide data portability where there is another legal ground for the processing. Consumers should not lose the right to claim data portability only based on the argument that they have not given their consent to the data processing.

It also has to be noted that data portability will depend on the availability of interoperable formats. The data controller is required to make personal data accessible in a 'structured, commonly used and machine-readable format'. But if such format does not exist, the data subject will not be entitled to claim access. In addition, if the data subject seeks access of third parties to the data, Article 20(2) GDPR only stipulates a right against the data processor to enable the transfer, but not a right against the new processor to accept the data especially in the particular format.

d) Data portability according to Article 20 GDPR as a template for future regulation

What learnings can be taken from this analysis for future legislation on additional access regimes? The analysis of Article 20 GDPR argues for an interest-oriented approach. But does this mean that data access regimes should always focus on the semantic level of data? In fact, in those cases in which the legislature has already provided for access regimes, this seems to be the case. The examples mentioned by the Commission in the European Data Economy Staff Working Document are of that kind, whether it is about on-board data of motor vehicles to which independent car repairers need to have access or banking account data on which providers of digital payment service depend or data on animal testing.[686]

But this does not mean that access rights in the digital economy must never be designed to allow for general access to whole datasets containing machine-generated raw data. This question should as well be answered against the backdrop of the interests concerned. In the copyright field, the Commission has proposed a broad provision that would allow for text and data mining by research organisations for scientific purposes.[687] This provision is not conceived as a data access rule but an exception in terms of copyright protection which requires as one of its conditions that the research organisation making use of the exception needs to have lawful access. Still, this provision—as a rule on 'copyright access'—shows that depending on the concrete interest, access can also be defined as access for purposes of data mining. Such broader access rules providing for access to the raw data generated by connected devices may become particularly important for the owners or users of connected products where they want to connect the devices of one manufacturer with other devices under their control, for instance, to enable smart homing, or where they ask for access to data generated by a connected device to receive a digital service from another service provider. Both purposes may go hand in hand where the independent service provider offers services that depend on connecting the different devices under the control of the consumer, such as typically in the case of smart homing.

In any instance, the data portability right of Article 20 GDPR is not sufficient to fulfil such needs. In the abovementioned cases, consumers of connected devices will also be in need of access to non-personal data, and oftentimes the requirement that the data be 'provided' by the data subject,

[684] See Art 20(1)(a) GDPR; Recital 68, 3rd and 4th sentence, GDPR.

[685] This is criticised by Janal (n 156).

[686] European Data Economy SWD (n 9) 37-38.

[687] Art 3 of the Proposal of the Commission of 14 September 2016 for a Directive of the European Parliament and the Council on copyright in the Digital Single Market, COM(2016) 593 final.

excluding any other information generated through a data analysis process, may additionally limit the scope of data access too much. Yet the data portability right of Article 20 GDPR can work as a role model for future legislation for data access rights, without, as argued here, being able to replace a proper analysis of the interests involved as a basis of the conditions and the scope of protection.

5.3 Targeted rights especially of consumers to access machine-generated data

The preceding analysis argues against the introduction of new property rights in data and supports the idea of access rights.[688] In the following, the Study will explore under which conditions such access rights should be accepted and how they could be designed.[689] Thereby, the Study puts an emphasis on the potential introduction of an access right for consumers with respect to data collected and processed by connected devices. In doing so, it will also answer Questions 6 through 8 listed in the introductory Part 1. In the light of this analysis, no answer needs to be given to the last Question 9.

a) The comparative advantages of data access rights

Before getting into the details of the legal design of such potential access rights, it is important to summarise the comparative benefits of an access right of the owners and users of connected devices as compared to data ownership rights.[690]

First, specifically responding to the underlying market failure of a data lock-in[691], access rights would be more targeted than a data producer's right. As compared to a property right *in rem*, an access right will not create any obstacles for the commercialisation of the aggregate data held by the manufacturer of the device. This is in the particular public interest, because state entities will often seek access to aggregate data, including data originating from consumers, for instance, for purposes of traffic regulation (as regard data collected from smart vehicles), for assessing and controlling demand of energy and water or for purposes of infrastructure and city planning (as regards data collected from the homes of consumers). There is no reason why the legislature should go beyond an access right by adopting a property right that would create additional exclusionary effects on secondary markets without any additional benefits.[692]

Secondly, access rights can be better protected against the risk of being contracted away where consumers find themselves in an inferior bargaining position. Such rights can either be implemented as part of mandatory contract law or as non-waivable statutory rights similar to the data portability right of the GDPR.[693]

---

[688] Equally recommending paying legislative attention to the development of data access right rather than creating a data ownership right, Weber and Thouvenin (n 44) 73.

[689] On the problems relating to the design of the rights, see also Weber and Thouvenin (n 44) 60-61.

[690] Hereby, the analysis builds on the Position Statement of the Max Planck Institute of 2017 (n 9) paras 20-22 as well as the previous publication in Drexl (n 9) 236-37.

[691] See at 2.3 a) above.

[692] Position Statement of the Max Planck Institute of 2017 (n 9) para 20.

[693] In favour of the latter, Position Statement of the Max Planck Institute of 2017 (n 9) para 21; see also Drexl (n 9) 236.

Thirdly, access rights can be allocated more flexibly in the light of the access interests involved. Allocation will not be restricted by an anyhow difficult factual assessment of who has 'produced' the data.[694]

Fourthly, a data access right can be enacted in a positive way, namely, through formulating requirements for the grant of such right. From a perspective of legislative technique, this is a clear advantage. As explained further above[695], by proposing a data producer's right, the Commission is aware that such right may go too far and therefore confirms the need to provide for specific exceptions and limitations.[696] However, formulating such exceptions and limitations is not an easy task, since the legislature would have to anticipate all different cases in which a data producer's right as a right *in rem* would go too far. In contrast, a data access right can be designed in a way to avoid excess protection upfront.[697]

Finally, the recognition of an access right would be in line with competition law principles. It can be designed as a tool to address cases in which there is a high risk that the manufacturer has strong incentives to refuse to grant access to the data with the objective and/or effect of excluding competitors from the market. In such instances, competition law enforcement would be too burdensome given the need to show market dominance in every single case, while the problem will become a mass phenomenon.[698] Conversely, in cases where the manufacturer has no interest in foreclosing the market, a data access right will not create any harm since the manufacturer will anyhow be willing to grant data access, eventually even free of charge, under competitive pressure in the markets for connected devices.[699]

b) Access to what data?

As noted in Part 5.2 of the Study, consumers enjoy a data portability right under Article 20 GDPR in respect of their personal data that they have provided to a data processor. Interpreted broadly[700], data portability can also be claimed for getting access to personal data collected by connected devices.[701] Although data collected by connected devices used by consumers will typically consist in personal data, the data portability right of Article 20 GDPR does not go far enough to respond adequately to the risk of data lock-ins.

The data portability right of Article 20 GDPR is limited in two regards: first, by only applying to personal data, it does not provide access to non-personal data to which access may also be needed in certain instances. More importantly, it is to be stressed that the objectives of the access right discussed do not relate to the character of the relevant data as personal. The interest of the purchasers and users to connect the different devices they use for private purposes—including their smartphones, tablets and PCs, household devices, cars, etc—will be growing enormously. Consumers will increasingly depend on the need to connect their devices, or to enter into contracts

[694] On the interest-oriented allocation of the right see Position Statement of the Max Planck Institute of 2017 (n 9) para 21; see also Drexl (n 9) 236-37.

[695] See at 5.1 f) above.

[696] European Data Economy Communication (n 9) 13.

[697] Position Statement of the Max Planck Institute of 2017 (n 9) para 22; Drexl (n 9) 237.

[698] On the limitations of competition law see already at 2.3. b) above.

[699] Drexl (n 9) 238.

[700] See at 5.2 c) above.

[701] See also Position Statement of the Max Planck Institute of 2017 (n 9) para 25 (arguing that Article 20 GDPR can already provide data access, for instance, in cases where smart wearables collect data on the bodily functions of a person to use it for health care purposes by a doctor or a hospital).

with other firms that provide data-based services[702], to make best use of all of these devices and the data they produce. Hence, rather than by the personal character of the data, the interest of consumers to get access to such data is explained by the need to make full use of these devices; consumers should be allowed to choose freely among suppliers of devices and providers of data-based services in a competitive market. Accordingly, the access rights to be discussed here should not be limited to personal data.

Secondly, Article 20 GDPR only provides a legal basis for claiming portability of data that are directly 'observed' by connected devices, thereby excluding data that is only 'derived' or 'inferred', especially through data analyses. This limitation may be justified against the backdrop of specific data protection objectives of the GDPR. However, the data access right to be discussed here aims to protect the interest of making full use of connected devices. Oftentimes, and even more so in the future, connected devices will make use of embedded, increasingly AI-based software, that immediately processes the data to generate new data. Legislation that limits the access right to only 'observed' data will therefore not achieve the goal of providing consumers with all the benefits that their devices could produce.

In times of the Internet of Things and cloud-computing, data generated by connected devices does not necessarily need to be analysed and processed within the device. Conversely, additional data will often be transferred to the device to guarantee the well-functioning of the device. Accordingly, it appears rather difficult to clearly delimit the scope of data to which access should be granted. Hence, a particular challenge will relate to drawing a line between data that is covered by the access right and other data that is not.

One possibility for drawing this line would be to limit the access right to all the data that is stored in the device. This, however, would enable the manufacturer to circumvent the data access right by transferring the data processing elsewhere. The appropriate approach would anyhow have to be technology-neutral. Accordingly, it seems better to extend the data access rights to all data that are generated or used by the device for enabling the well-functioning of the device and access to which is needed for providing ancillary data-based services. From an economic point of view, the fact that the consumer pays a price for purchasing or using the device can be considered to justify a duty of the holder of the relevant data to share data in the interest of the consumer.

c) Data access rights as a non-waivable statutory rights

Another question regards the legal nature of the access right. Consumers typically use connected devices after concluding a sales or rental contract. Hence, access rights—following the approach of the proposed Digital Content Directive[703]—could in principle be adopted as mandatory consumer contract law.

Yet, in the case of connected devices, the contractual relationships may take various forms and complex structures. Vehicles and household devices are typically sold by retailers. In such cases, use of these devices may require consumers to sign additional contract with other parties, especially the manufacturer, who will provide digital services linked to the use of the device. At least in respect of such ancillary services, there would be a direct contractual link between the consumer and the manufacturer.

[702] Such services can either be related to the management of multiple devices, such as in the case of smart homing, or relate to the operation of a specific device, such as a company controlling the functioning of a smoke detector or a food supplier that supplies certain foodstuff to refill the refrigerator.

[703] See at 4.5 i) above.

But this is not always the case. Outside the realm of consumer law, a most obvious example relates to smart farming. Smaller farmers often outsource farming activities to independent service providers who work the land with their farming machines. Such machines are nowadays able to collect large amounts of data concerning the soil. Yet, to get access to such data, the farmer will not be able to rely on a contract concluded with the manufacturer as the *de facto* data holder, if the machine is operated and owned by an independent service provider.[704]

Similar cases cannot be excluded as regards devices used by consumers. Providers of energy, power or water often install smart meters in the home of consumers and retain the property in the meters. Motor vehicles and bicycles get increasingly leased through rental companies or shared among consumers (car and bike sharing business models). Most importantly, in the field of smart homing, problems can arise where private homes are used under a rental contract. Tenants often bring their own household devices and will also want to connect these devices with those that were installed by the landlord. European contract law by itself would not be able to guarantee access to the data controlled by the manufacturers of the devices. It would have to interact with national tenancy law, which is not harmonised by the European level.

Accordingly, recognition of direct non-waivable statutory data access rights of the person having a legitimate interest in access against the manufacturer of the device therefore appears as a more straightforward approach to guaranteeing access. The interest-bound concept of data access rights has to exclude the framing of data access right as tradable rights.[705]

d) The scope of access rights and between whom the rights should be granted

Access rights should be vested in the persons who have a legitimate interest in getting access to the data generated by connected devices. The legitimacy test includes the requirement that the person requesting access is dependent on access to the data. Hence, the relevant data must be single-source data in line with the *Magill* competition case-law of the CJEU.[706] The 'legitimate interest' test thereby decides whether the right as such exists, who is entitled to claim the right and, finally, who is under the duty to grant access.

The legitimate interest has to relate to the data as defined above (at b)), namely, as the data that are generated or used by the device for enabling the well-functioning of the device or to which access is needed for providing ancillary data-based services. Accordingly, any person who is dependent on access to these data for making full use of the device for said purposes should be considered the holder of such an access right. This definition of the interest would more concretely circumscribe the set of cases where a person has an interest in 'un-locking' data.

Still, defining the relevant group of persons having such legitimate interest is not an easy task. An option could consist in defining this group of persons more concretely, as obviously the Commission is trying to do, by relying on the concept of the owner or long-term user of a device. In fact, short term use will typically not suffice to justify a sufficient interest in access. Yet, as the example of the farmer who outsources farming activities to independent service providers shows, exceptions to this rule can and should not be excluded. In addition, in the case of smart homing, it is not only the tenant who may seek data access. Landlords can as much depend on access to the data of the devices brought by the tenants, for instance, to control energy consumption in a larger

[704] See also Position Statement of the Max Planck Institute of 2017 (n 9) para 14; Drexl (n 9) 234.

[705] This seems to be overlooked by Zech (n 90) 319-322 (discussing data access rights as non-exclusive, freely assignable rights).

[706] See at 2.3 b) above.

apartment building. But landlords can hardly be considered users of devices that are owned and used by tenants in an apartment.

This argues in favour of sticking with the less precise but flexible interest-based definition of the persons entitled to data access as formulated above. Yet the owner or long-term user of the device could still be named as a person that is typically entitled to data access under this rule. The legislature could even introduce a rebuttable presumption that the owner or long-term user will be entitled to such data access.

As a non-waivable right, the data access right cannot be transferred to persons or entities that do not have such an interest. Nor is the holder of the data access right allowed to commercialise the data as received from the manufacturer for secondary purposes.

The person who is under the statutory duty to grant access to the data will be typically the manufacturer of the device. Yet it cannot be excluded that, under particular circumstances, the right should be granted against a different person or entity. Where machine-generated data is directly communicated and processed in a data-sharing network and where a joint venture, for instance, of different motor vehicle manufacturers, is managing the data sharing and, in particular, provides the relevant data-related service (such as services related to the operation of the car), it may make sense to grant the right directly against such person or entity. Another relevant case can be illustrated against the backdrop of the data portability right of the GDPR. Where a car is registering the driving habits of the driver on behalf of the insurer and directly communicates the data to the insurance company, it can be argued that the data portability right of Article 20(1) GDPR also has to be directed against the insurer as the data processor. This example shows that the definition of the person under the statutory duty to grant access should be defined in a more general way. Following the approach of the GDPR, which uses the broad concept of a 'data controller', it is proposed here to use the term 'data holder'. This is explained by the fact that, for the purpose of the data access right, the person addressed by the data access right has to be defined differently than the data controller for purposes of data protection, namely, as the person being in *de facto* or legal control of the relevant data.

e) Limitation to consumers?

Another question regards the need to limit application of data access right to consumers. In fact, the market failure addressed by the data access right is not specific for B2C relations. It does not make any difference whether somebody rents rooms in a building as a private flat or as office space. Businesses may even more depend on access to data collected and processed by connected devices and machines for purposes of smart manufacturing or smart farming. Therefore, the European legislature should consider much broader legislation beyond the boundaries of consumer law.

f) Third-party beneficiaries

As in the case of the data portability right of Article 20(2) GDPR, the access right should also include the right to have the data transmitted to third parties. This would enable the holder of the access right to receive digital services from third parties and thereby open up markets for the supply of data-based services to competition. Suppliers of connected devices would otherwise manage to retain the market of attached data services to them where access to the data is indispensable to provide such service.

Yet it has to be mentioned that, in many instances, granting a right to have data transferred to third parties will only be the second-best solution. This is shown by already existing sector-specific regulation. In the two cases of access to on-board repair data of motor vehicles for maintaining

openness of the market for independent car repairers[707] and regulation of access to account information of banks for enabling digital payment services[708], which are also mentioned by the Commission[709], the EU legislature has recognised direct data access rights for third-party service providers. In both cases, the recipient of the service can freely choose among services providers without having to claim and enforce access against the data holder. This is not only the most convenient solution especially for consumer; it is also the most efficient way of guaranteeing access. In the sectors concerned, to respond to the mass phenomenon of such access and to solve the problem of data interoperability, access will in practice only be implemented effectively by tools and interfaces developed and standardised by the business associations.

Against the backdrop of these two cases, the question is whether direct access rights of such service providers should be generalised as regards services linked to connected devices and even be implemented in a generally applicable data access regime. In fact, the interest-based test for identifying the person having a legitimate interest in getting access to the data seems flexible enough to also include third-party service providers. However, for this case, legislation should also require that the recipient of the service, who is entitled to claim access, has mandated the third-party to provide such service. This legislation could be complemented by a generally applicable mechanism of collective bargaining between business associations under the oversight of a competent regulatory agency as a basis for negotiating sector-specific access regimes whereby also the issue of data interoperability could be addressed.

g) General or sector-specific regulation?

Maybe the most difficult question is whether such access rights should be implemented through generally applicable law or only sector-specific regulation.

The Max Planck Institute for Innovation and Competition[710] has expressed a preference for sector-specific legislation on data access rights.[711] The reasons for this were twofold: first, examples for sector-specific regulation, such as access to the information needed to provide repair services for motor vehicles, show that such sector-specific regulation can be much more specific and targeted to provide the access regime with legal certainty and effectiveness.[712] Secondly, different sectors may need different rules especially as regards the question of whether and how access to data should be remunerated. A duty to pay for access to information needed for repairing a car seems perfectly justified.[713] In contrast, where access to personal data is sought in the field of health care, the balance of interest may well argue against remuneration.[714]

A third argument in favour of sector-specific application should be added: data access will always depend on the technical interoperability of data. Sector-specific regulation could better react to the challenge of standardisation of data formats and access to them to implement more advanced data access regimes.

---

[707] See at n 153 above.

[708] See at n 154 above.

[709] European Data Economy SWD (n 9) 38.

[710] Under the co-authorship of the author of this Study.

[711] Position Statement of the Max Planck Institute of 2017 (n 9) paras 23-25. This view seems to be shared by Weber (n 87) 154.

[712] Ibid, para 23.

[713] As provided for by Art 7 Regulation 715/2007 (n 153).

[714] See Position Statement of the Max Planck Institute of 2017 (n 9) para 24; Weber (n 87) 155.

Most importantly, however, sector-specific regulation would help address regulation based on a more holistic view of the interests of all the relevant stakeholders in the given sector. As Kerber and Frank have argued, sector-specific regulation has the potential of overcoming the rather two-dimensional and often simplifying debate on ownership versus access to implement sector-specific regulation from the perspective of data governance.[715] This data governance approach to regulation relies on a market failure analysis. Thereby, it is assumed that firms will in principle be able to provide for appropriate data governance structures through contract law, taking care of all interests involved. Yet especially in complex multi-stakeholder situations, specific market failures could prevent the emergence of such efficient data governance regimes.[716] To identify and address these market failures appropriately, the approach to regulation necessarily has to be sector-specific[717], taking account of the specific interests of stakeholders of the given sector and the already existing regulatory framework.

Beyond the case of connected cars, as analysed by Kerber and Frank, complex stakeholder structures can also be identified in sectors with considerable relevance for consumers. The best example is probably smart homing. In this case, device producers, many different kinds of suppliers, such as suppliers of energy, water, communications services and food, owners of the buildings and apartments as well their tenants and, last but not least, the state and the cities will rely on a large variety of economic, privacy-related and public interests that need to be coordinated to make modern data-related markets work with respect to smart-homing.

Following the data governance approach, the claim to introduce and the decision to design sector-specific access rights could well mark the closing point of the analysis of this Study. But adoption of legislation on sector-specific data governance regimes does not and should not exclude discussion on the adoption of a generally applicable data access regime.[718]

General legislation on data access and adoption of sector-specific governance regimes do not appear as mutually exclusive legislative approaches. Both approaches should be based on an assessment of all interests involved. Still, application of the generally applicable access regime should only play a subsidiary role. While the general regime applies to all sectors, it should take account of the already existing, often sector-specific regulation. Where existing regulation sufficiently takes care of the legitimate access interests, courts should refrain from recognising additional or broader access rights as part of the generally applicable regime. In the case of complex stakeholder situations, the rules proposed here for a generally applicable regime have been designed on purpose in a way to grant flexibility to courts to apply the access regime with due regard to specific circumstances of the case at hand. This also means that in applying the rules of the general access regime, the task to cater for workable data governance systems will be attributed to the courts. Accordingly, courts will find themselves very much in the same situation as the sector-specific regulator. They will therefore have to make their decisions against the backdrop of the interests of the stakeholders of the given sector and in awareness of the existing, oftentimes sector-specific, legislation.

It could even be argued that a general data access regime is needed to make the data governance approach work. The implementation of individual sector-specific data governance regimes will have to take the form of an evolutionary process. The data economy is not static. Rather, it disrupts many

[715] This has been exemplified by the two authors for the example of connected cars. See Kerber and Frank (n 35).

[716] Ibid, 8-9. It can also be argued that the typical presence of multi-stakeholder situations makes it particularly troublesome to device a generally applicable data ownership regime that allocate the property right uniformly across all sectors. The difficulty to allocate the data ownership right in multi-stakeholder situations is also confirmed in the literature on data ownership. See Becker (n 25) 255.

[717] Kerber and Frank exemplify their approach with an analysis of the sector of connected cars. Kerber and Frank, ibid. See also Wiebe (n 102) 878 (identifying six kinds of stakeholders having an interest in the data collected by cars).

[718] See also the proposal of Mezzanotte (n 45) 183-86 for a 'flexible, purpose-oriented general access system'.

sectors and its future development will require frequent adjustments of the regulatory system. Generally applicable legal instruments, equipped with the necessary flexibility, are therefore needed as the backbone of sector-specific regulation to achieve appropriate results while the data economy develops. The generally applicable access regime can also be used to gather new insights on the need for adjustments of the sector-specific data governance systems.

In particular, a general data access regime would have to address the issue of remuneration by implementing a flexible FRAND regime that would allow the data holder to charge a fair, reasonable and non-discriminatory fee for making available data if and to the extent this is justified in the light of the conflicting interests.[719]

h) Coordination with other systems of protection

Any access regime has to be coordinated with conflicting rights of others. In this regard, Article 20(4) GDPR, according to which the rights and freedoms of others must not be affected by the data portability right, does not provide a sufficient template for designing a workable framework for the data access right discussed here.

Yet Article 20(4) GDPR constitutes the applicable law for the portability of personal data. This does not exclude that a data access right protecting a different interest is more restrictive on the rights of others. Yet such data access rights should fully respect the data protection rights of other persons that could be affected. This means that the data access that would involve access to personal data of others will often depend on the consent by the other person according to Article 6(1)(a) GDPR.

The problem of conflicting sui generis database rights should be addressed by an exception in the Database Directive that gives precedence to the access rights.[720]

The more difficult question relates to the protection of trade secrets of the manufacturer. As argued above, trade secrets protection appears as a legitimate and adequate protection of the manufacturer also with respect to information contained in data generated by connected devices.[721] In particular, information to which independent repair service providers need to have access may easily fulfil the requirements of a trade secret of the manufacturer. Yet the recognition of a data access right for independent repairers of motor vehicles shows that EU legislation already gives precedence to data access rights over trade secrets protection. Yet the legislature should protect the secrecy interest against access of persons without any legitimate interest in data access. To implement this idea, legislation on the access right could require the holder of the access right to safeguard the secrecy of data provided by the manufacturer of the device. In the abovementioned example of repair information, this would prevent the repairer to provide information on the working of the connecting device to competitors of the manufacturer in the device market.

i) Coordination with end-user licence agreements and rules of vertical restrictions

As mentioned above[722], manufacturers will oftentimes not directly sell or rent connected devices to final consumers. This raises the question of how the access right would interact with restrictions that manufacturers may implement in their distribution agreements.

[719] FRAND principles are also discussed by the Commission in this context. See European Data Economy SWD (n 9) 39.

[720] In more detail, see at 4.2 i) above.

[721] See at 4.3 above.

[722] See at 5.3 c) above.

Although consumers will frequently buy connected devices through intermediaries (retailers), manufacturers may still try to impose restrictions on consumers on whether and how they get access to data and how they make use of those data based on an end-user licence agreement.[723] Of course, such an end-user licence agreement cannot exclude the data access right as a non-waivable statutory right. Conversely, however, the end-user licence agreement would also be needed to regulate the rights and duties of the parties, including the obligation of the purchaser to pay FRAND-compliant remuneration or keep information contained in data confidential.[724] Conclusion of such licence agreement is indeed needed if the EU legislature adopted a general access right to machine-generated data with the objective of guaranteeing best use of the device to clarify the rights and duties of the parties in the specific case. Yet the non-waivable access right should include the right to claim conclusion of such an end-user licence agreement which is compliant with the general principles set out by legislation. This also provides courts with the power to control the FRAND obligation.

Manufacturers may also try to include restrictions on data access through vertical agreements they conclude with retailers in the distribution chain.[725] Distribution agreements may be illegal and void to the extent that they restrict competition pursuant to Article 101 TFEU and the Vertical Agreements Block Exemption Regulation.[726] As pointed out further above, pursuant to Article 102 TFEU and the *Magill* case-law, manufacturers may be addressees of competition law where they directly refuse access to information as an indispensable input for other firms to enter and remain in the market.[727] Similarly, vertical distribution agreements that require distributors in downstream markets to foreclose access to such information may violate Article 101 TFEU. Yet the benefit of the data access right is that it relieves the person seeking access from the need to show that the requirements of a competition law violation are in fact fulfilled. Where the manufacturer imposes a restriction on a distributor that would undermine the access right of the end-user, the manufacturer should be considered being in violation of the access right.

In sum, access rights as non-waivable statutory rights should prevail over any conflicting obligation arising from a distribution agreement and end-user licence agreement. Yet the legislature should still consider implementation of two rules. According to the first rule, the legislature could clarify that the terms of granting access to the data can be regulated by an end-user licence agreement in full respect of the statutory framework of the access right. The second rule should declare void any contract term included in a distribution agreement that would oblige the distributor in the downstream market to restrict in any way the data access right. The latter rule would especially be needed to also enable the distributor to rely on the non-effectiveness of such clauses.

j) Enforcement

A last issue relates to the appropriate enforcement system. In principle, the data access rights is proposed as an individual rights of the person with a legitimate interest in data access. Hence, if data access is refused in violation of the statutory right, the holder of the access right will have to go to the competent court and sue the data holder. In case of dispute, the competent court will have to decide whether and under which conditions data access has to be granted.

[723] See Question 7 listed in Part 1 above.

[724] On the qualification of data access rights as compulsory licence regimes, see Weber (n 87) 145, and at 2.3 d) above.

[725] See question 8 listed in Part 1 above.

[726] Commission Regulation (EU) No 330/2010 of 20 April 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices, [2010] OJ L102/1.

[727] See at 2.3 b) above.

Yet use of the justice system to enforce the right may be particularly burdensome for consumers. In particular, private enforcement through the individual rightholder would be insufficient where individual manufacturers consistently refuse to grant access at appropriate terms to all holders of the access right. Hence, there is a case to think about additional forms of enforcement, namely, administrative enforcement and collective private enforcement.[728] If the EU legislature introduced a general data access regime based on a directive, the concrete form of enforcement could also be left to a large extent to the national legislature.

In this regard, it has to be noted that, as part of its New Deal for Consumers package, the Commission has just proposed a review of the Consumer Injunction Directive[729], which already includes some legal innovations concerning the topic of this Study.[730] In particular, the Commission proposes to extend representative actions to the competent courts and complaints to competent administrative bodies with regard to horizontal and sector-specific EU legal instruments that are specifically relevant for the protection of the collective interests of consumers.[731] Such sectors include inter alia the financial services, energy, telecommunications and health[732], which, in the future, will be characterised by a considerable growth of the application of connected devices. Hence, if the EU legislature decides to introduce a general and/or sector-specific access rights on which also, but not only, consumers could rely, the new Directive would also extend the system of representative actions to such fields. Moreover, this extension of the scope of application of the Directive would also include violations of data protection, hence, also including violations of the data portability right of Article 20(1) GDPR.[733] As regards the remedies, the Proposal considerably broadens the kind of redress that consumer associations can ask for,[734] which could also be enormously helpful to get judgments that generally bring precision to the terms of the licensing contract under which a data holder has to provide access. In sum, the upcoming legislative debate on this new proposal should also pay particular attention to the working of the new directive as regards access rights to consumers.

k) Conclusion

In line with the preceding analysis the EU legislature can be recommended considering legislation on a general data access right for enabling best use of connected devices. In parallel to such legislation, the Commission should engage in further empirical studies in different sectors where connected devices are used to build sector-specific data governance regimes. Whereas the field of

[728] In general, on the need to improve collective enforcement in the interests of consumers as regards the digital economy, see Micklitz (n 493) 21-23.

[729] See Directive 2009/22/EC of the European Parliament and of the Council of 23 April 2009 on injunctions for the protection of consumers' interests, [2009] OJ L110/30.

[730] Proposal of the Commission of 11 April 2018 for a Directive of the European Parliament and the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM(2018) 184 final.

[731] The concept of 'collective interest' is defined very vaguely by the 'interests of a number of consumers'. See Art 3(3) Proposed Directive. This means that the specific law that are violated do not need to be limited in scope to the protection of consumers.

[732] See Recital 6 Proposed Directive.

[733] Ibid. Collective actions of consumer associations against data protection violations are already possible in Germany. See Lea Kosyra and Irina Domrath, 'Datenschutz und Rechtsdurchsetzung' in: Hans-Wolfgang Micklitz, Lucia A Raisch, Gesche Josst and Helga Zander-Hayat (eds), Verbraucherrecht 2.0—Verbraucher in der digitalen Welt (Baden-Baden: Nomos, 2017) 135, 152-55 (with a discussion of the pros and cons). Courts in Germany accepted actions by consumer associations for violation of data protection rules even before. See Helberger, Zuiderveen Borgesius and Reyna (n 435) 1452.

[734] Art 6(1) Proposed Directive.

autonomous driving already attracts a lot of attention, from a consumer perspective, special consideration should be given to smart homing. Legislation on a generally applicable data access regime does not exclude parallel or later sector-specific legislation. Rather, its function is also to gather practical experience in the various sectors that can then be used for additional, oftentimes sector-specific regulation. In particular, legislation on the general regime should indicate in its recitals that such regime is not designed to replace sector-specific legislation. Rather, it could even include mechanisms, such as sector inquiries conducted by the Commission, similar to sector inquiries within the realm of competition law[735], to identify the need for sector-specific rules.

The general data access right should include the following elements:

(1) The data access right should be designed as a non-waivable statutory right of access to data against the *de facto* data holder of data.

(2) The access right should not be limited to personal data.

(3) The data access right should extend to all data that the holder of the right needs to make best use of a connected device. This includes data necessary for repairing the device, for connecting the device with other devices and for receiving or providing data-related services.

(4) The holder of the access right should be the person who holds a legitimate interest in making best use of the data, this includes in particular the owner or the long-term user of the device. An independent data-based service provider should not be considered holding such an interest without being mandated with providing such a service by a person with a legitimate interest in receiving the service.

(5) Legislation should not to be limited to the protection of consumers.

(6) The data access right should include the right to have the data transferred to a third person or entity providing a data-related service.

(7) The right must not be transferable to any other person with the exception of a person.

(8) The data access right should be without prejudice to the data protection rights of others.

(9) The data access right should take precedence over the sui generis database right and trade secrets protection of the manufacturer in the relevant data. However, the manufacturer should be authorised to impose confidentiality obligations on the holder of the data access right to secure trade secrets protection against third persons, especially competitors in the device market.

(10) Whether and under which conditions the holder of the access right is under an obligation to pay a fee for obtaining access should be regulated and decided in the framework of a flexible FRAND regime.

(11) The person under the duty to grant access should be allowed to regulate the concrete terms of access and use of the data in the framework of an end-user licence agreement in full respect of the data access right.

(12) Legislation should include a prohibition that prevents manufacturers from imposing restrictions on distributors of the connecting device that would obstruct the possibilities of the right holder to exercise the data access right.

[735] Art 17 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, [2003] OJ L1/1. On the EU level, Art 17 seems broad enough to be used by DG Competition to explore whether sector-specific access rights are needed.

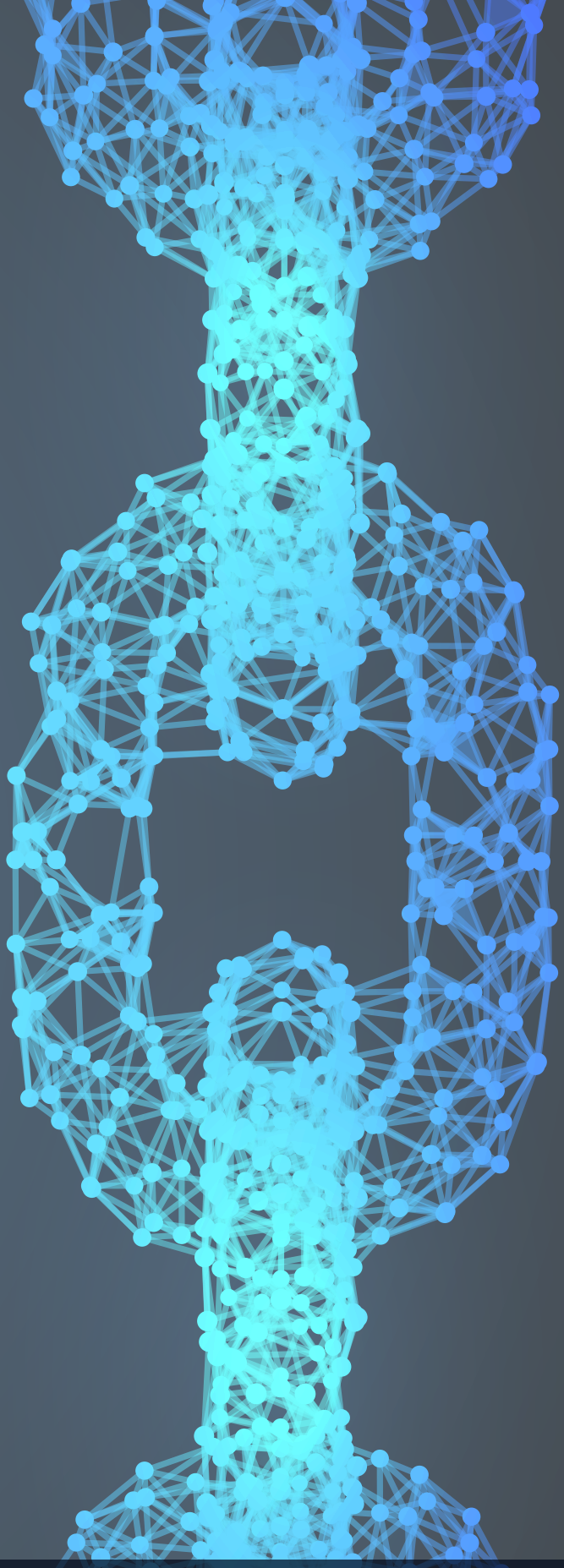
(13) There is also a need to provide for enforcement of the general access right—and, of course, of any sector-specific access rights—in the collective interest of consumers. The proposed new Directive of representative actions for the protection of the collective interests of consumers has the potential of providing collective redress against violations of data access rights. In the upcoming legislative debate, particular attention should therefore be paid to the working of this Directive with regard to access rights.

Published in December 2018 by BEUC, Brussels, Belgium.

BEUC-X-2018-111

The European Consumer Organisation
Bureau Européen des Unions de Consommateurs
Europäischer Verbraucherverband
Rue d'Arlon, 80 Bte 1, B - 1040 Bruxelles

BEUC The European Consumer Organisation



This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020). The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.