Owning Data via Intellectual Property Rights: : Reality or Chiemera?

Pihlajarinne, Taina Elisa

Kluwer Law International
2019-04-28

Pihlajarinne , T E & Ballardini , R M 2019 , Owning Data via Intellectual Property Rights: Reality or Chiemera? in R Ballardini , O Pitkänen & P Kuoppamäki (eds) , Regulating Industrial Internet through IPR, Data Protection and Competition Law . Kluwer Law International , Alphen aan den Rijn , pp. 115-133 .

http://hdl.handle.net/10138/312082

acceptedVersion

Chapter 9

Pihlajarinne, Taina – Ballardini, Rosa Maria

Owning Data via Intellectual Property Rights: Reality or Chimera?

§9.01 Introduction

Data, or information, is often referred to as 'the oil' of the digital era.[1] Despite the fact that this comparison is not very original, it is apt, since data has now become an essential asset for conducting business. Indeed, the data economy is reliant on the commercialisation of data. For example, data is essential for the digitisation of production (smart factories), for digitised products such as smart cars and smart wearables that can communicate with one another and the environment through the Industrial Internet and the Internet of Things, and for the development and use of smart systems like artificial intelligence (AI) programs. As such, it comes as no surprise that, in recent years, discussions about the regulation of data have increasingly caught the attention of academics, policy makers, and industry representatives. In the European Union (EU), the issue of regulating information has been considered by the Commission on many occasions, and has recently been on the political agenda as part of the Digital Single Market Policy.[2] The question is what kind of regulation is needed in order to make the data economy work.

Data can, with several caveats, largely be divided into the categories of personal and non-personal. This article focuses on the latter category. While the business models used by the major internet platforms of Web 2.0 and 3.0 were built mainly upon the use of personal data, soon the data economy will instead rely largely on non-personal (or industrial) data.[3] Non-personal data will be necessary not only for consumers to enjoy the benefits of the data economy, but also for many industries, as well as public authorities. In order for the complex framework of the data economy to function, it is essential to find a proper balance between controlling data and providing access to it.

Notwithstanding the importance of non-personal data to the data-driven economy, to date, the most important issues around its regulation (including issues relating to both control and access) remain either partially or completely unaddressed. Notably, issues of *protecting (ownership), accessing (access) and processing (trade)* data have been identified as the major challenges that could create barriers to the free flow of data, thus potentially hampering the

---

[1] Thomas Hoeren, *Big Data and the Ownership in Data: Recent Developments in Europe*, 36 EIPR 751 n.12 (2014); Christopher Rees, *Who Owns our Data?*, 30 Computer Law & Security Review 75 n.1 (2014); Robert A. Heverly, *The Information Semicommons*, 18 Berkeley Technology Law Journal 1128–1189 n.4 (2003).

[2] European Commission, *Digitizing European Industry: Reaping the Full Benefits of a Digital Single Market* (COM(2016)180 final); see also European Commission, *European Free Flow of Data Initiative Within the Digital Single Market*, Ec.europa.eu, http://www.europarl.europa.eu/news/en/headlines/economy/20180601STO04817/free-flow-of-data-enabling-the-digital-single-market (accessed 30th April 2019).

[3] Josef Drexl, 'The Future EU Legal Framework for the Digital Economy: A Competition-Based Response to the "Ownership and Access" Debate' in Sebastian Lohsse, Reiner Schulze & Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* 221-244 (2017), available at: https://doi.org/10.5771/9783845288185-221 (accessed 30th April 2019).

creation of a digital single market in the EU. However, while the Commission has clearly recognised the free flow of data as a prerequisite for an efficient data economy, there is as yet no coherent plan as to how this goal should be reached.

The principle of the free flow of data is closely connected to freedom of speech. For instance, Article 11 of the European Charter of Fundamental Rights explicitly mentions the freedom 'to receive and impart information'.[4] As the data economy has grown, several frameworks for fostering access to data have been presented in the scholarly literature.[5] In concrete terms, the EU has thus far only introduced a Regulation on the free flow of non-personal data in the European Union, which regulates some data storage and/or processing services and activities.[6]

This article contextualises the debate on the regulation of non-personal data in the context of data ownership via exclusive rights like intellectual property rights (IPR, IP). The paper focuses on the IPR regimes that are the most relevant to the protection of data, namely copyright, database rights, and soft IPRs such as trade secrets. Specifically, it aims at: 1) understanding whether the current IPR regime in the EU is applicable to the protection of data, 2) considering whether the current legal framework (including the recently proposed new legislation) fosters innovation in the data economy by striking an appropriate balance between controlling and providing access to data and, ultimately, 3) exploring more workable alternatives to current legislation. It concludes with a critique of the consequences of extending exclusive rights to data *per se*, as well as of the frequent tendency of the EU legislator to adopt related rights that are fragmentary and narrow in scope, without fully recognising their impact on the European copyright and IPR system as a whole. We argue that a better approach would be to strengthen the principle of the free flow of data (for instance, by embedding it as a core freedom in the EU internal market), thereby preventing the creation of any national measures hampering the free flow of data across the EU.

§9.02 What do we Mean by Data?

The starting point of this discussion relates to what is to be understood by the terms 'data' and 'information'. While there is a good explanation of the meaning of the term 'personal data' in EU law, there are no definitions of the terms 'non-personal data' or 'industrial data', nor of 'data' *per se*. According to the GDPR, personal data is information that refers to an

[4] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Framework for the Free Flow of Non-Personal Data in the European Union* (COM(2017)495), available at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data (accessed 30th April 2019).

[5] See, for instance, Herbert Zech, *A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data*, 11 Journal of Intellectual Property Law & Practice 468-470 n.6 (2016); Josef Drexl, Reto Hilty, Luc Desaunettes, Franziska Greiner, Daria Kim, Heiko Richter, Gintare Surblyte & Klaus Wiedemann, *Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*, Max Planck Institute for Innovation & Competition Research Paper N.16-10 (2016).

[6] European Commission, *supra* n. 4.

identified or identifiable person.[7] Non-personal data could, therefore, be defined in opposing terms as data that does not refer to an identified or identifiable person.

Industrial (big) data often refers to a large amount of diversified time series data generated at a high speed by industrial equipment.[8] Due to the fact that industrial data is generated by automated equipment and processes in a controlled environment where human involvement is kept to a minimum, it is usually more structured, more highly correlated, and more orderly than non-industrial data.

Even though there is no consensus on the meaning of the term 'data' *per se*, from a legal perspective it is possible to identify some basic elements on which there is agreement. In legal writings, an oft-cited point of reference for defining data is the wide-reaching definition developed by the joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), according to which data is the '[r]einterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing.'[9] While 'data' is usually seen as raw material, 'information' is understood to include an understanding of the significance of data; data is objective, while information is not.[10] Information theory defines information as 'the number of discernible signals or data points needed to transmit a message'.[11]

Several authors draw a distinction between data, syntax, and semantic content, whereby information is the semantic content that can be extracted from data or signals.[12] It has also been argued that the extraction of semantic content from a signal, a message, or a data set requires a combination of prior structural knowledge (i.e. an understanding of the semantics and syntax of the discrete symbols or the continuous signal) and contextual knowledge, acquired through learning.[13] For example, if a person has knowledge of the Finnish alphabet, he can read the words of a Finnish text, but without prior knowledge of Finnish syntax and vocabulary, he cannot understand the meaning of the text.

The distinction between data and semantic content is also important for distinguishing media products such as books, music, films, and news articles from the underlying data that encode this content. It is uncontroversial that media content is protected by IPRs, but what

---

[7] According to Article 4(1) of the General Data Protection Regulation (GDPR), '"personal data" means any information relating to an identified or identifiable natural person … an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

[8] The term 'big data' emerged in 2012, along with the concept of 'Industry 4.0', and refers to data created by industrial equipment that might hold potential business value.

[9] ISO/IEC 2382-1, revised by ISO/IEC 2382:2015 – Information technology – Vocabulary. The EU Commission also referred to this definition in European Commission, *Towards a Thriving Data-Driven Economy* (COM(2014)442 final), 4.

[10] Liane Colonna, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Principles in Light of the United States Government's National Intelligence Data Mining Practices* 31-32 (2016).

[11] Max Boisot & Agusti Canals, *Data, Information and Knowledge: Have we Got it Right?*, Internet Interdisciplinary Institute Working Paper Series WP04-002 (2004).

[12] Markel Vigo & Simon Harper, *Challenging Information Foraging Theory: Screen Reader Users are Not Always Driven by Information Scent*, Proceedings of the 24th ACM Conference on Hypertext and Social Media 60-68 (2013).

[13] See Nestor Duch-Brown, Bertin Martens & Frank Muller-Langer, *The Economics of Ownership, Access and Trade in Digital Data*, Digital Economy Working Paper 2017-01; JRC Technical Reports (2017).

about the data *per se*? In addition, if the law were to recognise the ownership of data through IPRs, it would be important to define where such rights would apply: would ownership relate to digital data sets themselves, in the form of bits and bytes, for instance, or to the information such data sets contain? Distinguishing between the two might not be an easy task.

Another important point to highlight when discussing IPR protection for data relates to whether the data is created by legal or natural persons, or generated by machines or sensors. Some of the literature on this subject makes a distinction between machine-generated and human-generated data.[14] The concept of machine-generated data is also often used to help distinguish between personal and non-personal data because most of the machine-generated data is non-personal. The distinction between direct and indirect human data sources, however, is not clear-cut, especially because much machine-generated data requires a direct or indirect human source. Indeed, the issue of the human or non-human creation of data is a sensitive one when discussing the possibility of applying IPRs to data, since IPR entitlement is based on the idea of human creators and inventors and the IP system is supposed to incentivise (human) creativity and innovation.[15] Machine-generated data challenges some of the basic principles of IP: firstly, the creation and use of such data takes place on a much larger scale, and in different forms, compared to traditional IP-protected works; secondly, the authorship and inventorship of such data is dispersed (e.g. between the owner of a sensor/machine, the machine's programmers, the person collecting the data, etc.), while the need to provide incentives for data creation is questionable.[16] Any discussion of protecting data by providing incentives through IPRs should take these points into consideration.

§9.03 The Challenge of Protecting Industrial Data Through Exclusive Rights

Probably the most challenging aspect of applying traditional concepts of property ownership to data is that data is a non-rival good, that is, multiple people can use the same data at the same time without any loss of information for any of the parties involved.

The IP system was established to deal with the non-rivalrous nature of intangible assets. A non-rivalrous good (e.g. data) is one that multiple people can use simultaneously without impeding the use of the same good by others. In the context of IPR, ownership refers to the negative right to exclude others from performing certain acts, instead of the traditional concept of ownership as a set of rights over property.[17] While the ownership of data as IP was not a concern in the analogue information age due to the fact that analogue datasets are usually costly to copy and reuse, the dramatic reduction in the cost of copying, merging, and transmitting digital content has made it significantly harder to create barriers that make the

[14] Zech, *supra* n. 5.
[15] An exception is trademark law, which primarily protects not innovativeness or creativity but commercial distinctiveness. See Taina Pihlajarinne, *Should we Bury the Concept of Reproduction – Towards Principle-Based Assessment in Copyright Law?*, 48 IIC 953, 970-971 n.8 (2017).
[16] Anette Alen-Savikko, Rosa Ballardini & Taina Pihlajarinne, *Tekoälyn Tuotokset ja Omaperäisyysvaatimus – Kohti Koneorientoitunutta Tekijänoikeutta?*, 116 *Lakimies* 975-995 nos 7-8 (2018); *see also* Chapter 7 of this book.
[17] Bernard H. Siegan, *Property Rights: From Magna Carta to the Fourteenth Amendment* (2001).

use, reproduction, and transmission of information excludable.[18] However, ownership in the IPR sense of the term might not be applicable to the creation and management of data, in which the concept of ownership tends to be used to assign responsibility and accountability.[19] As a consequence, even though there is a well-established legal framework for applying exclusive IPRs to the intangible and non-rival expression or implementation of ideas (e.g. through the copyright and patent systems), the legal status of data as regards IP ownership is less clear. Although there is no legislation on the ownership of data in the EU or its Member States, there are numerous pieces of legislation that have an impact on data control and access. In particular, ownership rights in non-personal data are partly regulated by the copyright law system and the *sui generis* database right,[20] combined with some provisions in the trade secrets regime and in general contract law.

[A] Data and Copyright

In terms of protectable subject matter, it seems reasonable to assume that copyright law is, to some extent, applicable to data. However, even though it is clear that things like the texts, sounds, and videos included within data sets are copyrightable, whether the data *per se* can receive copyright protection is highly questionable. On a general level, it has been argued that the UsedSoft decision of 2012[21] could have opened the door for a discussion of the ownership of intangible assets, such as data.[22] In fact, the Court of Justice of the European Union (CJEU) held that the commercial distribution of software via internet downloads is based not only on licensing, but also on the sale of goods. Therefore, following the principle of exhaustion, the owner of copyright in a piece of software cannot prevent a perpetual licensee from reselling his software (understood as a downloadable file). In other words, the CJEU's decision implies that there is a specific ownership right in intangible goods like software downloaded via the internet.

From the perspective of the legal principles of copyright law, two key issues need to be addressed: firstly, the conditions under which data can be considered a 'work' for copyright purposes are unclear; secondly, there is a major question over how to draw the line between copyrightable, original data and uncopyrightable, unoriginal data.

The Berne Convention states that a work is protected by copyright if it is a literary or artistic work. This qualification is quite broad and may cover virtually any creative piece of work. A piece of work may be protected regardless of its form or mode of expression, provided that it is original. Works excluded from protection include ideas and principles, facts and information, mathematical theories and algorithms, official decisions, and works that are no longer protected and have fallen into the public domain. Even though copyrightable works include categories like literary works, musical works, dramatic works,

---

[18] Mark A. Lemley, *IP in a World Without Scarcity*, Stanford Public Law Working Paper N.2413974 (2014), available at: https://ssrn.com/abstract=2413974 (accessed 30th April 2019).
[19] OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being* 195 (2015).
[20] Although data can also be protected by patent law, for instance in cases of industrial data resulting from process patents, this application of patent law is quite limited and, as such, is not discussed in this paper.
[21] Case C-128/11 *UsedSoft GmbH v. Oracle International Corp.* ECLI:EU:C:2012:407.
[22] See, for instance, Benoit Van Asbroeck, Julien Debussche & Jasmien Cesar, *Building the European Data Economy: Data Ownership* (White Paper) (2017).

etc, such categories should be viewed broadly. Depending on its nature, data could fall into several of these categories. Traditionally, the concept of a 'work' in copyright law has been considered alongside the originality requirement rather than being addressed separately. However, recent trends have highlighted the importance of creating a clear and independent definition of what is to be considered a 'work'. For instance, the Levola v. Smilde Foods case,[23] currently under consideration by the CJEU, raises the possibility of creations that cannot be perceived by sight and/or hearing qualifying as 'works'. It seems reasonable to suppose that while deciding on this specific case, the CJEU might also shed light on the question of how a 'work' should be characterised in general in order to attract copyright protection. This might provide some clarity on the issue of data as a work.

The originality requirement in European copyright law is defined in the Computer Programmes Directive,[24] the Database Directive,[25] and the Term Directive[26] as the stipulation that a work be its 'author's own intellectual creation'. Up until the *Infopaq* decision of 2009,[27] however, this requirement applied only to specific categories of works, namely photographs, computer programs, and databases. The *Infopaq* decision extended this interpretation of originality to all other categories of work. Based on the argument that the Information Society Directive (InfoSoc Directive) should be rooted in similar principles to those of other Directives, the CJEU held that copyright protection in the sense of Article 2(a) of the InfoSoc Directive should apply only to subject matter that is original in the sense that it is its author's own intellectual creation. The CJEU explained this interpretation further in other key decisions, such as *Murphy*,[28] *Painer*,[29] and *Football Dataco*,[30] stating that for a work to be considered its 'author's own intellectual creation', the author must 'stamp his *personal touch* or reflect his *personality* in the sense that he *expresses his creative abilities* in original manner by making free and creative choices (emphasis added)'. It might be difficult for data *per se* to attract copyright protection, both because data often lacks this level of creativity and because, as previously mentioned, most datasets nowadays are generated by machines rather than by creative humans. This second point especially raises the question of whether the requirement that a work be its 'author's own intellectual creation' (where an 'author' has traditionally been understood to mean a natural person)[31] can even be met by data. Moreover, even in cases where the production of machine-generated data can be linked

---

[23] See Case C-310/17 *Request for a preliminary ruling from the Gerechtshof Arnhem-Leeuwarden (Netherlands) lodged on 29 May 2017 — Levola Hengelo BV v. Smilde Foods BV* (2017), available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CN0310 (accessed 30th April 2019).
[24] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs Art. 1(3) (23 Apr. 2009), OJ L111.
[25] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases Art. 3(1) (11 Mar. 1996), OJ L 77/20 (DB Directive).
[26] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the Term of Protection of Copyright and Certain Related Rights Art. 6(1) (12 Dec. 2006) OJ L 372.
[27] Case C-5/08 *Infopaq International A/S v. Danske Dagblades Forening* ECLI:EU:C:2009:465.
[28] C-429/08 *Karen Murphy v. Media Protection Services Ltd* ECLI:EU:C:2011:631.
[29] Case C-145/10 *Eva-Maria Painer v. Standard VerlagsGmbH and Others* ECLI:EU:C:2013:138.
[30] Case C-173/11 *Football Dataco Ltd and Others v. Sportradar GmbH and Sportradar AG* ECLI:EU:C:2012:642.
[31] Rosa Ballardini, Kan He & Teemu Roos, 'AI-Generated Content: Authorship and Inventorship in the Age of Artificial Intelligence' in Taina Pihlajarinne, Juha Vesala & Olli Honkkila (eds), *Online Distribution of Content in the EU* (2019).

to a legitimate author, it might be very difficult to identify the person by whom the arrangements necessary for the creation of the work were undertaken. For instance, the authorship of the work and the ownership of the copyright could be dispersed amongst, *inter alia*: 1) the designer(s) of the smart system, 2) the data provider(s), and 3) the system's user(s). Ultimately, the most challenging aspect of determining whether a given set of machine-generated data is eligible for copyright protection is the assessment of whether the human contribution to the development of the data is sufficient to demonstrate the existence of a human's own intellectual creation or contribution to an inventive concept.[32]

[B] The Database Right Dimension

The EU legal regime for database protection[33] is a two-tier system: copyright protection is granted to creative, original databases, while *sui generis* protection is granted to databases that are the result of 'substantial investment'.[34]

Copyright protection applies to databases the structure of which is original, that is to say where the selection or the arrangement of the contents of the database is its 'author's own intellectual creation'.[35] This criterion does not apply to the data within the database; originality is needed in the structure of the database itself.

Sui generis database protection provides a better basis for protecting datasets in the data economy. However, this form of protection also has limitations, both in terms of the subject-matter and the scope of protection. Firstly, the *sui generis* database right only protects a database as a collection of data and not individual items of data per se. In fact, the DB Directive forbids the 'extraction' and 're-utilisation' of individual data included within a database only if these acts constitute a 'permanent or temporary transfer of all or a substantial part of the contents of a database to another medium'.[36]

Secondly, while the DB Directive includes a general aim of protecting investments,[37] this protection extends only to certain traditional types of digital database that are easily accessible and organised around a fixed base, for instance collections of articles, photos, or job advertisements; collections of information in booking systems for hotels or airline tickets; or search engines. In these databases, the collection or arrangement of the data is valuable. However, protection does not extend to non-traditional digital databases the value of which lies in large volumes of data in itself. The main reason why it might be difficult to protect non-personal data through the *sui generis* database right stems from the Directive's definition of a database, further developed by the CJEU. A database is defined as a 'collection of independent works, data or other materials arranged in a systematic or methodical way and

[32] Alen-Savikko et al., *supra* n. 16.
[33] DB Directive, *supra* n. 26.
[34] DB Directive, *supra* n. 26, at Arts 3 and 7.
[35] DB Directive, *supra* n. 26, at Art. 3(1) and recital 15.
[36] DB Directive, *supra* n. 26, at Art. 7(2)(a).
[37] For instance, DB Directive, *supra* n. 26, at recital 10 states that 'the exponential growth, in the Community and worldwide, in the amount of information generated and processed annually in all sectors of commerce and industry calls for investment in all the Member States in advanced information processing systems'.

individually accessible by electronic or other means'.[38] The CJEU has stated that the term 'independent works' refers to the fact that a database consists of 'any collection of works, data or other materials, separable from one another without the value of their contents being affected'.[39] A database must also include a 'method or system of some sort for the retrieval of each of its constituent materials'.[40] A 'systematic or methodical' way of arrangement and individual accessibility, regardless of whether the systematic or methodical arrangement is physically apparent or not, means that the collection must be contained within a fixed base. It must also include technical means, such as electronic, electromagnetic, or electro-optical processes, or other means, such as an index, table of contents, or particular plan or method of classification, to allow for the retrieval of any independent materials contained within it.[41] Although it is possible that the data collected and utilized by smart systems could create databases that fall under the scope of protection of the DB Directive, as such datasets might be valuable when separated from the systems that created them, it seems unlikely that these datasets would fulfil the requirements of systematic or methodical arrangement and individual accessibility required by the Directive, since smart systems usually capture, analyse, and utilize data immediately, without using any fixed base.

Thirdly, Article 7(1) of the DB Directive states that *sui generis* protection is reserved for databases for which there has been 'qualitatively and/or quantitatively a substantial investment' in the 'obtaining, verification or presentation' of their contents.[42] The CJEU stated in the British Horseracing Board case[43] that the notion of 'investment' refers to the resources used to monitor the accuracy of the materials collected when a database is created and during its operation, with a view to ensuring the reliability of the information contained within it. Resources used for verification during the creation of data or other materials that are subsequently collected in a database, on the other hand, count as resources used in creating materials and *cannot* be taken into account when assessing whether there was substantial investment in the database under the terms of Article 7(1) of the DB Directive. The CJEU has explained that the rationale for database protection is to promote the creation of storage and processing systems for existing information and not the creation of materials capable of being collected subsequently in a database.[44] 'Substantial' investment can consist of the investment of money, time, or labour. It is evident that substantial investment is necessary for developing smart systems, but such systems capture and collect data autonomously. If the development of the mechanism used to acquire an extensive collection of data required a large investment, it is possible that, for instance, obtaining the contents of the resulting database could be said to require substantive investment. If, however, there is no separate investment in the collection, verification, or presentation of the data, *sui generis*

[38] DB Directive, *supra* n. 26, at Art. 1(2) While the content of data is irrelevant, it must be in a form that is understandable by humans. See also Estelle Derclaye, 'The Database Directive' in Irini Stamatoudi & Paul Torremans (eds), *EU Copyright Law* 298, 302 (2014).
[39] Case C-444/02 *Fixtures Marketing Ltd v. OPAP* ECLI:EU:C:2004:697.
[40] *Ibid*.
[41] *Ibid.*
[42] On the substantial investment criterion, see Perttu Virtanen, *Evolution, Practice and Theory of European Database IP Law* 166-186 (2008).
[43] Case C-203/02 *The British Horseracing Board Ltd ym. v. William Hill Organization Ltd* ECLI:EU:C:2004:695.
[44] *Ibid.;* Case C-444/02, *supra* n. 40.

database protection does not apply. Scholars have pointed out that this requirement excludes many important spin-off databases, such as sport fixtures, television listings, and timetables, from *sui generis* protection.[45] For instance, investment in the creation of smart products with sensors that collect data is unlikely to be considered in the assessment of whether investment in a database counts as 'substantial'.

Finally, an additional problem with the application of database protection to datasets is similar to a point discussed earlier in the context of copyright: if a database is created by smart systems, it might prove difficult to identify its right holder(s).[46] Although the maker of a database is not defined in the DB Directive, Recital 41 of the Directive states that 'the maker of a database is the person who takes the initiative and the risk of investing'.[47] Naturally, there might be joint ownership of a database if it is created jointly by several actors. It is possible that, for instance, the person who collects the material for a database, the person who manages the technical implementation of the database, and the person who finances the database, could all be considered its creators. While traditional databases could have many contributors, for instance in the case of multimedia works,[48] the situation is far more complicated where the creator of a database formed by a machine, like an AI system, is concerned. A database's creator is the one who takes the initiative in obtaining, verifying, or presenting its contents and assumes the risk of those activities. Ultimately, the assessment of who has made the decision to develop a smart system that produces a database and who is financially responsible for this development, as well as for the maintenance of the smart system, will need to be made on a case by case basis.

[C] Protecting Data Through Trade Secrets and Contracts

Due to the limitations of the current IPR system when it comes to the protection of data, trade secrets, contractual mechanisms, and technical protection measures are often used to protect and trade data. In fact, these mechanisms can allow data that is not fully recognised by current regulations to be made excludable. It is possible to enter into a contractual agreement that states by whom data is owned and how the parties to the contract are entitled to use it.[49]

---

[45] See Estelle Derclaye, 'Database Rights: Success or Failure? The Chequered yet Exciting Journey of Database Protection in Europe in Christophe Geiger (ed.), *Constructing European Intellectual Property: Achievements and New Perspectives* 340, 344 (2013).

[46] DB Directive, *supra* n. 26, at Art. 4(1) states that '[t]he author of a database shall be the natural person or group of natural persons who created the base'. However, the issue of authorship is left partly to the discretion of individual Member States, since the Directive also states that the legislation of a Member State can designate a legal person as the right holder. The ownership of databases created by employees is an issue that has not been harmonized across Member States. Recital 29 of the directive states that a Member State can decide to adopt a provision according to which, if 'a database is created by an employee in the execution of his duties or following the instructions given by his employer, the employer exclusively shall be entitled to exercise all economic rights in the database so created, unless otherwise provided by contract.'

[47] This excludes subcontractors in particular from the definition of creator.

[48] Tanya Aplin, *Copyright Law in Digital Society: The Challenges of Multimedia* 89-90 (2005).

[49] As far as databases are concerned, freedom of contract has been restricted by Arts 6(1), 8, and 15 of the DB Directive, which confer rights on the lawful users of databases. However, the CJEU has stated in Case C-30/14 *Ryanair Ltd v. PR Aviation BV* ECLI:EU:C:2015:10 that the DB Directive does not apply to databases that do not meet the criteria for databases as defined by the Directive. Therefore, Articles 6(1), 8, and 15 do not preclude the author of such a database from laying down contractual limitations on its use by third parties, without prejudice to the applicable national law.

These measures may fail, however, especially in the context of data. The EU Trade Secrets Directive[50] strengthens protection against the unlawful acquisition, use, and disclosure of trade secrets (including data). However, this protection applies only to information not 'generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question'.[51] In other words, if data is shared with third parties or made publicly available (e.g. on a website), protection under the TS Directive does not apply. The TS Directive's lack of applicability to the modern data industry has led prominent scholars to argue that it is already technologically outdated.[52]

The use of contracts to protect data also has several issues, such as increased transaction costs and the unharmonised nature of European contract law, which leads to unpredictability and, in turn, creates impediments to the free flow of data. One important impediment arises from the fact that in many jurisdictions, third parties are not bound by contracts and therefore, contract clauses that relate to third parties are not enforceable. Different countries vary widely in their approaches to the principle of privity of contract and to how the actions of non-contractual third parties are perceived in relation to a contract.[53]

§9.04 A New Legal Paradigm to Protect Data?

In view of the rapidly growing importance of data to the digital economy, there is a need to address the issues surrounding the efficient protection of data in EU law. Currently, the poorly defined legal framework for data ownership, combined with limitations on the access to and trade of data, might inhibit the realisation of the full economic benefits of non-rival data, and could hinder innovation and effect the efficiency of data markets overall.[54] One could argue that creating incentives for data generation and the disclosure of data and promoting efficient markets for data-related products requires the creation of exclusive rights. Clear rules on who benefits from the utilization of data could promote the free flow of data.[55] The key question, however, is: what kind of regulation is needed in order to make the data economy work? Is the regulation of data ownership necessary? If so, what form should this regulation take?

[A] The Rise of Data Ownership Regimes at a National Level

Issues related to the IP ownership of data have been partially addressed in the case law of some national courts within the EU.

In a decision of 1995, for instance, the Higher Regional Court of Karlsruhe in Germany found that the deletion of data stored on a data carrier could infringe upon the right

---

[50] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure (8 Jun. 2016), OJ L 157 (TS Directive).
[51] TS Directive, *supra* n. 51, at Art. 2(1)(a).
[52] Drexl et al., *supra* n. 5.
[53] On these differences, see Marcus Norrgård, *Avtalsingrepp. Om Otillbörliga Ingripanden i Kommersiella Avtalsförhållanden* (2006).
[54] For more details on possible market failure see Duch-Brown et al., *supra* n. 13.
[55] Zech, *supra* n. 5.

of ownership in the data carrier itself. In other words, the protection of the ownership right in the data carrier was found to extend to the data stored on that carrier.[56] Issues related to data ownership in Germany have also been discussed in subsequent cases in the context of the employee-employer relationship. In a decision of 2013, the court of Nürnberg[57] had to decide whether former employees were allowed to delete data stored on their company-owned laptops. On the basis of the 'Skripturakt' doctrine (according to which the person who generates data gains ownership of that data, even if the data is used by the person's employer or business),[58] the court decided that employees were allowed to delete the data, i.e. the employees were conceived as having ownership rights in the data.

Another interesting development related to data ownership from a European national court came in a judgement from the French Supreme Court in 2015.[59] The *Cour de Cassation* found that downloading computer data without its owner's permission amounts to the offence of theft. In other words, the Court seems to acknowledge that data may actually be owned.[60]

Similar questions of data ownership have been addressed differently by the UK courts, which have thus far held that data is not property and, as such, cannot be stolen,[61] and that there is therefore no proprietary right in, for instance, the data included in an email.[62]

These actions at a national level, together with the aforementioned legal uncertainty over data ownership in the EU, have increased the Commission's concern over the barriers to the free flow of data in the EU, and the consequent need to tackle this issue.[63]

[B] New *Ad Hoc* Exclusive Rights

In the working paper on the free flow of data within the Digital Single Market, two alternative ways of protecting a 'data producer's right for non-personal or anonymised data' are discussed. The first option consists of creating a new transferable intellectual property right, probably as a related right, in 'non-personal or anonymised machine-generated data'. It would encompass 'the exclusive right to utilise certain data, including the right to license its usage'. This would include a set of rights enforceable against any party, independent of contractual relations, preventing further illegitimate use of data by third parties. The exclusive right would also include the right to claim damages for unauthorised access to and use of data. The second option (which is not discussed further in this paper) is 'a set of purely defensive rights', following the design of the protection of know-how in the TS Directive. This approach would be based on 'de facto possession' rather than ownership: a 'de facto data holder' could be entitled to the following civil law remedies for the 'illicit misappropriation of data' by third parties: 1) the right to seek injunctions preventing further use of the data by third parties who have no right to use it, 2) the right to have products built

[56] See *OLG Karlsruhe, Urt. v. 07.11.1995* 3 U 15/95 – Haftung für Zerstörung von Computerdaten; see also Van Asbroeck et al., *supra* n. 22, at 23-26.
[57] OLG Nürnberg 1. Strafsenat decision of 23 Jan. 2013, 1 Ws 445/12, par. 14.
[58] See Hoeren, *supra* n. 1.
[59] 20 May 2015 (N.14-81336).
[60] N. 14-81336, s*upra* n. 60.
[61] See *Oxford v. Moss*, 68 Cr App Rep 183 (1979).
[62] See *Fairstar Heavy Transport N.V. v. Adkins*, EWCA Civ 886 (2013).
[63] See European Commission, *Inception Impact Assessment: European Free Flow of Data Initiative Within the Digital Single Market*, Ec.europa.eu, http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_cnect_001_free_flow_data_en.pdf (accessed 30th April 2019).

on the basis of misappropriated data excluded from market commercialisation, and 3) the possibility of claiming damages for the unauthorized use of data.[64]

According to the Commission, the investments made and the resources put into the creation of the data would play a crucial role for acquiring a data producer's right. In this regard, the Commission has identified the manufacturer of sensor-equipped machines, tools or devices (generating the data) who have invested in the development and market commercialisation of such machine, tool or device and the economic operators using them have to pay a price (for purchase or lease) and, thus, have to amortise the costs as they are the main responsible for making the investments. Although, according to the Commission, joint rights in data might be possible, one problem it has already acknowledged is that data is often created by multiple parties and, as such, a new right based on 'ownership' would be difficult to implement.[65] At the time of writing. the data producer's right is still just a proposal; if implemented, this new right would increase the level of protection of industrial data in the EU to a much higher level than that currently offered by the database right. As previously explained, the database right protects data only on the condition that 1) the data is structured in a 'database' (the characteristics of which are specifically defined) and 2) the database is the result of 'substantial investment'. In contrast, the data producer's right would directly protect machine-generated data without any prerequisites.

Along the same lines as the Commission's approach to this issue, some scholars have suggested the creation of new *ad hoc* rights for the protection of data. Zech, for instance, has suggested the creation of a non-exclusive data producer's right with 'machine-readable coded information that is defined only by its representative characters (bits)' as its subject matter.[66] To be covered by the right, data would have to be created using automated measurement processes, intellectual activity, or simple computing power. The party economically responsible for the operation of the equipment generating the data would be given the status of right holder. Use of the data for statistical analyses would constitute an infringement of the data producer's right, but the independent creation of the same data would not. Only commercial acts would be counted as infringements, as Zech suggests an exception for use of the data for private and non-commercial purposes. Moreover, he suggests that the protection offered should be both short-term and transferable.[67]

[C] Fragmentation and Complexity do not Foster the Free Flow of Data

In EU copyright law, there is a general tendency to create new related rights whenever new interests in protecting certain investments emerge. Often, the creation of new rights stems from the spectre that valuable European assets are being misappropriated by large American companies. For instance, the idea of Google 'stealing' European news has already led to an

[64] See European Commission, *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*, Ec.europa.eu, https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy (accessed 30th April 2019).
[65] *Ibid.*, at 35.
[66] Zech, *supra* n. 5.
[67] *Ibid*.

introduction of a new neighbouring press publishers' right.[68] In a similar way, it was the fear that the European database industry would be unable to compete against its American counterpart that led to the creation of the *sui generis* database right.

The excessive introduction of new *ad hoc* neighbouring rights, however, might needlessly fragment and complicate the EU copyright system overall, creating insecurities in internal markets.[69] Furthermore, the newly-proposed data producer's right in particular has been criticized for reinforcing the bargaining position of data holders and for needlessly increasing transaction costs. There may not be any need to create additional incentives for the manufacturers of devices that produce data, since IPR already protects such hardware and software. The data aggregators and analysts who create new value in data markets, on the other hand, might actually need such incentives.[70] Furthermore, the potential impact of the data producer's right is unclear and ambiguous: it has the potential to both enhance and inhibit valuable activities in the data economy. As Kim points out, before examining data aggregators and analysts as potential candidates to be considered data right holders, the need to create additional incentives to facilitate the exchange and analysis of data should itself be scrutinized.[71]

Another problem with the Commission's proposed solution relates to the issue of data ownership. Interestingly enough, the Commission's initiative to introduce a new exclusive right in data has attracted considerable criticism not only from academia, but also from the industry.[72] There are two main reasons why the industry in particular is opposed to the introduction of new exclusive rights for data: firstly, many data-producing firms are also reliant on *access* to the data of other firms. Secondly, the criteria for who would qualify as the data owner under the new right are not at all clear. Although the Commission has expressed concern that a new right based on ownership might fail due to the fact that data is usually produced by multiple parties, a data producer's right based on the Commission's idea of having both manufacturers and users be classified as right holders might actually exacerbate this problem further. As Kim argues, it might not be possible to 'hit both birds with one stone'. On the one hand, she points out, one justification for granting exclusive rights in data to data users is the fact that users might not have access to the data gathered by the manufacturers of smart systems. On the other, however, a data producer's right might not be a suitable solution here, especially given the fact that multiple right holders could prove to be an impediment to opportunities to license data.[73]

---

[68] European Commission, *Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market* (COM(2016)0593 final), Art. 11. available at: https://ec.europa.eu/digital-single-market/en/news/proposal-directive-european-parliament-and-council-copyright-digital-single-market (accessed 30th April 2019).

[69] See Taina Pihlajarinne & Juha Vesala, *Proposed Right of Press Publishers: A Workable Solution?*, 13 Journal of Intellectual Property Law & Practice 200-208 n.3 (2018); see also Ana Ramalho, *Beyond the Cover Story – an Enquiry into the EU Competence to Introduce a Right for Publishers*, 48 IIC 71, 89 n.1 (2017).

[70] See Daria Kim, *No One's Ownership as the Status Quo and a Possible Way Forward: A Note on the Public Consultation on Building a European Data Economy*, 13 Journal of Intellectual Property Law & Practice 154, 163 n.2 (2018).

[71] *Ibid.*, at 163, 164.

[72] Drexl, *supra* n. 3; Andreas Wiebe, *A New European Data Producers' Right for the Digital Economy?*, 9 Zeitschrift fuer Geistiges Eigentum / Intellectual Property Journal 394-398(5) n.3 (2017).

[73] See Kim, *supra* n. 71, at 162-163.

More fundamentally, among the multiple negative aspects of this new right, a key drawback is that it would destroy the core principle in IP law that data *per se* is not protectable and that only creative, innovative, or other meritorious investments can receive protection.[74] The introduction of *sui generis* database protection has already weakened this fundamental idea. Making the same mistake again should be avoided: protecting investments that are not clearly connected to creativity is a path that should not be followed. It should also be noted that business and technology reports have highlighted that recognising ownership rights in single pieces of data (and small datasets) could lead to a scarcity of data, hindering innovation through big data analytics.[75]

Another point of concern over the data producer's right is that it would overlap with other IPR regimes, such as copyright and database rights, endangering the user freedoms guaranteed under these frameworks. Finally, it is also difficult to understand how this new right would work with the new text and data mining exception that is at the heart of the DSM Directive.

§9.05 Fostering the Free Flow of Data

[A] The Renaissance of the *Sui Generis* Database Right

A more workable alternative solution for regulating and protecting data could be sought by revising the existing *sui generis* database right regime. This solution could promote greater coherence within the copyright system instead of complicating it further and causing more insecurity in markets, as would the adoption of new *ad hoc* rights. Additionally, revising existing rights would make it easier to coordinate and harmonise existing provisions affecting the use of data.

This option would involve extending the scope of the protection provided by the *sui generis* right to cover datasets that currently fall outside it. This would mean, at the very least, that the definition of 'database' and the requirement of 'substantial investment' would need to be revisited. In practical terms, this would require either modifications to the text of the Directive and/or judiciary developments through case law interpretation. We argue that if these changes are to be made, developing a new line of interpretation via case law would be more flexible and suitable than changing the text of the DB Directive itself. As such, should this course of action be followed, revisions to the text of the Directive (e.g. a revision to the term of protection for datasets) should be kept to a minimum, while the scope of the protection it offers (as well as the requirements needed to qualify for protection) should be developed via case law interpretation.

The general definition of a database in the DB Directive as a 'collection of independent works, data or other materials arranged in a systematic or methodical way and

---

[74] Bernt Hugenholtz, 'Against Data Property' in 3 Hanns Ullrich, Peter Drahos & Gustavo Ghidini (eds), *Kritika: Essays on Intellectual Property* (2018), available at: https://www.ivir.nl/publicaties/download/Data_property_Muenster.pdf (accessed 30th April 2019).

[75] Zukunftsrat der Bayerischen Wirtschaft, *Zukunft Digital—Big Data: Analyse und Handlungsempfehlungen*, vbw-zukunftsrat, https://www.vbw-zukunftsrat.de/downloads/big_data/vbw_zukunftsrat_handlungsempfehlungen_langfassung_v15_rz_web.pdf (accessed 30th April 2019).

individually accessible by electronic or other means' could, for instance, be interpreted in such a way as to include some datasets. The core issue here would be the revision of CJEU interpretations of what constitutes a database to fit the purpose of providing protection for datasets. Both the fixed base requirement and the requirement for technical means to allow for the retrieval of data from this fixed base would need to be uncoupled from the definition of a database in order to provide protection for datasets. One way to achieve this would be the creation of separate categories of database, for instance 'traditional databases' (i.e. databases defined in accordance with the current interpretation of the DB Directive) and 'dataset databases' (i.e. a new type of protected subject matter to cover datasets, the scope of protection for which would need to be redefined via case law interpretation). In a way, this line of thinking could be compared to a similar approach in the field of copyright, where the definition of 'work' is used in an equally flexible manner, although different categories of work exist (and traditionally, different originality thresholds have been applied to these different categories)[76]. Similarly, different categories of database (including, but not necessarily limited to, traditional databases and dataset databases) could fall under the umbrella definition of a database, even though the concept of a database (like the concept of work in the copyright framework) would apply equally to all categories.

Different 'thresholds of investment' to attract protection would then need to be developed and applied. As such, the requirement for 'substantial investment' would need some reconsideration. The difficulty is that the DB Directive 7.1 Article requires substantial investment in the 'obtaining, verification or presentation' of the content of a database in order for it to receive protection. Thus, substantial investment in, for instance, the development of a smart system that collects data into a database is not counted for this purpose. Accepting these kinds of investment when deciding on whether to grant protection to a database could lead to too many IPRs being awarded to recoup the same/similar investments: in smart systems, the capture and collection of data is automated and, as such, these systems do not necessarily require further investment beyond that funnelled into the development of the smart machine itself. Moreover, though it is reasonable to grant IPRs to incentivize innovation in smart systems, it is questionable whether the developer of a smart machine should also be entitled to IP ownership rights in the output generated automatically by that machine: considering investment in developing a smart system as a valid reason to grant protection to a database could lead to exactly this outcome.[77] Therefore, a further, more specific requirement should be developed by the CJEU for determining whether datasets qualify for protection. One option could be to revisit interpretations and consider also investments devolved to the creation of smart systems by 1) raising the "threshold of investment" and 2) requiring certain "types of outcome". For instance, some kind of "super or extraordinary investment" in the developing of the machine that have subsequently resulted in the creation of "valuable" datasets DB could be required. This would likely mean that

[76] Since the CJEU's decision in the InfoPaq case (Case C-5/08, *supra* n. 28), the interpretation of originality as meaning work that is its 'author's own intellectual creation' should be applied equally to all categories of work. However, the abstract nature of this concept might still lead to differences in interpretation between different categories of work.

[77] This question relates to the issue of incentives, as well as to the requirements for IP entitlement and the definition of output in current interpretations of IP law. For more on this subject see, for instance, Ballardini et al., *supra* n. 32.

only a small group of datasets would be protected. Although this proposal could create new opportunities in terms of the protection of data, the subjectivity of its criteria might lead to further difficulties.

Another downside of the current provision is the duration of the *sui generis* right: fifteen years is clearly longer than is reasonably needed for the protection of datasets. A new maximum duration for the protection of datasets, for instance, five years, could be set instead. This change could not be achieved without revisiting the text of the DB Directive, however.

The extension of the reach of exclusive rights discussed above might lead to the need to introduce further mandatory exceptions and limitations (E&Ls) in addition to those currently contemplated in the Directive. This might be necessary to create a proper balance between providing protection for data, and access to it. E&Ls might be necessary, for instance, to guarantee that the interests of all the stakeholders involved in the collection of a set of data, for example public authorities, are respected. An extensive and flexible set of E&Ls might very well prove a necessity. A fair use limitation or exception would be the most suitable type, despite the challenges to introducing such a provision in civil law countries.[78]

Overall, even though there might be room to adjust the scope of the DB Directive (and revisiting the *sui generis* database right is certainly a better solution than creating new *ad hoc* rights, causing further fragmentation), the potential harm this could cause to the free flow of data might actually exceed the benefits of creating legal certainty on the ownership of data. A better solution would be to promote the free flow of data by fostering a model at the EU level that would impede the national barriers to the free flow of data created by, for instance, ownership-like legislation on data in the Member States.

[B] The Fifth Internal Market Freedom: The Free Flow of Data

Unquestionably, the best solution for fostering the free flow of data is non-regulation. Any further steps towards creating exclusive rights in data or information *per se*, that is to say protecting investments that do not have a clear link to creativity and inventiveness, should, in fact, be discouraged. Extending protection to data *per se* would not only conflict with the basic principles of IP law, but would also lead to an imbalance in favour of right holders, to the detriment of access. On the subject of incentives, it should also be noted that in the digital age, most datasets are generated by machines, not by creative humans. Even though there might be human involvement in the creation of data, human effort is usually directed towards the methods by which data is measured and the design of the machines and software that collect it. The design of machines and software falls within the scope of IPR protection; thus, in an indirect way, the system already provides incentives to create data. Moreover, as data is a representation of observed and measured facts, rather than a creation of the human mind, it is questionable whether the use of IPRs to incentivize developments in data production is even appropriate.

[78] Martin Senftleben, *The Perfect Match – Civil Law Judges and Open-Ended Fair Use Provisions*, 33 American University International Law Review 231-286 n.1 (2017), available at: https://ssrn.com/abstract=3002275 (accessed on 30th April 2019).

At the same time, there is a need to strengthen the principle of the free flow of data at the EU level by ensuring that no unjustified barriers to the free movement of data across the union arise at a national level. As previously discussed, recent developments at a national level seem to indicate that countries are leaning toward expanding the scope of exclusive rights to data. Indeed, an increase in this type of legislation is one of the reasons that the Commission has initiated legislative proposals on data regulation at the EU level. As discussed in this article, however, none of the solutions proposed by the Commission thus far seem suitable for balancing the protection of data against providing access to data. Existing IPRs might provide some protection to data already. Whether there is a need to increase the level of protection by introducing new ownership rights or extending the scope of existing rights is highly doubtful. Finding solutions to such an important issue requires us to take a step backwards and consider more fundamental and broad-minded approaches. As such, instead of looking at this issue from the narrow perspective of IPR or exclusive rights to data, there might be a need to create a new fundamental principle, that of the free flow of data, alongside the existing four Internal Market freedoms.[79] In this context, the idea of establishing the free flow of data as a fifth freedom in EU Treaties is worth considering. This discussion, however, is an entirely different subject, which goes beyond the scope of this paper.

§9.06 Conclusions

With the rise of the data economy, issues related to the regulation of non-personal data though ownership-like frameworks are becoming increasingly pressing and relevant. Data regulation via exclusive rights, however, should be approached carefully, in order to avoid the risk of adopting solutions that impede the free flow of data rather than fostering it.

Currently, the European Union's framework for data ownership is short-sighted in multiple ways. The consequence of this is that, on the one hand, no proper regulation for data exists (potentially harming innovation) while, on the other, solutions to tackle the issue of data ownership are starting to arise at a national level (potentially creating barriers to the free flow of data across the EU). Creating new *ad hoc* laws or exclusive rights for data, as the EU Commission currently proposes doing, would increase fragmentation and uncertainty in the field. A solution could be sought in revisiting the *sui generis* database right in the EU and broadening its scope. This would require revisions to database protection from multiple angles (including the scope of protection and term of protection). Ultimately, however, the potential harm this solution could cause to the free flow of data might actually exceed the benefits of creating this type of ownership right. Instead of adopting quick, short-term solutions, it would be advisable for the EU legislator and policymakers to keep calm in the face of the pressures posed by the data economy. In this spirit, the free flow of data could be fostered by preventing the construction of, *inter alia*, national barriers in the form of

[79] A similar idea was proposed by the Estonian Government in 2016 when the Commission initiated a consultation on this issue. See European Commission, *supra* n. 65; see also the speech by Estonian President Toomas Hendrik Ilves in the European Parliament on 2 Feb. 2016: European Parliament, *Debates,* Europarl.europa.eu, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20160202+ITEM-005+DOC+XML+V0//EN (accessed 30th April 2019).

ownership-like legislation on data in the Member States. Serious consideration should be given to establishing a fifth fundamental freedom in the EU, the free flow of data, as a way of reaching this long-term goal.