

The existing European IP rights system and the data economy – An overview with particular focus on data access and portability

Matthias Leistner*

A. Introduction

When the EU Commission launched its 2017 consultation ‘Building the European Data Economy’¹ many commentators were rightly concerned that this might lead to the creation of a new data producer’s right (or similar exclusive property rights in data) although doctrinal or empirical evidence on the need for any such right was completely lacking. The subsequent discussion has clearly shown that a data producer’s exclusive property right does not contribute to the solution of the very specific problems which have to be solved in order to foster the development of functioning data markets in the EU.² Since then, literature has increasingly focused on

* The author thanks his research assistants Lucie Antoine and Lukas Kleeberger for valuable help with research for this chapter.

1 See European Commission, ‘Public consultation on Building the European Data Economy’ (2017) <<https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy>> all accessed 31 August 2020.

2 Josef Drexel and others, ‘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’’ (2017) Max Planck Institute for Innovation and Competition Research Paper No 17–08 <www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf> accessed 31 August 2020; Wolfgang Kerber, ‘A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis’ (2016) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 989; Wolfgang Kerber, ‘Governance of Data: Exclusive Property vs. Access’ (2016) 47 *International Journal of Intellectual Property and Competition Law* 759.

contract law,³ competition law⁴ and/or possible regulation of data access including the more recent discussion on users' access rights.⁵

Consequently, and rightly so, the EU after the initial fact finding followed a very limited, targeted approach in the data economy sector by first enacting the Regulation on free flow of non-personal data in the EU,⁶ applicable as of 28 May 2019, whose main objective is to remove any remaining national law obstacles to the free movement of non-personal data within the EU, ie an almost complete abolishment of national data localisation requirements in the EU market. Moreover, the Commission has taken the important and useful initiative to formulate best practices for the contractual allocation of data in data related co-operation networks.⁷ In the 2020 Communication on 'A European strategy for data'⁸, the Commission concentrates (inter alia) on measures to improve access and use through a cross-sectoral data governance framework, infrastructures for hosting, processing and using data (in particular interoperability), and the develop-

3 Cf. briefly section D. below.

4 Heike Schweitzer, 'Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung' (2019) *Gewerblicher Rechtsschutz und Urheberrecht* 569; Heike Schweitzer and Martin Peitz, 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?' (2018) *Neue Juristische Wochenschrift* 275; Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era – Final report' (European Commission 2019) <<https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>> accessed 31 August 2020; Wolfgang Kerber, 'Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection' (2016) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* 639, 642–643; Jason Furman, Diane Coyle, Amelia Fletcher, Derek McAuley and Philip Marsden, 'Unlocking Digital Competition – Report of the Digital Competition Expert Panel' (UK Government 2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf> accessed 31 August 2020; Heiko Richter and Peter R. Slowinski, 'The Data Sharing Economy: On the Emergence of New Intermediaries' (2019) 50 *International Journal of Intellectual Property and Competition Law* 4.

5 See section C.IV. below.

6 Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59.

7 Communication of the European Commission of 25 April 2018 – 'Towards a common European data space' COM(2018) 232 final and detailed accompanying European Commission Staff Working Document, 'Guidance on sharing private sector data in the European data economy' SWD(2018) 125 final. See further Richter and Slowinski (n. 4).

8 Communication from the Commission of 19 January 2020 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 66 final.

ment of European data spaces in strategic sectors and domains of public interest. This distinctive focus on data access and portability has meanwhile led to the Commission's proposals for a Data Governance Act⁹ and a Digital Markets Act (DMA).¹⁰ In particular, the DMA, which follows a concept of targeted regulation in order to improve contestability and prevent unfair practices in the sector of so-called gatekeeper-platforms also contains data-related access and portability provisions inter alia in Article 6(1) lit. h), lit. i) and lit. j).

Apart from these targeted and useful European political projects, academic discussion on access rights has intensely continued since 2017 and developed more specific depth.¹¹ In particular different access scenarios have been considered. These scenarios – very roughly – comprise, first, access of lawful users to their own individual-level data (collected by the producer or service provider, e.g. in the context of IoT) and portability of such data to other operators.¹² Secondly, access of competitors to entire sets of aggregated data is discussed, where such access is necessary to establish workable competition in certain aftermarkets or complementary markets (and also, under stricter conditions, in the primary market). Thirdly, access to data generated by public bodies is a relevant case group because non-discriminatory access to such data for all interested parties can obviously generate significant positive externalities.¹³ Fourthly, and specifically in the context of competition law, access to large aggregated data sets of big data

9 Proposal of 25 November 2020 for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), COM(2020) 767 final.

10 Proposal of 15 December 2020 for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final.

11 See, for example, Crémer, de Montjoye and Schweitzer (n. 4); Josef Drexler, 'Data Access and Control in the Era of Connected Devices – Study on Behalf of the European Consumer Organisation BEUC' (BEUC 2018) <www.ip.mpg.de/fileadmin/ipmpg/content/aktuelles/aus_der_forschung/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 31 August 2020; Data Ethics Commission of the German Federal Government (*Datenethikkommission*), 'Opinion' (2019) 90–92, 124–157 <www.bmju.de/SharedDocs/Downloads/DE/TheMen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3> accessed 31 August 2020; Schweitzer (n. 4); Schweitzer and Peitz (n. 4) 279.

12 See further on this categorisation, which is also followed in this paper, Schweitzer, 'Datenzugang in der Datenökonomie' (n. 4) 572–74. Of course, different systematisations, some more detailed, exist in abundance.

13 See Richter and Slowinski (n. 4); Schweitzer (n. 4) 572; Opinion of the Data Ethics Commission (n. 11) 148; EU Commission, 'Towards a common European

conglomerates in order to develop entirely unrelated products or services has been discussed, resulting in the recent political initiative for the 10th Revision of the German Act against Restraints of Competition (*Gesetz gegen Wettbewerbsbeschränkungen, GWB*).¹⁴

All these case groups raise intricate problems concerning their relationship with IP protection of certain data-related creations, investments, products or processes.¹⁵ In that regard, EU policy has increasingly focused on the role of the Database Directive¹⁶ in different typical big data and AI use scenarios. Indeed, the Evaluation of the Database Directive by the Commission¹⁷ as well as in particular the underlying academic Evaluation Report¹⁸ have shown that the Database Directive is a case for imminent reform in this context.¹⁹ However, concentration on the database *sui generis*

data space' (n. 7) 4–8; cf. Heiko Richter, "Open Government Data" für Daten des Bundes' (2017) *Neue Zeitschrift für Verwaltungsrecht* 1408.

- 14 See Schweitzer, 'Datenzugang in der Datenökonomie' (n. 4) 576–80. As regards the Revision of the German Act against Restraints of Competition see the Government Bill *Gesetzentwurf der Bundesregierung – Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer wettbewerbsrechtlicher Bestimmungen (GWB-Digitalisierungsgesetz)* (9 September 2020) <www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&cv=6> accessed 15 September 2020. Concerning access contained in this draft see (from an economic perspective) Wolfgang Kerber, 'Datenzugangsansprüche im Referentenentwurf zur 10. GWB-Novelle aus ökonomischer Perspektive' (2020) *Wirtschaft und Wettbewerb* 249.
- 15 The same applies in regard to their interface with the protection of personal data under the GDPR; comprehensively on IP and personal data protection with a particular view to the ongoing and future regulation of the data economy see Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data – Rahmenbedingungen im europäischen Datenschutz- und Immaterialgüterrecht und übergreifende Reformperspektive* (Mohr Siebeck 2021).
- 16 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.
- 17 European Commission Staff Working Document, 'Executive Summary of the Evaluation of Directive 96/9/EC on the legal protection of databases' SWD(2018) 146 final.
- 18 Lionel Bently, Estelle Derclaye and others, 'Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases – Final Report' (2018) <<https://op.europa.eu/de/publication-detail/-/publication/5e9c7a51-597c-11e8-ab41-01aa75ed71a1>> accessed 31 August 2020.
- 19 See already 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* (Nomos 2018) 27.

right, although it is indeed the most imminent problem in EU IP law, fails to see the whole picture. In fact, the influence of the existing IP-rights system on (1) the possibility and form of possible access rights as well as (2) on the very infrastructure for data portability, ie the practical achievement of the necessary degree of interoperability and – on that basis possibly in the future – real-time exchange and portability of data, should not be underestimated. In this paper I will try to give an initial overview of the main issues which will have to be considered in this respect.

Accordingly, the focus is on selected aspects of the recent data access and portability discussion, where existing EU IP regulation has a particularly influential impact. First, problems concerning the infrastructural framework for data access and portability will be discussed: Namely, general copyright law, patent law and trade secrets protection should ideally not add unnecessary legal barriers to access to certain mainly technical infrastructures, such as data file formats, application programming interfaces (APIs) as well as interfaces in general (see below B). Secondly, the recent access discussion will be analysed from the perspective of current EU IP law, in particular copyright, sui generis protection and trade secrets protection, resulting in several proposals for an immediate revision of the database sui generis right (see below C). Thirdly, I will briefly discuss a couple of elements in the existing IP regime which might prove helpful as building blocks for a future regulation of the data economy (see below D).

B. IP rights and interoperable formats for data portability

I. Copyright law: freedom of interfaces and data formats

Access to data and the development of data markets in general require that there be free and accessible infrastructures for the exchange of data between different market players.²⁰ In fact, if real-time exchange of data is needed in certain areas beyond the technically rather limited non-real-time instrument in Article 20 General Data Protection Regulation (GDPR)²¹ – and from this author's viewpoint even to make the limited solution in Ar-

20 See, for example, Crémer, de Montjoye and Schweitzer (n. 4) 83 et seq. On interoperability see generally Furman and others (n. 4) 64 et seq.

21 Regulation (EU) 2016/679 of the European Parliament and 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 [2016] OJ L119/1.

ticle 20 GDPR at least work effectively in practice – open and accessible APIs are of the essence. Copyright protection for computer programs can be a potential problem in that regard if protection is extended to interface structures or data file formats (such as in the highly controversial Federal Circuit’s *Google/Oracle* case, which will now be ultimately decided by the U.S. Supreme Court).²²

In Europe, the situation seems less problematic and comparatively stable. The relevant EU Computer Program Directive²³ of 2009 (originally enacted in 1993) expressly acknowledges the need for interoperability *inter alia* in its Recitals 11, 15 and 19. Accordingly, the Court of Justice of the EU (CJEU) has decided in its *SAS Institute* judgment²⁴ that programming languages and data file formats as such are not copyright protected under EU protection for computer programs. Although this is still under discussion in Europe, many authors have derived *inter alia* from that judgment that API infrastructures as such should not be copyrightable under EU copyright law.²⁵

Also, Article 6 of the Computer Program Directive contains a specific exception to copyright for decompilation, i.e. use acts which are indispensable to obtain the information necessary to achieve interoperability. In line with this objective, the provision covers acts of decompilation performed in order to obtain information on the elements and structure of interfaces. This exception cannot be overridden by contractual agreement. Nonethe-

22 See *Oracle Am., Inc. v Google LLC* 886 F.3d 1179 (Fed. Cir. 2018); pending proceedings *Google LLC v Oracle Am., Inc.* before the US Supreme Court under Docket No. 18–956.

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

24 Case C-406/10 *SAS Institute v World Programming* ECLI:EU:C:2012:259, paras. 29–46.

25 Jochen Marly, ‘Der Schutzgegenstand des urheberrechtlichen Softwareschutzes’ [2012] *Gewerblicher Rechtsschutz und Urheberrecht* 773, 779; more open in the prognosis Simonetta Vezzoso, ‘Copyright, Interfaces, and a Possible Atlantic Divide’ (2012) 3 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 153, para. 40, who however herself requests freedom of interface structures; with a useful distinction between the interface structures and their specific implementation and programming in code Pamela Samuelson, Thomas C. Vinje and William R. Cornish, ‘Does copyright protection under the EU Software Directive extend to computer program behaviour, languages and interfaces?’ (2012) 34 *European Intellectual Property Review* 158–159, 163–164; similarly Christian Heinze, ‘Software als Schutzgegenstand des Europäischen Urheberrechts’ (2011) 2 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 97, para. 8.

less, the provision's impact in practice has remained limited, which might be due to the fact that Article 6 Computer Program Directive – like the majority of exceptions to copyright – does not give a subjective right to access but instead only exempts certain use acts from the scope of copyright protection. Therefore, the bigger problem in regard to access to interface information and other information necessary to achieve interoperability might be caused by factual limits on the accessibility of the information as well as by possible trade secret protection.²⁶

II. Patent law: from protection of data formats towards protection of formatted data?

1. Patents on data encryption and transfer processes, in particular standard-essential patents

German and European patent law is (and will become) much more relevant to the question of access to data portability infrastructures than might be assumed at first sight. In fact, data encryption and transfer processes can undoubtedly be patented as procedure patents under certain conditions. Where such patents are essential for the implementation of a standard (standard-essential patents, SEPs), typically, the patent holder will have submitted a so-called FRAND declaration²⁷ in the standardisation process.²⁸ In the EU, the enforcement of such FRAND-encumbered SEPs is

²⁶ See sub-section III. below.

²⁷ I.e. a declaration to license the patent to any interested party under fair reasonable and non-discriminatory conditions. See, for instance, ETSI's FRAND-licensing declaration <www.etsi.org/images/files/IPR/etsi-ipr-form.doc> accessed 31 August 2020, or the ITU's RAND-licensing declaration <www.itu.int/oth/T0404000002/en> accessed 31 August 2020.

²⁸ In particular, with regard to telecommunications standards, but also with regard to standards in the electronics sector and probably in future for many standards in the AI field, formal processes of de iure standardisation apply, where a valid FRAND declaration is a mandatory requirement for being considered for the standard; see, for instance, the respective policies of ETSI <www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf> accessed 31 August 2020, and ISO/IEC/ITU <https://isotc.iso.org/livelink/livelink/fetch/2000/2122/3770791/Common_Policy.htm?nodeid=63447648&vernum=-2> accessed 31 August 2020. For mere de facto standards it is currently under discussion whether the same principles should apply as under the Huawei/ZTE regime or whether a more limited approach, such as under the old judgment of the German Federal Supreme Court (BGH), 6 May 2009, Case KZR 39/06 (2009) Gewerblicher Rechtsschutz und Urheberrecht 694 – Orange

governed by the CJEU's judgment in *Huawei/ZTE*.²⁹ As for the original patent holder who submitted the FRAND declaration, this will result in a limited legal position which does not allow the patent holder to file proceedings for an injunction before making a FRAND offer to the implementer and seriously negotiating a FRAND licence. While there is no room to go into the details and considerable practical difficulties in this particular field,³⁰ at least on principle this enforcement regime seems capable of enabling sufficient access to the essential patents for any seriously interested party.

One more problem of general importance, however, should be briefly mentioned. This concerns the particularly intricate question of whether an *inter omnes* effect can be derived from the underlying network of FRAND declarations in such areas. Currently, significant problems arise with regard to situations where the patent has been transferred to third parties, in particular so-called non-practicing entities, which are themselves not bound by the FRAND declaration of the original patent holder. In a recent judgment, the Higher Regional Court of Düsseldorf has assumed that in such cases, if the patent is standard essential and vests a dominant market position in the person of the acquirer, the FRAND declaration will have a 'quasi in rem' effect and equally bind the acquirer.³¹ While this is a workable, convincing result,³² the underlying dogmatic construction of the court (i.e. the assumed in rem effect of the FRAND declaration as such) seems not entirely beyond doubt.

Book Standard, should apply. See for a differentiated view on this with further references Matthias Leistner, 'Intermediary Liability in a Global World' in Tatiana E. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Wolters Kluwer 2019) 471.

29 Case C-170/13 *Huawei* ECLI:EU:C:2015:477.

30 See further, for example, Matthias Leistner, 'European Experiences: EU and Germany' in Kung-Chung Liu and Reto M. Hilty (eds), *SEPs, SSOs and FRAND – Asian and global perspectives on fostering innovation in interconnectivity* (Routledge 2019) Ch. 15; Peter G. Picht, 'The ECJ Rules on Standard-Essential Patents: Thoughts and Issues Post-Huawei' (2016) 37 *European Competition Law Review* 365; Peter G. Picht, 'FRAND Injunctions: an overview on recent EU case law' (2019) *Zeitschrift für Geistiges Eigentum* 324.

31 Düsseldorf Higher Regional Court (*OLG Düsseldorf*), 22 March 2019, Case 2 U 31/16 (2019) *Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report* 6087 – *Improving Handovers*.

32 See already Hanns Ullrich, 'Patente und technische Normen: Konflikt und Komplementarität in patent- und wettbewerbsrechtlicher Sicht' in Matthias Leistner (ed.), *Europäische Perspektiven des geistigen Eigentums* (Mohr Siebeck 2010) 14.

Instead of this construction, from this author's viewpoint, an essentially competition law-based solution should be considered as follows.³³ As for Article 102 TFEU, the CJEU in *Huawei/ZTE* did not require that it is the current SEP holder who has declared her willingness to license the patent to any third party on FRAND terms.³⁴ Instead, the judgment can be read to say that the Court only required that the patent as such be subject to a FRAND declaration in order to trigger the duties under Article 102 TFEU for any subsequent market-dominant acquirer of the patent in question. Therefore, the EU competition law-based specific enforcement regime for SEPs should apply to any market-dominant patent holder who has acquired a FRAND-encumbered patent without regard to the question of whether the (new) patent holder herself declared her willingness to license the acquired patent under FRAND conditions.

Moreover, depending on the applicable substantive law,³⁵ the FRAND declaration can also entail a contract for the benefit of third parties between the declaring patent holder and the standard-setting organisation whereby the third party, ie the implementer, is entitled to assert the claim to FRAND licensing independently (*Vertrag mit Schutzwirkung zugunsten Dritter; stipulation pour autrui*). The catalogue of duties arising from this contract should in principle be the same as under the *Huawei/ZTE* regime established by the CJEU. From this author's viewpoint, the duties from this contract will also, in certain situations, be passed on to subsequent acquirers of the patent under the principle of good faith as an ancillary duty of the acquiring party under Section 241(2) German Civil Code (obligation to have regard to the generally known interest of the seller to pass on

33 I first encountered this basic idea in my Munich seminar on German and European intellectual property law, where it was brought to my attention by my student Mark Hillenbrand.

34 Cf. Case C-170/13 *Huawei* ECLI:EU:C:2015:477, para. 49, according to which the case was characterised by the fact 'that the patent at issue is essential to a standard established by a standardisation body, rendering its use indispensable to all competitors which envisage manufacturing products that comply with the standard'. This clearly refers to the *patent as such*, not to the person of the patent holder.

35 As for the hitherto practically important ETSI FRAND declarations (which might become even more important in the future as ETSI is also preparing standards in the AI field), the applicable substantive law will be French law; see Mary-Rose McGuire, 'Die FRAND-Erklärung – Anwendbares Recht, Rechtsnatur und Bindungswirkung am Beispiel eines ETSI-Standards' (2018) *Gewerblicher Rechtsschutz und Urheberrecht* 128; Matthias Leistner and Lukas Kleeberger, 'FRAND-Erklärungen ohne Rechtswahl am Beispiel der Standardisierungsorganisationen ITU/ISO/IEC: Ein praxisrelevantes dogmatisches Problem im internationalen Privatrecht' (forthcoming 2021).

the FRAND obligation in order to keep the sales contract valid) even if the parties do not expressly stipulate that obligation in the contract underlying the transfer of the patent. This entire approach, which is set out in another paper,³⁶ cannot be deepened here in detail. Suffice it to say that, in regard to SEPs which are essential for certain existing or possible future data exchange standards or AI applications, competition and contract law-based solutions can be developed which will ultimately at least on principle enable workable access on fair, reasonable and non-discriminating conditions for any seriously interested party. Moreover, under a more general perspective the contract law-based approach under the principle of good faith and Section 241(2) German Civil Code which has been briefly sketched here might also be useful to acquire limited inter omnes effects of certain basic structural elements of contract-based data biotopes (networks) when parts of the data are passed on to outsiders.

2. Scope of patents concerning formatted data sequences

Another even more intricate and difficult problem in patent law, which has the potential to significantly hamper the development of free and accessible technical data exchange infrastructures in the EU and Germany, concerns the scope of protection of process patents on certain data encryption or compression processes, specifically in regard to the data sequences which result from the application of the patented process. In two more recent judgments the German Federal Supreme Court has held that such data sequences or information might enjoy patent protection as a product which is produced directly by a patented process (see Section 9 No. 3 Patent Act).³⁷ Meanwhile, this therefore conceivable protection has been

36 See Matthias Leistner and Lukas Kleeberger 'Die Drittwirkung von FRAND-Erklärungen aus kartellrechtlicher und vertragsrechtlicher Sicht' (2020) Gewerblicher Rechtsschutz und Urheberrecht 1241.

37 German Federal Supreme Court (BGH), 21 August 2012, Case X ZR 33/10 (2012) Gewerblicher Rechtsschutz und Urheberrecht 1230 – *MPEG-2-Videoenkodierung*, in which the Court assumed that a data sequence directly resulting from the operation of the patented MPEG-2 video compression procedure had to be regarded as a direct product of the patented process and that consequently any import, marketing or distribution concerning such sequences could on principle infringe the patent rights of the holder of the underlying process patent; slightly more cautious already German Federal Supreme Court (BGH), 27 September 2016, Case X ZR 124/15 (2017) Gewerblicher Rechtsschutz und Urheberrecht 261 – *Rezeptortyrosinkinase II*.

subjected to certain qualifications³⁸ and, what is more, patent protection for such data sequences as a direct product of a patented process will generally be exhausted upon first sale of the sequence.³⁹ Nonetheless, such reach-through patent protection for data files seems unnecessary to incentivise innovation in the field of data encryption and compression technology. At the same time, it has obvious dysfunctional potential to block necessary access to the information as such, based on the mere format in which the information is encrypted or compressed. Therefore, from this author's viewpoint, as a more straightforward solution, patent protection should not be granted for mere data sequences on the basis of Section 9 No. 3 Patent Act.

III. Trade secrets

Obviously, trade secret protection can play a large role with regard to secret information on data file formats and interfaces where this is necessary to achieve interoperability and portability.⁴⁰ According to European competition law, access to IP-protected information and data structures will be granted if the information in question is indispensable to offer a new product or service in a secondary market in relation to the (hypothetical) licensing market and if the unjustified denial of access would effectively foreclose workable competition on that market.⁴¹ In these cases, access will be generally granted on the condition that the user pays a fair and reasonable licensing fee, ie on the basis of a compulsory licence. Such access on the basis of compulsory licences can also be granted where trade secret protected information on interfaces is necessary to achieve interoperability, if the conditions of Article 102 TFEU are met.⁴² In fact, in the *Microsoft* judg-

38 Information as such will not be protected; instead, the information must be structured in a way which still clearly reflects the patented process and gives the resulting data sequence part of its substantial value; moreover, the resulting data sequence as such will have to be capable of being marketed and traded in a way which is typical for an independent product. See further on these qualifications the judgment in *Rezeptortyrosinkinase II* (n. 37).

39 German Federal Supreme Court in *MPEG-2-Videosignalkodierung* (n. 37).

40 See further on the EU framework for trade secrets protection section C.III below.

41 Cf. generally Joined Cases C-241/91 P and C-242/91 P *RTE v Commission* ('Magill') ECLI:EU:C:1995:98; Case C-418/01 *IMS Health* ECLI:EU:C:2004:257.

42 Cf. Case T-201/04 R *Microsoft v Commission* ECLI:EU:T:2004:372 and Case T-201/04 *Microsoft v Commission* ECLI:EU:T:2007:289. See also section C.IV.3.b) (3) below.

ment, which concerned trade secret-protected interface information the General Court has even watered down the new product or service condition to a mere requirement that the emergence of a competing product with innovative elements must be prevented by the denial of access.⁴³ Also, while this case group is traditionally based in the prevention of leveraging a dominant position between a primary market and a secondary aftermarket or market for complementary products or services, at a closer look, in the field of compulsory licences for the use of IP rights and trade secrets the CJEU's case law has effectively extended these cases to also cover situations where a new product or service in the actual primary (product or service) market is prevented. This is because in the *IMS Health* judgment, the Court regarded a merely hypothetical upstream market for licences in which the rightholder, who was only active in the downstream product market, had a dominant position as sufficient for a finding of leveraging between two markets.⁴⁴ Effectively, thus, a competitor who wanted to offer a competing product in the actual downstream product market where the rightholder was active, was granted a compulsory licence in the so-called (hypothetical) upstream market for licences for the essential IP right.⁴⁵

In regard to trade secrets protection this overall competition law framework provides for a structure which seems reasonably balanced between the possible need to protect the secrecy of essential technical information also in the field of interface infrastructures, and the objective to grant access to interface information in order to protect or enable workable competition. In detail, in cases in which real leveraging between two markets takes place and when the rightholder is indeed a market-dominant undertaking in the upstream market, the new product or service criterion should be given up;⁴⁶ but this can be achieved in case law and does not require legislative action. From a practical viewpoint, one might also ask whether the competition law instruments, because of their specific rules on burden of proof and their specific enforcement structures, will not often come too late to remedy actual access problems in the field of the data economy. This indeed is a justified concern which will be discussed below (C IV 3 b (3)) in the context of possible 'IP-internal' provisions on compulsory li-

43 Case T-201/04 *Microsoft v Commission* [2007] ECLI:EU:T:2007:289, paras 643–665.; Schweitzer (n. 4) 578.

44 Case C-418/01 *IMS Health* ECLI:EU:C:2004:257, paras 44–45.

45 See further Matthias Leistner, 'Intellectual Property and Competition Law: The European Development from Magill to IMS Health Compared to Recent German and U.S. Case Law' (2005) 3 *Zeitschrift für Wettbewerbsrecht* 138.

46 Cf. Leistner (n. 45) 150–152; Schweitzer (n. 4) 578.

cences for systematically identifiable situations, where barriers to market entry necessarily and directly follow from IP protection for certain data. Similar specific provisions for compulsory licences concerning access to trade secret-protected interface information should have been considered in the enactment of the Trade Secrets Directive of 2016;⁴⁷ however, at the moment, this is not an immediately pressing political need which would require a revision of the Directive in the short term.

As for the specific issue of decompilation of computer programs in order to obtain information necessary to achieve interoperability of computer programs and portability of data (ie information on data file formats and interfaces), however, a remarkable systematic tension between the approach of the Computer Program Directive⁴⁸ and the approach of the Trade Secrets Directive can be observed, which has to be solved immediately. The Trade Secrets Directive provides for a general limitation of protection for any act of ‘observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer’ (ie reverse engineering, see Article 3(1)(b) Trade Secrets Directive). However, this liberty of the acquirer can be limited by contractual agreement. Insofar as the specific case of decompilation of computer programs is concerned, which will typically be the case when an acquirer tries to obtain information on data file formats and interfaces, this is in tension with the more liberal rule in the Computer Program Directive, which provides for an exception for decompilation that can expressly not be overridden by contract.⁴⁹ This latter rule reflects the fact that typically interface information will be of particular importance to foster dynamic efficiency through interoperability, while at the same time interfaces will typically be an essential part of the developed software anyway, so that no additional protection to incentivise innovation in the area via the very strong and long-term copyright regime is needed. The same cost-benefit ratio in fact seems to apply to acts of reverse engineering of interfaces in regard to trade secrets protection; what is more, such tinkering (in this specific field as well as generally) has increasingly become a valuable source of innovation in AI and big data.⁵⁰ From this author’s viewpoint,

47 Directive (EU) 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 L157/1.

48 See section I. above.

49 See section I. above.

50 Pamela Samuelson, ‘Freedom to Tinker’ (2016) <<https://ssrn.com/abstract=2800362>> accessed 31 August 2020.

therefore, in cases where decompilation is essential to obtain information necessary for interoperability and data portability, the Computer Programs Directive's approach, as a *lex specialis*, should be applied, thus also exempting the necessary acts from possible trade secrets protection without a possibility for the owner of the trade secret to override this by way of contractual agreement.⁵¹

C. The discussion on access to and portability of data and the existing EU IP-rights framework, in particular database sui generis protection and trade secrets

I. Overview

As for the relationship of access and portability regimes to existing IP protection in Europe, an immediate overlap can indeed occur when use of data is concerned that are as such IP-protected or only accessible via an IP-protected database. Direct IP protection of information as such exists neither in patent law nor in copyright law. However, the database *sui generis* protection right (and partly also copyright protection in database works), although in theory merely protecting substantial investment into databases, in practice comes close to a protection of information as such in certain situations. Therefore, the main problematic area of IP law which will have to be discussed in this part is the *sui generis* protection right for databases. Besides, the protection of trade secrets could also sit uncomfortably with data access regimes requiring disclosure of confidential data and will therefore also have to be included in the analysis.

51 Thomas Dreier, in Thomas Dreier and Gernot Schulze (eds), *Urheberrechtsgesetz* (6th edn, C.H. Beck 2018) Sec. 69e UrhG para. 5.

II. Access to data, copyright in databases and database sui generis protection – Current problems and the case for immediate reform of the Database Directive

1. Introduction – impact of European database protection on big data and AI use scenarios

The recent discussion of the function and relevance of the Database Directive's⁵² sui generis right for the European data economy has been partly characterised by the assumption that in most big data situations the crucial condition of a 'substantial investment' will not be fulfilled.⁵³ I have shown elsewhere that this assumption might be mistaken.⁵⁴ Instead, one should be aware that database sui generis protection (and partly also copyright protection) can potentially come into play in numerous different typical big data and AI use scenarios. Compilations of independent elements such as geographical data, certain kinds of sensor-measured data (although a number of differentiations has to be made in this case group), sales and all kinds of commercial data etc. can potentially qualify for protection depending on the circumstances of the case. This is not to say that investments in the compilation of such data should be protected in all these different case groups. Instead, this analysis should serve as a *warning* that the database sui generis right might be more relevant than generally thought for both the protection and the access aspects of big data use case scenarios.⁵⁵

2. Copyright in database works – limited and balanced approach in the EU

The typical creativity involved in the development of big data-based AI models and applications, i.e. the structuring and weighing of the cost functions, selection and combination of training data etc.⁵⁶ seems on principle eligible for protection as a database work under EU copyright law, i.e. it is potentially copyrightable as a structured compilation of independent ele-

52 Database Directive (n. 16).

53 European Commission SWD (n. 17) 2.

54 Leistner (n. 15). With the same conclusion and a rigorous analysis see also Drexel (n. 11) 67–85; more differentiated also Bently and others (n. 18) 29–31.

55 Cf. also Bently and others (n. 18) 29 referring to Leistner.

56 See further Drexel and others (n. 2).

ments.⁵⁷ The same might potentially apply to any creative structuring process (selection or arrangement) behind the creation of inferred data.⁵⁸

Given that in particular in the EU the exceptions to copyright are too narrow and rigid to accommodate the dynamic and multipolar use of training data and weighing factors in different contexts and problem-specific combinations (data biotopes), copyright law could therefore be a significant source of additional transaction costs and contribute to lock-in and even holdup potential if it were over-extended to everyday methods of selecting, structuring and combining datasets. However, the CJEU has rightly specified the condition of copyright protection in Europe in a very strict and targeted way in its more recent case law. Hence, according to the CJEU's judgment in *Football Dataco/Yahoo* mere intellectual effort, skill, judgment and labour in the selection and structuring of the elements of a database work will not suffice for copyright protection. In particular, technical or rather abstract mathematical considerations or methods will not qualify if they do not leave room for the expression of personal creativity in an original manner by making free and creative choices and thus stamping the database with a 'personal touch'.⁵⁹

For this reason, database copyright protection in the EU, while on principle being capable of protecting certain outstanding achievements in the area of AI and big data (in particular certain outstanding sets of training data in specific areas), will not protect the typical selection and combination of data in order to compile and combine optimised training data sets and the respective weighing of factors to optimise the cost functions in

57 By contrast, copyright protection for computer programs will typically not play a significant role in these cases because copyright protection of computer programs is limited to the creative coding as such, whereas the development of underlying mathematical structures, algorithms, abstract procedures etc. is not covered. See Art. 1(2) Computer Programs Directive (n. 23).

58 On the category of inferred data see Crémer, de Montjoye and Schweitzer (n. 4) 24–29; Schweitzer, (n. 4) 571; proposing such categorisation already World Economic Forum, 'Personal Data: The Emergence of a New Asset Class' (January 2011) 7 <www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf> accessed 31 August 2020.

59 Case C-604/10 *Football Dataco v Yahoo* ECLI:EU:C:2012:115, paras 31 et seq., in particular paras 38 et seq. Similarly, in the recent *Funke Medien* judgment, the Court has applied strict criteria to potential copyright protection for mere factual reports and their structure when it is guided by the underlying practical purpose, thereby decidedly reducing the potential of copyright law to protect mere practical, AI-aided 'creations' in the area of written works. See Case C-469/17 *Funke Medien NRW* ECLI:EU:C:2019:623.

normal cases. Therefore, in the EU, copyright in computer programs⁶⁰ and compilations (database works) is currently not a significant cost factor for the future development of AI and big data and will presumably not pose substantial obstacles to the future technological development either. Instead, it seems that copyright law is comparatively well adjusted, as it might contribute to incentivising certain highly original, free and creative breakthrough developments in specific areas (in particular the development of fundamentally important, highly original data combinations as training data sets), while it does not have the potential to hamper the normal development of the data economy. If there is any problem with the current status of copyright law at all, it might even be a problem of under-incentivisation concerning the development and publication of valuable training data sets. However, if there were a problem in this sector, this would not be a problem copyright itself could solve. This is because copyright with its exclusive property right character and the unreasonably long term of protection is obviously poorly equipped to serve the – at least conceivable – need for tailor-made flexible and short protection in this area.

By contrast, with regard to underlying materials which are *used* for the compilation of training data and which might be protected by copyright law, the situation in European copyright is more problematic. Indeed, the question has to be asked whether the existing exceptions to copyright law in Europe are sufficient in that regard. Since the topic of this chapter is access to and protection of data (and not of the ‘raw material’ to create certain data), suffice it to say in this context that even the new text and data mining exceptions in Articles 3 and 4 DSM Directive⁶¹ do not seem sufficient in that regard. Further reform seems imminent and it is submitted that the Japanese copyright law exception for text and data mining (as a non-conclusive case example in the larger realm of irrelevant uses which do not allow the enjoyment of the work as such) could form a model in that regard.⁶²

⁶⁰ See section B.I. above.

⁶¹ Directive (EU) 2019/790 of the European Parliament and the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.

⁶² Art. 30–4 Japanese Copyright Act. See further Tatsuhiro Ueno, ‘A general clause on copyright limitations in civil law countries: Recent discussion toward the Japanese-style “fair use” clause’, in Shyamkrishna Balganes, Ng-Loy Wee Loon and Haochen Sun (eds), *The Cambridge Handbook of Copyright Limitations and Exceptions* (Cambridge University Press 2021) 211.

3. *Database sui generis protection right: current problems and immediate need for reform*

- a) Condition of protection and legal uncertainty in the area of volunteered and observed data

The database *sui generis* protection right – although on the face of it being limited to the protection of certain substantial investments in the obtaining, verification and presentation of the contents of a database – in many cases can practically come close to granting an exclusive property right against the use of certain data as such. The attempt of the CJEU to ameliorate this situation by excluding investments into the mere generation of data, often resulting in so-called sole-source data, in its leading judgment in *British Horseracing Board* and the resulting complex status quo have been comprehensively discussed elsewhere.⁶³ Only a brief overview shall be given here.

Concerning the condition of protection of a substantial investment in the obtaining, verification or presentation of the contents of a database, the situation is problematic mainly because at the moment it is characterised by undeniable legal uncertainty about the exact impact of database *sui generis* protection in typical data collection scenarios (namely concerning volunteered and observed data). In future, further specification of the condition of protection will be required – either in the written law or in case law – which should reflect the comparatively advanced discussion on the need to access these categories of data.

Thus, the collection of data, which on principle can be collected by any competitor, can qualify as a potentially substantial investment. Concerning the particularly problematic and uncertain case group of measured or observed data, the necessary distinctions should be guided by the principle that database *sui generis* protection should never directly raise unsurmountable barriers to market entry, both in the primary market as well as in aftermarkets or complementary markets.⁶⁴ Thus, the guiding principle should be that whenever observed or measured data cannot be observed or measured independently, ie data internal to the very application of a certain product or service (e.g. in particular certain real-time operating data concerning the operation of the product or service as such), the respective investments should not qualify for potential *sui generis* protection. This is

63 Leistner (n. 19).

64 Similarly Drexler (n. 11) 68, 71–73.

because in these cases, necessarily, there will be no other source for these data and therefore IP protection (in addition to factual control) would as such directly lead to a market-dominant position in the (actual or hypothetical) licensing market for this specific kind of data. By contrast, if certain external data are collected or observed only in the wider context of the application of a product or a service (e.g. a car measuring the outside temperature or collecting certain data on the road conditions; certain observed use data in the context of internet services; agricultural data delivered by farming machines; non-real-time motion profiles of a natural person), the respective investments can qualify for *sui generis* protection. This is because in these cases, at least if there is competition in the product or service market, such data can be acquired from different operators (sometimes even in different markets, such as different motion profiles which might be compiled by a car as well as by a smartphone) or could even be measured, observed or collected independently.

For the moment, these proposed initial guideposts, however, are neither laid down in the Database Directive nor in case law. Instead, the merely grammatical distinction between so-called ‘generated’ data and so-called ‘compiled’ data reigns in this sector and creates legal uncertainty. As a consequence, while there are no significant problems in the field of inferred data, in the area of volunteered or observed data⁶⁵ the *sui generis* right causes legal uncertainty and obviously has significant potential to lead to future access problems and to lock-in effects in certain situations depending on future CJEU case law in this area.

b) Scope of protection and problems for access to aggregated data sets

This is aggravated by the fact that the exclusive rights under Article 7(2) Database Directive, i.e. extraction and re-utilisation, have been construed very broadly in the CJEU’s case law. In fact, practices such as indirect extraction and even extraction for the compilation of substantially changed, value-added databases of a more or less different nature will be covered by these exclusive rights.⁶⁶ Moreover, the activities of typical meta-databases or meta-search websites, i.e. the automated gathering and compiling of da-

65 Crémer, de Montjoye and Schweitzer (n. 4) 24–29; Schweitzer (n. 4) 571.

66 Case C-304/07 *Directmedia Publishing* ECLI:EU:C:2008:552, paras 29–60.

ta from a multitude of different sources, are potentially infringing the sui generis right.⁶⁷

Compared to this rather broad construction of the exclusive rights, the limitation of the protected subject matter, i.e. the limitation to the use of substantial parts of a database or systematic and repeated extraction of insubstantial parts which add up to be a substantial part of the database,⁶⁸ is not an efficient means to protect freedom of competition and to prevent leveraging potential with respect to many typical big data uses. This is because in particular in the case group where competitors need access to aggregated data sets, typically, complete datasets, possibly even from different sources, will be needed. Consequently, the limitation of the protected subject matter to substantial parts of databases does not solve potential problems with access to data, which might arise in this case group.⁶⁹

To mirror this against the different discussed data categories and access scenarios: The database sui generis right can raise serious information and transaction cost problems in its current state, which is characterised by substantial legal uncertainty concerning its potential to protect volunteered or observed data. This particularly concerns the use scenario in which competitors need access to complete, aggregated data sets to access the primary market or certain entirely new, complementary or aftermarkets. Moreover, the sui generis right can worsen lock-in problems and even lead to holdup potential in certain situations where large amounts of individual-level use data are concerned.⁷⁰

c) Exceptions to the sui generis right, public sector data and further problems

Considering access to IP-protected subject matter, the exceptions to the concerned IP right come into focus. In the overarching general framework of EU fundamental rights, such exceptions express genuine user rights to freedom of expression and information which have to be fairly balanced with the right to protection of IP.⁷¹ On a more detailed, technical level, the existing exceptions to the sui generis right (Article 9 Database Directive) undoubtedly are too narrowly designed, in particular in comparison to the

67 Case C-202/12 *Innoweb* ECLI:EU:C:2013:850, paras 37–38.

68 Case C-203/02 *British Horseracing Board* ECLI:EU:C:2004:695, paras 87–88.

69 Cf. also Matthias Leistner as reported in Bently and others (n. 18) 57.

70 See section C.IV.3.b)(2) below.

71 Case C-469/17 *Funke Medien NRW* ECLI:EU:C:2019:623, paras 57–58.

broader general copyright exceptions.⁷² In fact, this critique becomes even more imminent with respect to the challenges of the data economy.

First, it seems to have been ignored in the legislative process that the *sui generis* right, by virtue of its autonomous nature, would not be subject to certain traditional limitations set out in national laws with regard to works protected under copyright. This leads inter alia to a significant problem in respect of databases established by public authorities, which are covered by exclusive *sui generis* protection even in countries where official works by public bodies are generally exempted from copyright under certain conditions. For the moment, this issue should be solved by an analogy to the copyright exception for official databases by public bodies.⁷³ However, the CJEU never explicitly decided on that question, hence this issue remains legally uncertain on the level of Union law. This also results in considerable tensions between the framework for access and use under the PSI Directive⁷⁴ and possible *sui generis* protection for databases created by public bodies (which will worsen when the new Open Data Directive⁷⁵ is implemented). For these problems, it seems that the appropriate solution straightforwardly follows from a contextual comparison to general copyright law. In general copyright law, such creations authored by public bodies are exempted from copyright protection, if the very policy or legal purpose of the creation is to be disseminated to the public to the maximum extent. It seems that under that same condition (i.e. legal or policy interest in maximum dissemination of certain data), a fortiori, databases created by public bodies should also be exempted from possible *sui generis* protection under the Database Directive. Only in the remaining cases where a direct

72 Annette Kur and others, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases - Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich' (2006) 37 *International Review of Intellectual Property and Competition Law* 551, 556-557. See also Matthias Leistner as reported in Bently and others (n. 18) 59.

73 Cf. Matthias Leistner, 'Anmerkung zu BGH, Beschluß vom 28 Spetember 2006, I ZR 261/03 – Sächsischer Ausschreibungsdienst' (2007) *Zeitschrift für Gemeinschaftsprivatrecht* 190, 193-94. With an overview of the current status of the debate on whether the exception of German copyright law for 'official' copyrighted works can be extended by way of analogy: Martin Vogel, in Ulrich Loewenheim, Matthias Leistner and Ansgar Ohly (eds), *Urheberrecht: Kommentar* (6th edn, C.H. Beck 2020) Sec. 87b UrhG paras 67-68.

74 Former Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 on the re-use of public sector information [2003] OJ L 345/90.

75 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L172/56.

legal or policy interest in maximum dissemination does not exist, but instead access only seems reasonable in order to increase dynamic efficiency, can alternative access regimes, such as FRAND licences, be considered and will then have to fulfil the requirements provided for by the Open Data Directive.⁷⁶

This particularly problematic example points, secondly, to a more general problem. In fact, the narrow exceptions to the *sui generis* right should at the very least be aligned and dynamically linked with the exceptions to copyright law under the Information Society Directive.⁷⁷ It is therefore of considerable practical interest to enable and oblige Member States to extend, *mutatis mutandis*, the exceptions and limitations applying to works protected under copyright to *sui generis* protection of non-original databases.⁷⁸ The obligation should be phrased so as to establish a dynamic link between both fields, to the effect that limitations set out in new copyright legislation would automatically also become applicable, under suitable terms and circumstances, to the *sui generis* right. The new copyright provisions for text and data mining and certain other exempted uses in Articles 3–6 and 8 DSM Directive are examples in point: Rightly, they explicitly extend the scope of the newly proposed exceptions to the database maker's *sui generis* right. However, the problem is of a more general nature and should be solved in a general way when revising the Database Directive by simply mandatorily aligning the exceptions to the *sui generis* right with the general exceptions to EU copyright law.

In this context, it should also be clarified that permitted use under the exceptions also covers use acts in respect of complete databases. This is because the current wording of Article 9 Database Directive seems to suggest that even exempted acts must be limited to the use of substantial parts. However, a limitation of the exempted uses to the use of only substantial parts of a database could hardly be accommodated with the access needs of competitors and new market entrants in the context of big data activities. Moreover, the limitation of the personal scope of application of the exceptions to 'lawful users of a database' should be abolished. This qualification is inconsistent with the system of general copyright law exceptions which do not contain an additional legitimacy test since the considerations on whether the use is legitimate are already embedded in the very definition

76 See Open Data Directive (n. 75). See Richter (n. 13) in regard to the German E-Government Act of 2017.

77 Kur and others (n. 72) 556–557.

78 Leistner as reported in Bently and others (n. 18) 16; Drexler (n. 11) 81.

of the scope of the exceptions as such. Therefore, an additional condition of lawful use is systematically inconsistent and unnecessarily endangers the practical utility of the rules on exceptions.

Finally, the strict limitation of the exceptions to non-commercial uses certainly has to be put under scrutiny. This is a more general problem of certain exceptions in EU copyright law, which will have to be discussed generally in future, in particular because it is also inherent to the exception for text and data mining under Articles 3 and 4 DSM Directive.⁷⁹ Also, as a more general and by no means new proposition, it should also be considered in future to make the optional exceptions and limitations in the Information Society Directive mandatory in nature.⁸⁰ Article 17(7) DSM Directive, with its somewhat arbitrary and therefore insufficient selection of certain now mandatory exceptions and its limited sector-specific scope, can only be a beginning in that regard.⁸¹

4. Summary

In sum, existing European copyright protection in the realm of database works and computer programs does not raise any imminent concern with regard to the balanced and efficient development of the data economy and currently does not need to be immediately revised in this context. However, the hitherto insufficient new exception for text and data mining is a case for (another) revision at least in the middle term.

By contrast, depending on the development of future case law in the area, the database *sui generis* protection right in its current state has the undeniable potential to substantially aggravate the existing and acknowledged access problems which already follow from factual control over different data sources.⁸² Even in areas where it is currently unclear whether the right will develop significant dysfunctional impact, the resulting legal uncertainty is problematic in itself as it can have a chilling effect on certain

⁷⁹ Cf. section C.II.C.2. above.

⁸⁰ Leistner (n. 19) 47–48; Drexl (n. 11) 81.

⁸¹ Matthias Leistner, ‘European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge?’ (2020) 12 *Zeitschrift für Geistiges Eigentum* 121.

⁸² Cf. Drexl and others (n. 2) 1-2.; Communication of the European Commission of 10 January 2017 – ‘Building the European data economy’ COM(2017) 9 final, 9–10.

innovative commercial activities (e.g. the different meta-search platforms in the internet⁸³ and activities based on certain public sector information⁸⁴). At the same time, the right tends to miss the opportunity to address certain very well defined and targeted protection needs, in particular for high-quality training data, if these needs could in fact be validated beyond the realm of (very limited) copyright protection in the area). The existing database sui generis regime is thus in need of rigorous reform.

III. Trade secrets protection: A defensive, more flexible hybrid regime which is better equipped for the data economy

Trade Secrets Protection in Europe has recently been harmonised in the Trade Secrets Directive of 2016⁸⁵ which has been implemented in Germany in the entirely new Trade Secrets Act.⁸⁶ Similarly, the U.S. have recently consolidated legislation on trade secrets protection on the federal level in the Defend Trade Secrets Act of 2016.⁸⁷

Trade secrets protection, as a hybrid regime,⁸⁸ does not constitute property rights in rem, but instead only complements and intensifies de facto exclusivity because of secrecy.⁸⁹ Accordingly, it does not vest an exclusive right in the person of the trade secret holder but instead only provides for 'defensive' remedies against certain prohibited acts of misappropriation by third parties.⁹⁰ Far from being a disadvantage, the flexible hybrid character of trade secrets protection, which establishes a limited inter omnes effect by way of defensive remedies which can be invoked against acquirers of data and other third persons only under certain conditions and will then be

83 See section C.II.3.b) above.

84 See section C.II.3.c) above.

85 Trade Secrets Directive (n. 47).

86 Trade Secrets Act (*Gesetz zum Schutz von Geschäftsgeheimnissen*) [2019] Bundesgesetzblatt I 466.

87 Defend Trade Secrets Act of 2016 Publ L 114–153.

88 Cf. Ansgar Ohly, 'Germany: The Trade Secrets Protection Act of 2019' in Jens Schovsbo, Timo Minssen and Thomas Riis (eds), *The Harmonization and Protection of Trade Secrets in the EU – An Appraisal of the EU Directive* (Edward Elgar 2020, forthcoming).

89 Herbert Zech, 'Information as Property' (2015) 6 Journal of Intellectual Property, Information Technology and E-Commerce Law 192, para. 26.

90 Tanya 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* (Nomos 2018) 59, 70.

specified in enforcement in a very flexible and proportional way, seems to be particularly well suited to serve the purposes of the data economy.⁹¹

On principle, while a single datum will typically not qualify as a trade secret, datasets⁹² and data analysis techniques of even mere potential commercial value can qualify for trade secrets protection on condition that they are kept secret, i.e. not generally known in the relevant circles,⁹³ and that reasonable steps have been taken to maintain secrecy (Article 2(1) Trade Secrets Directive).⁹⁴ This latter condition, which is modelled on the comparable requirement in Article 39 TRIPS, should be interpreted in a rather flexible, broad way, because it is in certain tension with the general objective of trade secrets protection to save transaction costs for factual protection measures⁹⁵ and it might unnecessarily disincentivise limited disclosure of trade secrets in protected environments, which is important for the optimal development of data pools in the data economy.

An essential problem of the EU Trade Secrets Protection Regime as a tool in the data economy is the comparatively vague definition of the rightholder in regard to trade secrets (Article 2(2) Trade Secrets Directive).⁹⁶ In fact, not only in common data pools, but also in the realm of connected devices and all kinds of data-related networks, it will often be very difficult or even impossible to identify the person or persons who lawfully control the respective trade secrets. This is a problem common to any attempt to regulate the data economy on the basis of instruments which entail property-right elements and therefore need a uniform, clear and unambiguous allocation. By contrast, it is characteristic for the input to and use of data in common datapools and data-related networks that a clear allocation of rights to specific parts of the pool will often simply no longer be possible. In that regard, clearly, only contracts and, consequently, best

91 Josef Drexler, 'Designing Competitive Markets for Industrial Data – Between Propertization and Access' (2016) Max Planck Institute for Innovation and Competition Research Paper No. 16–13, 24 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2862975>; Aplin (n. 90) 70.

92 See explicitly European Commission Staff Working Document, 'On the free flow of data and emerging issues of the European data economy – Accompanying the document Communication Building a European data economy' SWD(2017) 2 final, 20. See further on the requirements and differentiations in this field Schweitzer (n. 4) 571.

93 Aplin (n. 90) 65–66.

94 Ibid.

95 See already Mark A. Lemley, 'The Surprising Virtues of Treating Trade Secrets as IP Rights' (2008) 61 Stanford Law Review 311, 348–350 (on Art. 39 TRIPS).

96 Aplin (n. 90) 69.

practices guidance or even non-mandatory default rules in contract law will be able to solve the problems related to allocating ownership shares and – since precise ownership allocation will often no longer be possible in a reasonable way, even more importantly – the mutual relations of numerous co-owners to each other and to outsiders. However, the Trade Secrets Directive does not contain any provisions on licensing or other contracts in the field of trade secrets ownership and use, which is – arguably – its main shortcoming for the purposes of the data economy. It is submitted that the ongoing initiative of the Commission to establish best practices with regard to contractual allocation of rights to data in common data pools⁹⁷ is of essential importance in that respect and that the efforts in this sector should even be intensified.

As for the scope of protection, the Trade Secrets Directive generally has model character as a modern, balanced and proportional protection regime. First, it establishes certain lawful acts, most importantly for the data economy, comprising independent discovery or creation and, particularly, reverse engineering (Article 3 Trade Secrets Directive).⁹⁸ Only secondly does it define the unlawful acts and effectively provide for mere intensified tort remedies against certain specific acts of misappropriation (Article 4). Thirdly, it provides for a number of exceptions including a catch-all clause for any ‘legitimate interest recognised by Union or national law’ (Article 5). Finally, the Trade Secrets Directive’s provisions on enforcement (Articles 6–15), in particular on injunctions, contain numerous qualifications and flexibilities which, if applied correctly and with caution by the courts, will ideally allow enforcement to be flexibly adjusted to the underlying, innovation-oriented goal of the protection regime. Although certain flexibilities in enforcement are clearly necessary and customary in this sector, given the broadly defined, particularly vague character of the protected subject matter, these modern provisions in the Trade Secrets Directive go further – and way beyond the balances and flexibilities in the older, more general Directive on the enforcement of intellectual property rights

97 See generally Communication from the Commission of 19 February 2020 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions – A European strategy for data, COM(2020) 66 final, 14.

98 Cf. also section B.III. above and further European Commission, ‘Towards a common European data space’ (n. 7) with European Commission SWD, ‘Guidance on sharing private sector data’ (n. 7).

of 2004.⁹⁹ They have genuine model character for a modern and balanced enforcement regime in the data economy.

Only a couple of points should be kept in mind in the current and future application of the new European trade secrets protection regime in order to streamline it for the purposes of the data economy. Thus, the provisions on lawful acts and on exceptions justly pay particular attention to certain public interest issues (in particular whistleblowing activities, protection of workers and employees etc.), while specific exceptions for the purpose of enhancing competition or for particular needs of the data economy are neither expressly stipulated nor considered. Also, the definition of prohibited acts goes particularly far in regard to the definition of infringing goods in Article 2(4) Trade Secrets Directive, which even comprises goods the marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed.¹⁰⁰ This goes even further than the protection for direct products of a patented procedure in patent law, which is problematic for the data economy in its own right, and might pose particular problems for some of the currently economically most important big data applications, as it might have chilling effects on certain marketing methods, based on large data pools, whenever the legal situation of all data in the pool cannot be completely cleared. In order to better accommodate these two problematic points with the needs of the data economy, the criterion of 'significant benefit' as well as the catch-all clause in the catalogue of exceptions should generally be interpreted with a particular view to the just objective to enhance competition and innovation – including by newcomers and with regard to follow-up innovation and innovation in unrelated markets.

In sum, it is submitted that the new EU trade secrets protection regime is rather well equipped to contribute a flexible protection instrument to the regulation of the data economy, justly targeted on confidential, non-disclosed information of at least potential commercial value. To fully exploit this potential, the numerous flexible open-ended provisions in the Trade Secrets Directive will have to be consistently interpreted with a view to enhancing competition and innovation, including follow-up innovation, in the concerned markets.

⁹⁹ Directive 2004/48/EC of the European Parliament and of the Council of 29.04.2004 on the enforcement of intellectual property rights [2004] *OJ L* 195/16.

¹⁰⁰ Aplin (n. 90) 70.

IV. *Access to data, sui generis database protection and trade secrets: The perspective of current and future access regimes*

1. *Basic consideration: Access to data and use of data*

The following part focuses on the more prospective question of how (the occasional current) and possible future access regimes for certain use scenarios can be accommodated to the sui generis right and what IP law can contribute to the specific shaping of such access regimes.

Initially, in the discussion of access rights and IP protection two different levels have to be distinguished. Access rights provide for an individual right to have data disclosed and might then also entail certain regulation of the conditions of further use of these data (protection of authenticity of data, reciprocal disclosure, use for free or against payment, details of portability, certain limitations of use etc.). IP protection, in particular protection under the database maker's sui generis right, mainly concerns the regulation of *use* of data, i.e. has an impact only on the second 'half' of such access regimes. Therefore, IP rights as such can hardly help to answer the question of when secret or other access-restricted data should be disclosed.¹⁰¹ In that regard, they are all but an additional barrier, such as the sui generis right or trade secrets protection. At best, they will expressly allow such disclosure, but as such (with very minor exceptions) they will never require it. By contrast, as far as the level of regulation of use of the accessed data is concerned, certain elements of IP rights, and even of the sui generis protection right, might be helpful to further structure the specific conditions in that regard.¹⁰²

2. *The basic case groups*

As for actual or potential access needs, as has been said before, it seems possible to roughly distinguish certain categories of access and use interests¹⁰³ where the database sui generis right will likely be affected. First, as has been described above, the limitation of the exclusive rights to use acts in respect of substantial parts of a database cannot effectively accommo-

101 See on that problem Bently and others (n. 18) 41–42.

102 Partly different Drexl (n. 11) 154–155; see further section D below.

103 Similarly Bently and others (n. 18) 39–40; Schweitzer (n. 4) 572 ff.; see also Drexl (n. 11) 81–82.

date the possible need for use of entire aggregated sets of machine- or sensor-generated use or other data which in certain situations might be necessary for third parties in order to develop, produce, market or distribute value-added or entirely new products or services or to compete in the primary market (case group 1). Secondly, even individual-level use data of single users will often add up to a substantial part of a protected database which is owned by the provider of the product or service, who observes and collects these data (case group 2). As has been shown, the *sui generis* right sits uncomfortably with the possible legitimate use interests in both these areas. Thirdly, *sui generis* data base protection already raises actual problems in its relationship to the European access regime in the field of public sector information (PSI) (case group 3). Case group 3 has been discussed already and a solution has been proposed.¹⁰⁴

As regards case group 1, the discussion meanwhile mainly centers on competition law-based compulsory licences¹⁰⁵ as well as on possible specific provisions for ‘IP-internal’ compulsory licences concerning access to so-called sole-source data in the context of the *sui generis* protection right.¹⁰⁶ In the case of the *sui generis* right such ‘IP-internal’ provisions on compulsory licences in certain well-defined cases should indeed be considered (see further below at D.). Also, Article 6(1) lit. h) and lit. i) of the newly proposed Digital Markets Act on access and data portability for business or end users of gatekeeper-platforms will be helpful in that regard, although the scope of these provisions is limited to certain very large gatekeeper-platforms (as defined in Article 3 of the proposed DMA). Significantly, these provisions do not specifically regulate the relationship with possibly existing IP-protection. This somewhat fits into the general character of the proposed DMA, which as a measure of sector-specific regulation, focuses on further specification and enforcement by the Commission. However, the problems concerning data access and portability go beyond the limited realm of gatekeeper platforms and can probably only be solved on the basis of individual access and portability rights encompassing further specification and remedies in private law. Therefore, the following considerations of the relationship of such future access rights to existing IP protection and of the accommodation of both regulatory systems in the context of private access and portability rights are of particular importance also for a reasonable and workably specification of these new instruments through

104 See section C.II.3c).

105 Schweitzer (n. 4) 576–580.

106 Drexl (n. 11) 81–83.

the Commission (in particular concerning the actual scope and conditions of access, portability and subsequent use).

Concerning case group 2 (see further below at 3.b)(2)), the structural analysis of individual customers' potential needs to access and port their individual-level data to other providers has recently been further developed and generalised for connected devices in a study by Drexl.¹⁰⁷ Drexl's approach is expressly based on future sector-specific access rights. That means that, on the basis of the distinction established in the preceding part, it focuses on both access to/disclosure of data and use of data. In this context, it seems systematically consistent that the study regards such access rights as independent of the legal status of the concerned data, in particular possible IP protection for the concrete form in which these data are collected and stored, and instead proposes sector-specific access regimes which 'should prevail over any sui generis database right'.¹⁰⁸ The details concerning such data access and use should instead be regulated in the context of these sector-specific access regimes themselves, including the question of whether and in which cases such use should be remunerated. In particular, concerning the question of remuneration, the study argues against the background of balanced economic incentives, which should not go beyond what is necessary to sufficiently incentivise the creation of databases in certain situations. Consequently, e.g. in regard to sensor-produced data and in particular concerning smart devices, the study rightly raises the fundamental question of whether remuneration will be needed at all where data access is necessary and justified.¹⁰⁹

From Drexl's viewpoint, the Database Directive and EU IP instruments in general only need to be complemented with what we would call a passive 'interface provision', i.e. a general exception which clarifies that IP protection 'does not apply where, and to the extent to which' sector-specific regulations require access to data.¹¹⁰ However, the devil of this approach of course is in the details as it begs the question of how use of such data should be regulated in detail in the different future cases and whether certain basic case groups can already be distinguished in this regard. In fact, while the approach seems systematically consistent and deserves approval as far as access as such is concerned, in regard to subsequent (commercial) use of the accessed and ported data, any such access regime will need fur-

107 Ibid.

108 Ibid 82.

109 Ibid 82.

110 Ibid 83.

ther refinement of the conditions for and scope of such use anyway. And in that regard, its accommodation to existing IP protection from this author's viewpoint can hardly be entirely ignored, since the existing IP protection rights, including the *sui generis* right for databases, already contain certain (more or less conclusive) assumptions of the legislature on the need and tailoring of incentives for innovation in certain specifically defined fields. On the contrary, from this author's viewpoint, certain elements of the existing EU IP regime can even provide structural guidance for the further regulation of data *use* in the context of different access scenarios (see further below 3 and D). Similarly, with regard to Article 6 (1) lit. (h) and (i) of the proposed DMA, both the specification by the Commission as well as a system of functional private remedies devised to enforce these duties of gatekeeper platforms should certainly be inspired by and accommodated with certain principles and experiences concerning the regulation of access in the existing IP regime in order to make them work effectively in practice.

Now how should these two very basic cases (individual access to and portability of customer data *inter alia* to prevent lock-in; general access to complete databases by competitors or businesses to enable workable competition) be treated from the viewpoint of IP and in particular from the viewpoint of the *sui generis* right concerning the *use* of such data?

3. Details of the interface with IP protection, in particular sui generis protection

a) Cases that should be excluded from protection

From the viewpoint of *sui generis* protection, in certain cases the general incentives rationale behind the *sui generis* right might indeed be fundamentally flawed from the outset, if at a closer look incentives are typically not at all necessary in order to foster dynamic competition. As for the protection conditions of *sui generis* protection, the crucial question is whether these cases can be structured and described in a sufficiently abstract and stable way, i.e. in clearly identifiable case groups that are independent of specific market conditions and can therefore be generalised. If this is the case, from a contextual point of view, respective investments should not be covered by the *sui generis* right in the first place. Instead, investments in such cases should be excluded from the protectable subject matter as such and consequently should not qualify as relevant for *sui generis* protection. Actually, the *British Horseracing Board* case, which concerned a typical spin-off situation in which the relevant databases resulted from another (main)

commercial activity and an additional protection of the investment to create the database was therefore obviously not necessary, is a case in point.¹¹¹ This is another reason why generation of data, if it is not based on observation or measurement of available outside factors and if the structuring of the information does not reach the outstanding level of creativity required for copyright protection in Europe, should remain excluded from the protectable subject matter of the *sui generis* right. This should be expressly clarified and specified in the Directive. Further case groups should and can be developed.¹¹² Such cases should be carved out in the application of the condition of protection¹¹³ and *sui generis* protection should be denied from the start.

- b) Cases where the incentive rationale of the *sui generis* protection right has to be taken into account, but has to be balanced with a specific access and use interest

(1) Overriding interest in access and use

By contrast, in cases where relevant investments are protected by the *sui generis* regime because incentives generally seem necessary and at least on principle justifiable to foster the creation and structured dissemination of databases, as a starting point, the express will of the legislature of the Database Directive, that use of the protected databases should generally not be for free, has to be accepted.

However, this legislative balancing of interests is not necessarily conclusive in regard to recent technological developments and certain specific, newly emerging access and use interests. Therefore, there might be cases in which the basic balancing of rights and interests (and between static efficiency (access) and dynamic efficiency (incentives)), indeed needs to be overridden beyond the limited possibilities of competition law. Generally, these cases will require the most thorough and specific analysis in particular with regard to the question on which conditions use of the data should be granted. In that regard, in an untechnical way, the existing EU IP regime might provide for some structural guideposts.

111 Case C-203/02 *British Horseracing Board* ECLI:EU:C:2004:695 (n. 68).

112 See further section C.II.3.c) above and more comprehensively section C.IV.3.b) below.

113 See section C.II.3.a) above.

(2) Access rights for individual ‘lawful customers’ with regard to sensor-produced data of smart devices

This is because, naturally, not only for the interface of IP and competition law, but also with a view to the ‘IP-internal’ structures, these are not entirely new questions. Hence, it is not surprising that existing ‘anchors’ in EU IT-related copyright law and in the provisions on the sui generis right can already be identified for both case groups, which characterise the current access discussion.¹¹⁴

Case group 2, concerning individual customer access, use and portability (namely transfer of the received data to different providers) in the realm of smart devices, sensor-produced data etc., is systematically related to the copyright concept of the so-called lawful user in both the Computer Programs¹¹⁵ and the Database Directive. Accordingly, the Database Directive contains a provision on mandatory core minimum rights of lawful users of databases which cannot be overridden by contract (Arts 8(1) and 15 Database Directive). Under a broader perspective, another example in the wider context of such mandatory minimum rights of customers outside IP law is Article 16(4) Digital Content Directive,¹¹⁶ which in turn was modelled on Article 20 GDPR.

In fact, this regulatory technique already partly used in European copyright law, i.e. the provision of certain mandatory minimum rights of legitimate users, has the potential to substantially streamline the function of IP rights in online networks. This is because legally, these minimum rights ‘travel’ with the legitimate user, who may perform certain minimum acts deemed necessary to effectively use the respective databases.¹¹⁷ It is this very mechanism that could easily be extended to cover access to data and use rights concerning the transfer to other providers for lawful users of smart devices and machinery which produce sensor-generated sui generis

114 As for the third relevant case group, data generated by public bodies, see C.II.3.c) above.

115 See Art. 5 Computer Programs Directive (n. 23).

116 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

117 See fundamentally case C-128/11 *UsedSoft* ECLI:EU:C:2012:407. Although, in case C-263/18 *Nederlands Uitgeversverbond v Tom Kabinet* ECLI:EU:C:2019:1111, the CJEU refused to generalise the *UsedSoft* doctrine for all categories of copyright-protected works under the InfoSoc Directive, it might still be extended to the area of databases where minimum rights of lawful users are expressly provided for in the Database Directive for both copyright and the sui generis right.

protectable data. Typically, for such use no additional remuneration should be set out since the database producer can factor the associated costs into the conditions of the underlying sales or service contract. Accordingly, the EU copyright framework also regards such rights as part of the contractual consideration and does not provide for additional remuneration claims. The provisions on the minimum rights of lawful users therefore offer the ideal functional context to implement possible sector-specific individual customer access and porting rights in the area of smart devices etc. where these are deemed necessary and where they will be possibly provided in sector-specific regulation in the future. Of course, the main challenge for such sector-specific regulation is to make access and use rights of individual customers functional in practice. In that regard, the model of Article 20 GDPR should be closely followed and IP law should contribute to functional, accessible infrastructures by safeguarding free access to APIs, data formats and other comparable infrastructural technical elements in order not to put additional legal trammels on the at least conceivable future development of tools and service providers for possible real-time porting of specific use data.¹¹⁸

The most intriguing question in this regard, which has also in the past been the subject of intense debate in copyright law,¹¹⁹ is to what extent such rights of lawful users should indeed have mandatory character.¹²⁰ This question is not easy to answer in a generalised way, as it depends on the degree of connection between the product or service and the data market and the information of the customer on the resulting dangers of lock-in or leveraging in a given product or service market. An initial consideration might be to provide for mandatory access and portability rights of private users, while access and portability rights of commercial users could be designed as mere non-mandatory default rules. But this bright-line distinction might miss the point in future multipolar data markets, as the example of certain small-scale business customers, such as Uber drivers, shows.

118 See also section B. above. See further in regard to open standards, formats etc. Furman and others (n. 4) 64–74.

119 Cf. for the broad discussion on the dogmatic nature of the provision and the scope of the so-called mandatory core of Art. 5 Computer Programs Directive (n. 23) (and its counterpart in Sec. 69d German Copyright Act) the references in Gerald Spindler, in Ulrich Loewenheim, Matthias Leistner and Ansgar Ohly (eds), *Urheberrecht: Kommentar* (6th edn, C.H. Beck 2020) Sec. 69d paras 1 and 13–14.

120 Schweitzer (n. 4) 575: non-mandatory; Drexler (n. 11) 154, 156: mandatory, at least in regard to consumers. Furman and others (n. 4) 10 seems to be generally sceptical about far-reaching mandatory solutions.

Ultimately, the justification to provide for such access and portability rights in a mandatory way will depend on the concrete market structure and empirical proof of information asymmetries on the side of the customers in specific sectors. If these conditions are fulfilled, admittedly, implementing possible access rights as mandatory minimum rights of the lawful user in this context still results in a certain cross-subsidisation of users who rely on these rights and actively use them to switch their providers, at the expense of less active users who do not use this option. This is because such access and portability rights will generally raise the cost of the provider, which no longer has the possibility to contractually bind certain customers on the basis of control over aggregated individual-level customer data in a closer way and therefore loses possibilities for price discrimination. However, in sectors in which such regulation seems necessary and proportionate to prevent existing or likely concrete lock-in problems, this very effect might be desirable. After all, it would enable and enhance competition in the interest of all customers by nuancedly subsidising the more active customers in their switching endeavours.

Future reform of the Database Directive should keep this overall context in mind. Further details, such as a possible definition of the minimum (mandatory or mere default) use rights and their ‘portability’ should be regulated in future sector-specific access regulation, where and as far as this is reasonable and necessary. At the ‘receiving’ end, the current *sui generis* regime is not at all complete, but at least initially prepared in its basic structures: In future, the dogmatic category of the minimum rights of the lawful user could be extended to cover use in such cases referring to the different sector-specific access regulations. For the moment, the limitation of the rights of the lawful user of a database to extract and re-utilise only insubstantial parts of a database should be eliminated; instead, the lawful user should be able to perform the necessary use acts also in regard to substantial parts of or complete databases.

(3) Access and use rights for competitors: compulsory licences in the specific context of the *sui generis* right and of trade secrets protection

Access and use rights in regard to entire aggregated datasets and corresponding use rights for competitors or other businesses in order to enhance competition in the area of sole-source data follow different principles. Typically, such use should be remunerated as it seems that the incentives rationale behind the *sui generis* right will generally be intact in such

cases, whereas it is only a specific market situation which requires that the property rule be turned into a liability rule.¹²¹

In fact, specific compulsory licensing provisions have been considered since the very beginning of policy discussions about a possible need for database *sui generis* protection in the 1990s.¹²² In that regard, it is of particular interest that an earlier Proposal for the Database Directive explicitly included provisions on compulsory licences.¹²³ Article 8 of the Proposal provided for a compulsory licence on ‘fair and non-discriminatory’ terms for publicly available sole-source databases as well as for publicly available databases compiled by public bodies.

Meanwhile, the existing case law and practice even more clearly suggest that competition law-based compulsory licences will simply often come too late in the typically very dynamic markets for data-based products or services.¹²⁴ Therefore, it seems that specific provisions on compulsory licences in the Database Directive can at least be useful in cases in which the mere generation/collection distinction fails to pro-actively prevent *sole-source situations*, e.g. because ‘collected’ databases develop into an industry standard, independent obtainment becomes impossible because of ex post network effects or subsequent public regulation etc.¹²⁵ Hence, at least a compulsory licensing provision for sole-source databases should be added in the Database Directive. Whether additional cases are conceivable in the wake of big data and the multipolar data economy remains to be seen and should be left to sector-specific analysis and regulation.

As regards the sole-source criterion, the definition of indispensability should follow the CJEU’s definition in *Bronner* (concerning a physical newspaper distribution scheme). Hence, a successful claim to a compulsory licence should require that the creation of a comparable database not be viable under reasonable economic conditions for a competitor of compara-

121 Cf. also Leistner (n. 19) 42–46.

122 Jane C. Ginsburg, ‘Creation and Commercial Value: Copyright Protection of Works of Information’ (1990) 90 Columbia Law Review 1865.

123 Art. 8 Proposal for a Council Directive on the legal protection of databases, COM(1992) 24 final. See further Bently and others (n. 18) 36–37, with further references.

124 Drexl (n. 91) 42–44; Josef Drexl and others, ‘Position Statement of the Max Planck Institute for Innovation and Competition on exclusive and access rights of 16 August 2016’ (2016) 11–13 <www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI-Stellungnahme_Daten_2016_08_16_final.pdf> accessed 31 August 2020.

125 Cf. on possible reasons and case groups for compulsory licences Bently and others (n. 18) 39–43 (albeit with a more open conclusion).

ble size and resources as the original database maker.¹²⁶ Moreover, access to the data would have to be indispensable for access to a downstream market in relation to the (hypothetical) upstream licensing market for the data. It has to be noted that, according to the CJEU's *IMS Health* judgment, this so-called downstream market can also be the market where the database maker already offers its own products or services to customers, since the (hypothetical) upstream market would be the (hypothetical) licensing market in such cases, regardless of whether the database maker grants licences to third parties in that market at all.¹²⁷ By contrast, the additional criteria from general competition law for compulsory licences (in particular, prevention of the offer of a new product or service) should not apply in case of *sui generis* protection of sole-source databases.¹²⁸ The enhancement of competition in the product or service market or in a downstream, complementary or entirely new market as such should suffice to justify the compulsory licence.¹²⁹

Remuneration should be set on fair and non-discriminatory terms.¹³⁰ Depending on the circumstances of the case, this might also result in free use of data where parties might reasonably have negotiated a zero licence fee. In the broader context of the discussion to turn the *sui generis* right into a registered industrial property right,¹³¹ one might consider making the EUIPO responsible for the granting of such compulsory licences for use in the EU market.¹³² In that context an arbitration mechanism and, ultimately, an appeal to the General Court should be provided for in order to set the conditions of such compulsory licences.

An intriguing question, and one that has also been recently asked by Schweitzer, is whether such compulsory licences should generally only be granted on the condition of reciprocity, i.e. the granting of a cross-licence by the licence seeker.¹³³ Patent law has chosen this solution in Article 31(1) (ii) TRIPS (see also Sec. 24(2) German Patent Act). Also, the usual FRAND and RAND declarations in the context of standard-essential patents offer the SEP holder the option of granting a FRAND licence only on the condi-

126 Cf. Case C-7/97 *Bronner* ECLI:EU:C:1998:569, paras 46–47.

127 Cf. Case C-418/01 *IMS Health* ECLI:EU:C:2004:257.

128 Similarly Schweitzer (n. 4) 578.

129 See already Leistner (n. 45) 150–151; critically Drexl (n. 91) 52.

130 Cf. also Drexl (n. 11) 82.

131 Cf. Leistner (n. 19) 49–50, 56; Leistner as reported by Bently and others (n. 18) 65, 84.

132 Cf. Bently and others (n. 18) 42–43.

133 Cf. Schweitzer (n. 4) 579.

tion of reciprocity.¹³⁴ Nonetheless, it seems that the specific situation concerning the database sui generis right is of a slightly different nature. Whereas patents vest a genuine exclusive use right in the person of the rightholder, the sui generis protection right only protects the investment in the collection and presentation of the contents of a database and, as such, does not always exclude independent creation of a comparable or better database. Accordingly, there might be cases in which a mandatory condition of cross-licensing would not necessarily yield the efficient result, such as if a very small, innovative market entrant, under the reciprocity condition, had to grant access to data the incumbent could easily acquire independently. All in all, it might be the best solution to expressly state the possibility that FRAND conditions might comprise a cross-licensing duty on the implementer, but should leave it to the competent authority and, ultimately, to the courts to decide whether such a reciprocity condition is a part of reasonable and non-discriminatory licensing conditions on the facts of a given case.

Compulsory licences under the proposed mechanism on principle¹³⁵ should also extend to non-published databases, i.e. should take the form of genuine rights to access and disclosure, where this is needed to enable workable competition.¹³⁶ Naturally, this raises intricate issues of third-party rights and interests, in particular concerning privacy protection, protection of personal data and confidentiality in regard to natural persons, but also in regard to businesses whose data are stored in such sole-source databases.¹³⁷ Remarkably, even the original Proposal of the Commission, which still envisaged compulsory licences only for published databases, already dealt with the relationship to other legislation concerning privacy, protection of personal data and confidentiality. As for protection of personal data, today it follows mandatorily from the GDPR that respective information duties in relation to and a veto right of affected individual persons must be provided for in cases of upstream compulsory licensing when a business that has stored data relating to these natural persons is con-

134 See, for example, ETSI IPR Policy para 6.1 <www.etsi.org/images/files/IPR/etsi-ipr-policy.pdf> accessed 31 August 2020.

135 But see immediately below on necessary differentiation for databases which are additionally protected as a trade secret, which will often be the case.

136 Still differently and limiting compulsory licences to published databases Ginsburg (n. 122) 1929; Art. 8 of the original Commission's Proposal for the Database Directive (n. 123).

137 Cf., for example, Drexl and others (n. 2) 18-19; Bently and others (n. 18) 42 and Drexl (n. 11) 82.

cerned. At first sight, this might seem like a considerable practical trammel on compulsory licensing. On the other hand, customers would probably rather seldom veto such compulsory licences if they allowed for the offer of new or more efficient products or services. Also, if only individual customers vetoed such licensing this would not entirely devalue the utility of the remaining parts of the database, subject to compulsory licensing.

As for trade secrets it seems that if trade secrets are concerned, compulsory licences should only be granted under the additional circumstances of the CJEU's *IMS Health* decision¹³⁸ and the General Court's *Microsoft* ruling.¹³⁹ Accordingly, in these cases compulsory licences would require that access to the data in question be indispensable to offer a new product or service¹⁴⁰ in a downstream market in relation to the (hypothetical) licensing market and that the denial of access would effectively foreclose workable competition on that market. However, this qualification would not have to be implemented in the new compulsory licensing provision in the Database Directive, as it self-evidently follows from the independent nature of trade secrets protection, which would as such not be affected by a compulsory licensing provision for the database sui generis protection right.

Whether further conditions or qualifications would be needed should be a matter for future research.¹⁴¹ This might concern issues such as additional guideposts for the specification of FRAND terms in certain cases as well as procedural backing for the process of specifying FRAND terms, such as possible specific rights to information and other procedural rules.

D. Selected elements of IP rights as building blocks for the regulation of future data markets

Finally, apart from the targeted access-oriented perspective, under which IP rights will typically be observed as a 'negative' possible barrier to access, one might also ask which elements of IP rights might indeed be particu-

138 Case C-418/01 *IMS Health* ECLI:EU:C:2004:257.

139 Case T-201/04 R *Microsoft v Commission* ECLI:EU:T:2004:372 and Case T-201/04 *Microsoft v Commission* ECLI:EU:T:2007:289.

140 But see already B.III. above on the meanwhile very low requirements for a 'new' product or service in this sense.

141 See from the more recent literature comprehensively on compulsory licensing Reto M. Hilty and others (eds), *Compulsory Licensing – Practical experiences and ways forward* (Springer 2015).

larly helpful in building the future legal infrastructure for data markets. Under this ‘positive’ perspective, a couple of general ideas come to mind where elements of existing IP rights might serve as guideposts or building blocks for the solution of certain recurring problems in the discussion on the legal infrastructure for the data economy.

First, as data markets are currently mainly regulated by contracts, even more complex forms of multipolar, multi-purpose data biotopes develop, mainly on the basis of networks of bilateral or multilateral agreements with mere inter partes effects. It is characteristic of the discussion on the future regulation in this sector that at least in regard to certain aspects of regulation (data access, authenticity of data, control over specific data sets, conditions of use by third parties) a significant need for a *flexible inter omnes effect* of such contracts is felt. Recently, the Data Ethics Commission has proposed the provision of a limited inter omnes effect of data-related contractual agreements roughly modelled on Article 4(4) Trade Secrets Directive.¹⁴² The same general idea, albeit in a different context and much more limited way, has recently been followed in Japan, where the revision of the Japanese Unfair Competition Prevention Act provides for new protection of certain non-secret but ‘managed’ limited-access data against misappropriation (wrongful acquisition or improper disclosure) and extends this to the use of such data with the knowledge that it was wrongfully acquired.¹⁴³ These flexible approaches deserve attention. Indeed, if a need for additional inter omnes regulation (beyond contract law and the effects of contract-based networks) could be concretely proven in certain sectors or with regard to certain rights and interests, concepts and elements from trade secrets law with its rather flexible set of substantive and enforcement provisions would be certainly better equipped to accommodate such regulation needs than any property rights-based regime.¹⁴⁴ Nonetheless, whether such regulation is required at all in certain sectors remains to be seen. Any additional layer of regulation inevitably adds transaction costs, including information costs, trade secrets protection itself being an example in point.¹⁴⁵ As for the inter omnes effect of FRAND licensing declarations, patent practice is just in the process of developing appropriate in-

142 Opinion of the Data Ethics Commission (n. 11) 22, 144, 155.

143 See further Art. 2(7) and Art. 2(xi) et seq. Japanese Unfair Competition Prevention Act.

144 Aplin (n. 90) 59.

145 See on the problems concerning the identification of ownership and even the identification of the exact protected subject matter Aplin (n. 90) 59 and section C.III. above.

struments on the basis of the *existing law*. From this author's viewpoint, this latter development in case law should rightly be based on both contract law and competition law, without a current pressing need for new legislation.¹⁴⁶

Second, protection of personal data under the GDPR puts considerable trammels on the development of data biotopes, based on networks of contracts, whenever personal data of third parties (consumers or customers) are concerned.¹⁴⁷ In fact, the increasing commodification of data and the development of data related contracts are hampered in this field by the very strict requirements for informed consent laid down in the GDPR as well as by the general principle, underlying the GDPR, that such consent can be freely withdrawn anytime (Article 7(3) GDPR). Accordingly, the interface between new data-related approaches in contract law, such as the new Digital Content Directive,¹⁴⁸ and the comparatively strict requirements of the GDPR raises many questions.¹⁴⁹

In this respect, it has to be noted that German and continental European copyright laws have for decades had to grapple with similar problems concerning the personality-rights core of copyright and have developed contractual and statutory instruments to bridge the gap. Thus, to mention just one example, copyright law (see Section 42 German Copyright Act) does indeed allow the withdrawal of commercial use rights because of a changed personal attitude towards the work, but subjects this right of the licensor to qualifications and a duty to compensate the licensee for her resulting frustrated expenses. Another, similar instrument for the accommodation of contractual obligations on one hand, and the inalienable moral rights of the author on the other, can be found in Section 41 German Copyright Act. In general, it seems that some highly developed ideas on

146 See section B.II.B.1. above.

147 Schweitzer (n. 4) 573–574; Cr  mer, de Montjoye and Schweitzer (n. 4) 73–87; Schweitzer and Peitz (n. 4) 276–278; Kerber (n. 4) 644–646.

148 Digital Content and Digital Services Directive (n. 116).

149 Axel Metzger and others, 'Data-Related Aspects of the Digital Content Directive' (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 90; Axel Metzger, 'A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?* (forthcoming); Gerald Spindler and Karin Sein, 'Die Richtlinie   ber Vertr  ge   ber digitale Inhalte' (2019) Multimedia und Recht 415 and 488; Andreas Sattler, 'Neues EU-Vertragsrecht f  r digitale G  ter – Die Richtlinie (EU) 2019/770 als Herausforderung f  r das Schuld-, Urheber- und Datenschutzrecht' (2020) Computer und Recht 145.

contracts concerning personality rights can be found in copyright law.¹⁵⁰ However, to effectively make use of these approaches in the data economy, it seems that changes to the GDPR will hardly be avoidable in future.

E. Conclusion

The existing EU IP rights system is in reasonably good shape as regards its balanced approach to the protection of APIs, data formats and other more technical infrastructure, which should be open and accessible in order to enable and enhance data portability including future real-time data portability. Only details should be adjusted in this respect. In patent law, compressed or formatted data sequences should not be protected as a direct product of patented data compression or other processes. Minor adjustments are also necessary in regard to the relationship of the respective provisions of the Computer Program Directive and the Trade Secrets Directive on decompilation and reverse engineering. Both problems can be solved in case law. An imminent need for legislative activity cannot be identified in this sector.

As regards the accommodation of the different existing and proposed future access and use regimes for the data economy, the picture is slightly different. Again, European copyright law in the strict sense currently poses almost no significant problems for the development of the data economy. Only the hitherto insufficient new exception for text and data mining is a case for (another) revision at least in the middle term. By contrast, the database *sui generis* right is in immediate need of reform. Concrete reform proposals have been made in this paper, namely clarifications concerning the substantive condition of protection, new compulsory licensing provisions for sole-source databases and many others.

By contrast, EU trade secrets protection, which has been recently harmonised in the Trade Secrets Directive of 2016, is a modern and remarkably balanced protection regime comprising numerous open-ended terms which provide for necessary flexibility on all levels of substantive law and enforcement. With its hybrid character as a mere protection against misappropriation with certain flexible and qualified – in result only very limited – property rights elements, and with its focus on the protection of confi-

150 Axel Metzger, 'Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform?' (2019) *JuristenZeitung* 577, 578.

dential, non-disclosed information, it seems particularly well equipped to serve the regulation needs of the data economy. Only minor details will have to be adjusted in the future, and this can be achieved by construing the many open-ended terms and concepts in the Directive with a view to reducing unnecessary barriers to market entry and enhancing workable competition.

Finally, the IP system can contribute certain building blocks and experience to the overall discussion on a balanced and workable regulation of the data economy. Namely, existing experience and instruments in copyright law concerning the accommodation of the protection of personality rights on the one hand, and the commodification of such rights through contracts on the other, as well as existing specific remedies in trade secrets law, based in contractual agreements, but with a limited *inter omnes* effect, could be particularly helpful in drafting a future regulation of the data economy. Such elements, in a generalised form, could be useful parts of a future, balanced regulation which, from this author's viewpoint, should be based mainly on the further development of contract law and competition law.

