jipitec

1 | 2019

Volume 10 (2019)
Issue 1 ISSN 2190-3387

10 YEARS of JIPITEC

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 10 Issue 1 May 2019
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J. (NYU)
KIT - Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe Germany

Prof. Dr. Axel Metzger, LL. M. (Harvard)
Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin

Prof. Dr. Gerald Spindler
Dipl.-Ökonom, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by
DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

Articles

Editorial

by **Axel Metzger**

Recommended citation: Axel Metzger, Editorial, 10 (2019) JIPITEC 1 para 1.

1 It is a great pleasure to introduce the new issue of JIPITEC – the Journal of Intellectual Property, Information Technology and E-Commerce Law – to its esteemed readers. Issue 10(1) marks the celebration of an important milestone for the journal, its 10th anniversary. The journal was founded in 2009 by Thomas Dreier (Karlsruhe), Gerald Spindler (Göttingen), and Axel Metzger (Berlin) with the help of the Deutsche Forschungsgemeinschaft (DFG). In the years following, the board of editors was enlarged as we welcomed Séverine Dusollier (Paris), Lucie Guibault (Halifax), Miquel Peguera Poch (Barcelona), Chris Reed (London), and Karin Sein (Tartu) as members. With the help of the new editors, JIPITEC has developed during its first ten years into a European journal with international aspiration. Since 2016, the Deutsche Gesellschaft für Recht und Informatik (DGRI) has supported JIPITEC as its main sponsor and partner of cooperation. Statistics show that visits to JIPITEC's website have tripled in the last five years – from around 10,000 in 2014 to 30,000 in 2018. The majority of the readers in 2018 originated from the United States (13,961), followed by the United Kingdom (3,911), Germany (2,130), the Netherlands (1,023), and France (1,004).

2 JIPITEC is thus read and cited across Europe and beyond. It has just recently been included on HeinOnline and will soon be listed on Scopus, two major international publication and citation databases. Since 2009, JIPITEC has published three to four issues per year, comprising scientific peer reviewed articles, with occasional supplementary material, such as, political statements by academics, case notes and reports, as well as book reviews. The current issue shows how vibrant the scientific community of JIPITEC is today. Its editors received 17 article submissions for this issue – none of which were solicited actively. All the submissions have been reviewed by at least one (often two) expert(s) in the field in a double-blind peer review process. We are extremely grateful to our reviewers, all renowned experts in their field, who undertook the burden of quality control of the journal's contents in the last ten years on a voluntary basis.

3 The contributions of issue 10(1) reflect the main areas of interest of JIPITEC over the last ten years. *Daniel Gervais* provides a broad overview of the challenges to the different types of intellectual property rights raised by big data and artificial intelligence ("Exploring the Interfaces Between Big Data and Intellectual Property Law"). *Tatiana Eleni Synodinou* explains the still vague but practically very important concept of lawful use in European copyright law ("Lawfulness for Users in European Copyright Law"). In their paper, *Mathew Heim* and *Igor Nikolic* consider how the European FRAND access regime could be applied as a regulatory solution for dominant digital platforms ("A FRAND Regime for Dominant Digital Platforms"). *Amélie Pia Heldt* explores the human rights dimension of the use of filter technologies by intermediaries ("Upload-Filters: Bypassing Classical Concepts of Censorship?"). *Begoña Gonzalez Otero* evaluates the current initiatives of the European Commission to foster data sharing in the private sector with a special emphasis on data access for artificial intelligence training purposes ("Evaluating the EC Private Data Sharing Principles"). *René Mahieu, Joris van Hoboken* and *Hadi Asghari* examine the question of who is responsible for observing data protection obligations in networked service settings under the current European data protection rules ("Responsibility for

Data Protection in a Networked World"). *Maren K. Woebbeking* explores how smart contracts can be situated within the traditional Western concept of contract law and how they differ from traditional contracts in the individual phases of a contract's life cycle ("The Impact of Smart Contracts on Traditional Concepts of Contract Law").

4 We hope that the current issue will attract your attention and inspire your own scientific and practical legal work. Stay tuned to JIPITEC!

Exploring the Interfaces Between Big Data and Intellectual Property Law

by **Daniel Gervais***

Abstract: This article reviews the application of several IP rights (copyright, patent, sui generis database right, data exclusivity and trade secret) to Big Data. Beyond the protection of software used to collect and process Big Data corpora, copyright's traditional role is challenged by the relatively unstructured nature of the non-relational (noSQL) databases typical of Big Data corpora. This also impacts the application of the EU sui generis right in databases. Misappropriation (tort-based) or anti-parasitic behaviour protection might apply, where available, to data generated by AI systems that has high but short-lived value. Copyright in material contained in Big Data corpora must also be considered. Exceptions for Text and Data Mining (TDM) are already in place in a number of legal systems and likely to emerge to allow the creation and use of corpora of literary and artistic works, such as texts and images. In the patent field, AI systems using Big Data corpora of patents and scientific literature can be used to expand patent applications. They can also be used to "guess" and disclose future incremental innovation. These developments pose serious doctrinal and normative challenges to the patent system and the incentives it creates in a number of areas, though data exclusivity regimes can fill certain gaps in patent protection for pharmaceutical and chemical products. Finally, trade secret law, in combination with contracts and technological protection measures, can protect data corpora and sets of correlations and insights generated by AI systems.

Keywords: Copyright; patent; data exclusivity; artificial intelligence; big data; trade secret

Recommended citation: Daniel Gervais, Exploring the Interfaces Between Big Data and Intellectual Property Law, 10 (2019) JIPITEC 3 para 1

A. Introduction

1 The interfaces between "Big Data" (as the term is defined below) and IP matters both because of the impact of Intellectual Property (IP) rights *in* Big Data, and because IP rights might interfere with the generation, analysis and use *of* Big Data. This Article looks at both sides of the interface coin, focusing on several IP rights, namely copyright, patent, data exclusivity and trade secret/confidential information.[1] The paper does not discuss trade marks in any detail, although the potential role of Artificial Intelligence (AI), using Big Data corpora,[2] in designing and selecting trade marks certainly seems a topic worthy of further discussion.[3]

B. Defining Big Data

2 The term "Big Data" can be defined in a number of ways. A common way to define it is to enumerate its three essential features, a fourth that, though not essential, is increasingly typical, and a fifth that is derived from the other three (or four). Those features are: volume, veracity, velocity, variety, and value.[4] "Volume" or size is, as the term Big Data suggests, the first characteristic that distinguishes Big Data from other ("small data") datasets. Because Big Data corpora are often generated automatically, the question of the quality or trustworthiness of the data ("veracity") is crucial. "Velocity" refers to "the speed at which corpora of data are being generated, collected and analyzed".[5] The term "variety" denotes the many types of data and data sources from which data can be collected, including Internet browsers, social media sites and apps, cameras, cars, and a host of other data-collection tools.[6] Finally, if all previous features are present, a Big Data corpus likely has significant "value".

3 The way in which "Big Data" is generated and used can be separated into two phases.[7]

4 First, the creation of a Big Data corpus requires processes to collect data from sources such as those mentioned in the previous paragraph. Second, the corpus is analysed, a process that may involve Text and Data Mining (TDM).[8] TDM is a process that uses an Artificial Intelligence (AI) algorithm. It allows the machine to learn from the corpus—hence the term "machine learning" (ML) is sometimes used as a synonym of AI in the press.[9] As it analyses a Big Data corpus, the machine *learns and gets better at what it does.* This process often requires human input to assist the machine in correcting errors or faulty correlations derived from, or decisions based on, the data.[10] This processing of corpora of Big Data is done to find correlations and generate predictions or other valuable analytical outcomes. These correlations and

* Dr. Gervais is Professor of Information Law at the University of Amsterdam and the Milton R. Underwood Chair in Law at Vanderbilt University. The author is grateful to Drs. Balász Bodó, João Quintais, and to Svetlana Yakovleva of the Institute for Information Law (IViR), to participants at the University of Lucerne conference on Big Data and Trade Law (November 2018), to Ole-Andreas Rognstad and other participants at the Data as a Commodity workshop at the University of Oslo (December 2018), and to the anonymous reviewers at JIPITEC for most useful comments on earlier versions of this Article.

1 The Article considers IP rights applied by all or almost all countries, namely those contained in the Agreement on Trade-related Aspects of Intellectual Property Rights, Annex 1C of the Agreement Establishing the World Trade Organization, 15 April 1994. As of January 2019, it applied to the 164 members of the WTO, including all EU member States and the EU itself.

2 This use of the term "corpus" in this context is an extension of its original meaning as either a "body or complete collection of writings or the like; the whole body of literature on any subject", or the "body of written or spoken material upon which a linguistic analysis is based". Oxford English Dictionary Online (accessed 21 December 2018).

There is a debate about the proper form of the plural. Both Oxford and Merriam-Webster indicate that "corpora" is the proper form, although the author has encountered the form "corpuses" in the literature discussing Big Data. See e.g., the 2014 White House report to the President from the President's Council of Advisors on Science and Technology titled "Big Data and Privacy: A Technological Perspective", at x. "Corpora" is the form chosen here, although the predicable future is that the perhaps more intuitive form "corpuses" will win this linguistic tug-of-war.

3 For example, AI systems can create correlations between trademark features (look, sound etc.) and their appeal, thus allowing the creation and selection of "better" marks.

4 Jenn Cano, 'The V's of Big Data: Velocity, Volume, Value, Variety, and Veracity', XSNet (March 11, 2014), <https://www.xsnet.com/blog/bid/205405/the-v-s-of-big-data-velocity-volume-value-variety-and-veracity> (accessed 10 December 2018).

5 Ibid.

6 The list includes "cars" as cars as personal vehicles are one of the main sources of (personal) data—up to 25 Gigabytes per hour of driving. The data are fed back to the manufacturer. See Uwe Rattay, 'Untersuchung an vier Fahrzeugen - Welche Daten erzeugt ein modernes Auto?', ADAC, <https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx> (accessed 11 December 2018).

7 The two components are not necessarily sequential. They can and often do proceed in parallel.

8 See Maria Lillà Montagnani, 'Il text and data mining e il diritto d'autore' (2017) 26 AIDA 376.

9 Cassie Kozyrkov, 'Are you using the term 'AI' incorrectly?', Hackernoon (26 May 2018), <https://hackernoon.com/are-you-using-the-term-ai-incorrectly-911ac23ab4f5>.

10 How IP will apply to the work involved in the human training function of machine learning is one of the interesting questions at the interface of Big Data and IP. The term "training data" is used in this context to suggest that the machine training is supervised (by humans). See Brian D Ripley, *Pattern Recognition and Neural Networks* (Cambridge: Cambridge University Press, 1996) 354.

insights can be used for multiple purposes, including advertising targeting and surveillance, though an almost endless array of other applications is possible. To take just one different example of a lesser known application, a law firm might process hundreds or thousands of documents in a given field, couple ML with human expertise, and produce insights about how they and other firms operate, for example in negotiating a certain type of transaction or settling (or not) cases.

5 A subset of machine learning known as *deep learning* (DL) uses neural network, a computer system modelled on the human brain.[11] This implies that any human contribution to the output of deep learning systems is "second degree". When considering the possible IP protection of outputs of such systems, this separation between humans and the output challenges core notions of IP law, especially authorship in copyright law and inventorship in patent law.

C. Framing the issues

6 ML and DL can produce high value outputs. Such outputs can take the form of analyses, insights, correlations, and may lead to automated (machine) decision-making. It can be expected that those who generate this value will try to capture and protect it, using IP law, technological measures and contracts. One can also expect competitors and the public to try to access those outputs for the same reason, namely their value.

7 How far should IP go to protect value generated by ML? The old adage that "if it is worth copying it is worth protecting" has long been discarded.[12] A more nuanced question to ask might be, do entities that collect, process and use Big Data *need IP incentives* or *deserve additional rewards* to do what they do. Is protecting Big Data corpora and their processing outputs comparable to providing an incentive for trees to grow leaves in the spring? Specifically, does the creation of incentives help generate *new or better* data corpora, analyses, and thus produce welfare increases, taking account of welfare losses that rights *in* Big Data might cause, such as increased transaction and licensing costs?

8 In many cases, Big Data corpora are protected by secrecy, a form of protection that relies on trade secret law combined with technological protection from hacking, and contracts. Deciding which IP rights may apply should thus distinguish Big Data corpora that are not publicly accessible (say the Google databases powering its search engine and adverting) and those that are. A secret corpus is often de facto protected against competitors due to its secrecy, meaning that competitors may need to generate a competitive corpus to capture market share.[13] A publicly available corpus, in contrast, must rely on erga omnes IP protection—if it deserves protection to begin with. Copyright protects collections of data; the sui generis database right (in the EU) might apply; and data exclusivity rights in clinical trial data may be relevant. All three are topics explored below.

9 The *outputs* of the processing of Big Data corpora may contain or consist of subject matter that facially could be protected by copyright or patent law. Big Data technology can be—and in fact is—used to create and invent. For example, a Big Data corpus of all recent pop music can find correlations and identify what may be causing a song to be popular. It can use the correlations to write its own music.[14]

10 The creation of (potentially massive amounts of) new literary and artistic material without direct human input will challenge human-created works in the marketplace. This is already happening with machine-written news reports.[15] Deciding whether machine-created material should be protected by copyright could thus have a profound impact on the market for creative works. If machine created material is copyright-free, machines will produce free goods that compete with paid ones, that is, those created by humans expecting a financial return. If the material produced by machines is protected by copyright and its use potentially subject to payment, this might level the commercial playing field between human and machine, but then who (which natural or legal person) *should* be paid for the computer's work? Then there will be border definition issues. Some works will be created by human and machine working together. Can we apply the notion of joint authorship? Or should we consider the machine-produced portion (if separable) copyright-free, thus limiting the protection to identifiably human-authored portions?

11 With "deep learning model, the algorithms can determine on their own if a prediction is accurate or not... through its own method of computing – its own 'brain', if you will" Brett Grossfeld, 'A simple way to understand machine learning vs deep learning', ZenDesk (18 July 2017), online: <https://www.zendesk.com/blog/machine-learning-and-deep-learning/>.

12 *University of London Press v University of London Tutorial Press*, [1916] 2 Ch. 601 at 610.

13 Thanks to Prof. Bernt Hugenholtz (Univ, of Amsterdam) for discussing this insight with me.

14 See Gaëtan Hadjeres & François Pachet, 'DeepBach: A steerable model for Bach chorales generation' (3 December 2016) 1, online: <https://arxiv.org/pdf/1612.01010v1.pdf>.

15 See Corinna Underwood, 'Automated Journalism – AI Applications at New York Times, Reuters, and other mediants', eMerj (22 June 2018, updated 29 November 2018), online: <https://bit.ly/2Q84BTV>.

11 If such major doctrinal challenges—each with embedded layers of normative inquiries—emerge in the field of copyright, Big Data poses existential threats in the case of patents. AI tools can be used to process thousands of published patents and patent applications and used to *expand the scope of claims in patent applications*. This poses normative challenges that parallel those enunciated above: who is the inventor? Is there a justification to grant an exclusive right to a machine-made invention? To whom? Then there are doctrinal ones as well. For example, is the machine-generated "invention" disclosed in such a way that would warrant the issuance of a patent?

12 It gets more complicated, however. If AI machines using patent-related Big Data can broaden claim scope or add claims in patent applications, then within a short horizon they could be able to *predict the next incremental steps in a given field of activity* by analysing innovation trajectories. For example, they might look at the path of development of a specific item (car brakes, toothbrushes) and "predict" or define a broad array or what *could* come next. Doctrinally, this raises questions about inventive step: If a future development is obvious to a machine, is it obvious for purposes of patent law? Answering this question poses an epistemological as well as a doctrinal challenge for patent offices. The related normative inquiry is the one mentioned above, namely whether machine-made inventions (even inventions the scope [claims] of which were merely "stretched" using Big Data and AI) "deserve" a patent despite their obviousness (to the machine).

13 This use of patent and technological Big Data could lead to a future where machines pre-disclose incremental innovations (and their use) in such a way that they constitute publicly available prior art and thus make obtaining patents impossible on a significant part of the current patentability universe. Perhaps even the best AI system using a Big Data corpus of all published patents and technical literature will not be able to predict the next pioneer invention, but very few patents are granted on ground-breaking advances. AI systems that can predict *most* currently patented inventions, (which tend to be only incrementally different from the prior art) would wreak havoc with the patent-based incentive system.[16]

14 Let us take an example. It is possible that deep-learning algorithms could parse thousands of new molecules based on those recently patented or disclosed (in applications) and even predict their medical efficacy. If such data (new molecules and predicted efficacy) were available and published, it would significantly hamper the patentability of those new molecules due to lack of novelty.

15 The unavailability of patents would dramatically increase the role of data exclusivity rights (the right to prevent reliance in clinical data submitted to obtain marketing approval) in the pharmaceutical field.[17] If this prediction of future inventions by AI became an established practice in fields where this (separate) protection by data exclusivity is unavailable, the very existence of the incentive system based on patents could be in jeopardy.

16 In the pages that follow, the Article takes a deeper look at each of these challenges and draws the contours of possible answers.

D. Copyright

17 Let us get an easy point out of the analytical picture at the outset: the human-written (AI) software used to collect (including search and social media apps), store and analyse Big Data corpora is considered a literary work eligible for copyright protection, subject to possible exclusions and limitations.[18] The analysis that follows focuses on the harder question of the protection of the *Big Data corpora* and of the *outputs* generated from the processing of such corpora.

18 Before we delve more deeply into the interface between Big Data and copyright, it is necessary briefly to review briefly a fundamental element of copyright law, namely originality.

I. The Key Role of Originality

19 The main international instrument in the field of copyright is the Berne Convention, to which 176 countries were party as of January 2019.[19] That

16 See Shlomit Yanisky Ravid & Xiaoqiong (Jackie) Liu, 'When Artificial Intelligence Systems Produce Inventions: An Alternative Model for Patent Law at the 3a Era' (2018) 39 Cardozo L Rev 2215, 2254; and Ted Baker, 'Pioneers in Technology: A Proposed System for Classifying and Rewarding Extraordinary Inventions' (2003) 45 Arizona L Rev 445.

17 See Daniel Gervais, 'The Patent Option' (*forthcoming*, North Carolina J. L. & Tech), available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3266580> (accessed 15 December 2018).

18 This is recognized for example in Article 10.1 of the TRIPS Agreement (note 1 above), which provides that "[c]omputer programs, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)".

19 Berne Convention for the Protection of Literary and Artistic Works, of 9 September 1886, last revised at Paris on 24 July 1971, and amended on September 28, 1979 [hereinafter Berne Convention]. On membership of the Berne Union (countries party to the Convention), see <http://www.wipo.

Convention protects "literary and artistic works", a term that the Convention only defines by providing a list of categories of "productions" (another undefined term) that fit into the literary and artistic categories.[20]

20 There is more to this story, however. A Committee of Experts meeting under the auspices of the World Intellectual Property Organization (WIPO), which administers the Berne Convention, concluded that, although this is not specified expressly in the text of the Convention, the only mandatory requirement for a literary or artistic work to be protected by the Convention is that it must be "original". To arrive at this conclusion, the Committee considered both the Convention's drafting history and the use of the expression "intellectual creation" in the Convention as a functional synonym of the term "work".[21] This also means that *no mandatory formality* may be required to obtain copyright protection.[22] The same statement, namely that the only applicable criterion is originality, can be made about EU law.[23]

21 The Convention contains important hints as to what constitutes an "original" work. In its Article 2, when discussing the protection of "collections", it states that "[c]ollections of literary or artistic works such as encyclopaedias and anthologies which, by reason of the *selection and arrangement of their contents*, *constitute intellectual creations* shall be protected *as such*, without prejudice to the copyright in each of the works forming part of such collections."[24] Selection and arrangement are exemplars of what copyright scholars refer to as "creative choices".[25] Creative choices need not be artistic or aesthetic in nature, but it seems they do have to be human.[26] Relevant choices are reflected in the particular way an author describes, explains, illustrates, or embodies his or her creative contribution. In contrast, choices that are merely routine (e.g. the choice to organize a directory in alphabetical order) or significantly constrained by external factors such as the function a work is intended to serve (e.g. providing accurate driving directions), the tools used to produce it (e.g. a sculptor's marble and chisel), and the practices or conventions standard to a particular type of work (e.g. the structure of a sonnet) are not creative for the purpose of determining the existence of a sufficient degree of originality.

22 When the Berne Convention text was last revised on substance in 1967,[27] neither publicly available "electronic" databases nor any mass-market database software was available. The "collections" referred to in the Convention are thus of the type mentioned by the Convention drafters: (paper-based) anthologies and encyclopaedias. The negotiators' objective was to create a separate copyright for the maker (or "arranger") of a collection, knowing that most if not all of the entries in the collection (say, an encyclopaedia) were written by third parties, each an expert in her or his own field and each entitled to his or her own copyright in the entry. In a collection of this type, there are thus two layers of copyright; first, a right in each entry, and in each illustration or photograph, which is either transferred or licensed to the maker or publisher of the collection; and, second, a copyright in what one might call the "organizational layer", granted to the maker of the collection based on the "selection or arrangement" of the individual entries, photographs and illustrations. The second layer—the collection such as encyclopaedia—is generally treated as a collective work.[28]

int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15>.

20 Ibid art. 2. The term "production" seems to refer to the fact that a work must be objectified to be protected, that is, a work is not a work if it only exists in the mind of an author. See Ivan Cherpillod, *L'Objet du Droit d'Auteur* (Centre du Droit de l'Entreprise de l'Université de Lausanne, 1985) 35-41.

21 See WIPO Committee of Experts on Model Provisions for Legislation in the Field of Copyright, First Session, document CE/MPC/I/3, of March 3, 1989, at 16; and Memorandum prepared for the WIPO Committee of Experts on Model Provisions for Legislation in the Field of Copyright, document CE/MPC/I/2-III of Oct. 20, 1988, at 10.

22 See Jane C. Ginsburg, '"With Untired Spirits and Formal Constancy": Berne Compatibility of Formal Declaratory Measures to Enhance Copyright Title-Searching' (2013) 28:3 Berkeley Technology LJ 1584-1622. Countries are allowed to impose a second requirement, namely fixation. Berne Convention, art. 2(2).

23 Football Dataco, CJEU 1 March 2012, C-604/10, para. 40. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [hereinafter "Database Directive"]. Recital 16 of the Database Directive, for example, notes "no criterion other than originality in the sense of the author's intellectual creation should be applied to determine the eligibility of the database for copyright protection, and in particular no aesthetic or qualitative criteria should be applied". See also Daniel Gervais and Estelle Derclaye, 'The Scope of Computer Program Protection after SAS: Are We Closer to Answers?' (2012) 34:8 EIPR 565

24 Berne Convention (n 11) art. 2(5) (emphasis added).

25 See Daniel Gervais and Elizabeth Judge, 'Of Silos and Constellations: Comparing Notions of Originality in Copyright Law' (2009) 27:2 Cardozo Arts & Entertainment LJ 375.

26 Deciding whether Big Data corpora are protectable in the absence of an identifiable human author would be the subject of a separate analysis, well beyond the scope of this paper. Suffice it to say that views differ. Contrast s. 9(3) and 178 of the CDPA with this statement from the United States Copyright Office: "Examples of situations where the Office will refuse to register a claim include: [...] The work lacks human authorship". United States Copyright Office, Compendium of U.S. Copyright Office Practices, (3rd edition, 2017) 22.

27 An Appendix for developing countries was added in Paris in 1971 but it did not modify the definition of "work".

28 For example, section 101 of the US Copyright Act (Title 17

II. Application to Big Data

23 When "electronic" databases started to emerge in the 1990s, data generally had to be indexed and re-indexed regularly to be useable. The TRIPS Agreement (signed in 1994 but essentially drafted in the late 1980s up to December 1990), is a reflection of this development.[29] Using language meant to parallel art. 2(5) of the Berne Convention, it states that:

> *Compilations of data or other material, whether in machine-readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself.*[30]

24 The data in typical (relational or "SQL") databases in existence in the 1990s generally was "structured" in some way, for example via an index, and that structure might qualify the database for (thin) copyright protection in the database's organizational layer. Older databases also contained more limited datasets ("small data").

25 Facebook, Google, and Amazon, to name just those three, found out early on that relational databases were not a good solution for the volumes and types of data that they were dealing with. This inadequacy explains the development of open source software (OSS) for Big Data: the Hadoop file system, the MapReduce programming language, and associated non-relational ("noSQL") databases such as Apache's Cassandra.[31] These tools and the corpora they helped create and use may not qualify for protection as "databases" under the SQL-derived criteria mentioned above. This does not mean that no work or knowhow is required to create the corpus, but that the type of structure of the dataset may not qualify. As the CJEU explained in *Football Dataco*,

> *[S]ignificant labour and skill of its author, as mentioned in section (c) of that same question, cannot as such justify the protection of it by copyright under Directive 96/9, if that labour and that skill do not express any originality in the selection or arrangement of that data.*[32]

26 Indeed, Big Data is sometimes defined in *direct contrast* to the notion of SQL database and reflected in the TRIPS Agreement (and the EU database directive discussed in the next section). A McKinsey report, for example, notes that "Big Data" referred to "datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyse."[33] Those data are often generated automatically but at times less so, as when Google scanned millions of books for its massive book scanning project.[34] This was a most ambitious project but copyright "got in the way", especially for access to the corpus outside the United States:

> *Google's idea was to digitize as many published works as possible in as many languages as possible for the purpose of creating a universal digital library made up all printed books from every culture. The problem is that books are intellectual property, and intellectual property laws, cultures, and practices are not uniform around the world.*[35]

27 Big Data software is unlikely to "select or arrange" the data in a way that would meet the originality criterion and trigger copyright protection. In the *Google Books* case, the database basically consists of word-searchable scans of the books. From a copyright standpoint, therefore, it is doubtful whether a Big Data corpus of this sort, or a "dump" of, say, personal data scraped from online search engines or social media sites, would benefit from copyright protection. Hacking and other methods of unauthorised access to such corpora might be better handled via computer crimes and torts.

28 An argument has been made that tables or other outputs (such as analysis results generated by a TDM system) can be protected by copyright. An example

of the United States Code) defines "collective work" as "a work, such as a periodical issue, anthology, or encyclopedia, in which a number of contributions, constituting separate and independent works in themselves, are assembled into a collective whole".

29 For a longer description of the negotiating history, see Daniel Gervais, *The TRIPS Agreement: Drafting History and Analysis* (4th ed) (Sweet & Maxwell, 2013).

30 TRIPS Agreement (n 1) art. 10.2 (emphasis added). A difference between Berne and TRIPS that need not be belaboured here but is worth noticing is the different conjunction used between "selection" and "arrangement". Emphasis added. See also s. 3A of the Copyright, Designs and Patents Act 1988 (CDPA).

31 See April Reeve, 'Big Data and NoSQL: The Problem with Relational Databases' (7 September 2012), available at <https://infocus.dellemc.com/april_reeve/big-data-and-nosql-the-problem-with-relational-databases/> (accessed 18 November 2018). It is worth noting that it is because code is protected by copyright (see TRIPS Agreement, art. 10(1)), that owners of code can license it and impose open source terms.

32 Football Dataco (n 15) para 42.

33 James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, and Angela Hung Byers, Big Data: The next frontier for innovation, competition, and productivity, at 1, (McKinsey, 2011), available at <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx>.

34 See books.google.com. See also Daniel Gervais, 'The Google Book Settlement and the TRIPS Agreement' [2011] Stanford Tech LR 1.

35 Lyombe Eko, Anup Kumar, Qingjiang Yao, 'To Google or Not to Google: The Google Digital Books Initiative and the Exceptionalist Intellectual Property Law Regimes of the United States and France' (2012) 15 J Internet L 12, 13–14.

often mentioned in this context is the controversial car valuation database case concerning the catalogue of used car prices known as the *RedBook* in the United States.[36] The US Court of Appeals for the Second Circuit found that a collection of prices of used cars based on an algorithm factoring in age, mileage, model, etc. could benefit from protection.[37] The court's opinion "seems quite artificial and not directed to preserving the creativity and ingenuity inherent in any view of creative authorship."[38] It obscures the principle that ideas are not protected by copyright, an internationally recognized principle.[39] Moreover, even if that case is still good law, the question whether machine-created productions can qualify as copyright works is either still open, or resolved in favour of a need for human authorship.[40]

29 An interesting argument has been put forward by Harvard law professor Ruth Okediji for a different role for copyright in this context. She asserts that governments could claim protection of data-driven innovation to allow them to "develop appropriate conditions that ensure that more members of the public have access to any new works created."[41] The purpose would be to ensure that "free or heavily subsidized access to Big Data is available to the broader public at marginal cost or not much more."[42]

This idea resembles the General Public License (GPL) model, which uses copyright licenses to maintain the "open" nature of computer code based on previous open source software.[43] Indeed, OSS has been critical in shaping the technology that supports Big Data.[44]

30 Finally, it is worth noting that, in some jurisdictions, even absent copyright protection for Big Data, other IP-like remedies might be relevant, such as the tort of misappropriation applicable to "hot news" in US law, or the protection against parasitic behaviour available in a number of European systems.[45] This might apply to information generated by AI-based TDM systems that have initially high but fast declining value, such as financial information relevant to stock market transactions, as data "has a limited lifespan--old data is not nearly as valuable as new data--and the value of data lessens considerably over time".[46]

III. The Sui Generis Database Right

31 In EU law, there is also a *sui generis* right in databases.[47] This right is not subject to the originality requirement.[48] The Directive refers to the database maker's investment in "obtaining, verification or presentation of the contents" and then provides a right "to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."[49] The directive also mentions in its recitals that a database includes "collections of independent works, data or other materials which are *systematically or methodically arranged* and can be individually accessed."[50] This, according to Professor Bernt Hugenholtz, "squarely rules out protection –

36 See eg Peter DiCola et al., 'Legal Problems in Data Management: IT & Privacy at the Forefront: "Big Data": Ownership, Copyright, and Protection' [2015] John Marshall J. Information Technology & Privacy L, 565, at 576.

37 CCC Info. Servs., Inc. v. Maclean Hunter Mkt. Reports, 44 F.3d 61 (2d Cir.1994).

38 C.D. Freedman, 'Should Canada Enact A New Sui Generis Database Right?' (2002) 13 Fordham Intell. Prop. Media & Ent. LJ 35, 85.

39 See TRIPS Agreement, art. 9(2).

40 The US Copyright Office, for example takes that view, See United States Copyright Office. Compendium of U.S. Copyright Office Practices, 3rd edition (2017) at 3-4. See Amir H. Khoury, 'Intellectual Property Rights for "Hubots": On the Legal Implications of Human-Like Robots as Innovators and Creators' (2017) 35 Cardozo Arts & Ent. LJ 635, 665. For an older but potentially still relevant article on the same topic, see Daniel Gervais, 'The Protection Under International Copyright Law of Works Created with or by Computers', (1991) 5 IIC Int'l Rev. Ind'l Prop. and Copyright Law, 629, 644-45. For a critique, see Shlomit Yanisky-Ravid, Luis Antonio Velez-Hernandez, 'Copyrightability of Artworks Produced by Creative Robots and Originality: The Formality-Objective Model' (2018) 19 Minn. J L Science & Tech. 1. A recent proposal suggests applying the work-made-for-hire doctrine for AI works so that the human operating the AI system would be the author under US law. See Shlomit Yanisky Ravid and Samuel Moorhead, 'Generating Rembrandt: Artificial Intelligence, Accountability and Copyright -The Human-Like Workers are Already Here - A New Model' [2017] Michigan State LR 659.

41 Ruth L. Okediji, 'Government as Owner of Intellectual Property? Considerations for Public Welfare in the Era of Big Data' (2016) 18 Vanderbilt J Entertainment and Technology L 331, 361.

42 Ibid.

43 "The distributor of a GPL-licensed work, for example, must make the source code of that work available under the terms of the GPL". Eli Greenbaum, 'Open Source Semiconductor Core Licensing' (2011) 25 Harvard J L & Tech. 131, 139.

44 David J. Kappos, 'Open Source Software and Standards Development Organizations: Symbiotic Functions in the Innovation Equation' (2017) 18 Columbia Science & Technology LR 259, 261. Mr, Kappos is the former head of the United States Patent and Trademark Office.

45 See Victoria Smith Ekstrand and Christopher Roush, 'From "Hot News" to "Hot Data": The Rise of "FinTech", the Ownership of Big Data, and the Future of the Hot News Doctrine' (2017) 35 Cardozo Arts & Entertainment LJ 303.

46 D. Daniel Sokol & Roisin Comerford, 'Antitrust and Regulating Big Data' (2016) 23 George Mason LR. 1129, 1138.

47 Database Directive (n 19). See also Daniel Gervais, 'The Protection of Databases' (2007) 82:3 Chicago-Kent LR 1101.

48 See P Bernt Hugenholtz, 'Intellectual Property and Information Law' in Jan J.C. Kabel and Gerard J.H.M. Mom (eds.), *Essays in Honour of Herman Cohen Jehoram* (The Hague/London/Boston: Kluwer Law International 1998) 183-200.

49 Directive (n 22), art 7(1).

50 Ibid, recital 7.

whether by copyright or by the sui generis right – of (collections of) raw machine-generated data."[51] The use of noSQL technologies may mean that Big Data corpora are not protected by the sui generis right. It also seems fair to say that the machine produced outputs (such as new data corpora) based on analyses of Big Data are neither "obtained" nor "collected"; they are generated by the machine. This would seem to leave them unprotected by the sui generis right.

32 The Database Directive also mentions, however, that if there is an *investment* in obtaining the data, that investment may be sufficient for the corpus to qualify as a database.[52] "Recitals 10-12 preceding the Directive illustrate that the principal reason for introducing the sui generis right was to promote investment in the (then emerging) European database sector".[53] If the directive were applied to Big Data corpora, then crawling through the data might constitute prohibited "extraction" unless it was minimal.[54]

33 While this matter cannot be fully investigated here, there are serious doubts about the power of this argument to justify the application of the directive to Big Data corpora. The Court of Justice of the European Union defined "investment" in obtaining the data as "resources used to seek out existing materials and collect them in the database but does not cover the resources used for the creation of materials which make up the contents of a database."[55] Professor Hugenholtz explained that "the main argument for this distinction, as is transparent from the decision, is that the Database Directive's economic rationale is to promote and reward investment in database production, not in generating new data".[56] This casts doubt on whether the notion of investment is sufficient to warrant sui generis protection of Big Data corpora, though Matthias Leistner suggested caution in opining that the "the sweeping conclusion that all sensor- or other machine-generated data will typically not be covered by the sui generis right is not warranted".[57]

34 Arguably, indirect confirmation that "Big Data" corpora are protected neither by copyright nor by the sui generis right in database may be found in a Commission staff document accompanying a 2017 Communication from the Commission in which the idea was floated to create a data producer's right.[58] The Staff document noted that

> *"[T]he Database Directive did not intend to create a new right in the data. The CJEU thus held that neither the copyright protection provided for by the Directive nor the sui generis right aim at protecting the content of databases. Furthermore, the ECJ has specified that the investment in the creation of data should not be taken into account when deciding whether a database can receive protection under the sui generis right".*[59]

35 The idea of creating a new exclusive right in data was conspicuously absent in an April 2018 document on the creation of a "European data space".[60]

IV. Exceptions and Limitations for Big Data TDM

1. The need for exceptions and limitations

36 TDM software used to process corpora of Big Data might infringe rights in databases that are protected either by copyright or the EU sui generis right, thus creating a barrier to TDM.[61] The rule that *copyright works* reproduced in a Big Data corpus retain independent copyright protection has not been altered. This means that images, texts, musical works and other copyright subject-matter

51 P. Bernt Hugenholtz, 'Data Property: Unwelcome Guest in the House of IP', [2018] Kritika. Essays on Intellectual Property, vol. III. See also Estelle Derclaye 'The Database Directive', in Irini Stamatoudi and Paul Torremans (eds), *EU Copyright Law* (E. Elgar, 2014) 302-303.

52 Database Directive (n 12) art. 7(1).

53 Mark J. Davison & P. Bernt Hugenholtz, 'Football fixtures, horse races and spin-offs: The ECJ domesticates the database right' (2005) 27:3 EIPR 113, 116.

54 See Irini A. Stamatoudi, 'Text and Data Mining', in Irini A. Stamatoudi (ed.), *New Developments in EU and International Copyright Law* (Wolters Kluwer, 2016) 266.

55 *Fixtures Marketing Ltd v Oy Veikkaus Ab*, ECJ 9 November 2004, case C-46/02, ECR [2004] I-10396; *British Horseracing Board v William Hill Organization*, ECJ 9 November 2004, case C-203/02, ECR [2004] I-10415; *Fixtures Marketing Ltd v Svenska Spel AB*, ECJ 9 November 2004, case C-338/02, ECR [2004] I-10497; *Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP)*, ECJ 9 November 2004, case C-444/02, ECR [2004] I-10549.

56 Hugenholtz (n 27).

57 Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' (September 7, 2018). Available at SSRN: <https://ssrn.com/abstract=3245937>.

58 European Commission, 'Staff Working Document on the free flow of data and emerging issues of the European data economy', Brussels, 10 January 2017, SWD(2017) 2 final, 33-38. See also European Commission, 'Building A European Data Economy', Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 10 January 2017, COM(2017) 9 final, 13.

59 Ibid. p. 20.

60 See Communication from the Commission to the European Parliament, The Council, the European Economic and Social Committee and the Committee of the Regions, "Towards a common European data space", COM(2018) 232 final, 25 April 2018.

61 See Daniel L. Rubinfeld & Michal S. Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339, 368.

contained in a Big Data corpus are still subject to copyright protection until the expiry of the term of protection. This second point is by far the one that has attracted the largest amount of attention. Geiger et al. opined that "[o]nly TDM tools involving minimal copying of a few words or crawling through data and processing each item separately could be operated without running into a potential liability for copyright infringement."[62] This might explain why several jurisdictions have introduced TDM limitations and exceptions.

37 Four examples should suffice to illustrate the point. The German Copyright Act contains an exception for the "automatic analysis of large numbers of works (source material) for scientific research" for non-commercial purposes.[63] A corpus may be made available to "a specifically limited circle of persons for their joint scientific research, as well as to individual third persons for the purpose of monitoring the quality of scientific research."[64] The corpus must also be deleted once the research has been completed.[65]

38 France introduced an exception in 2016 allowing reproduction, storage and communication of "files created in the course of TDM research activities."[66] The reproduction must be from lawful sources.[67]

39 The UK statute provides for a right to make a copy of a work "for computational analysis of anything recorded in the work," but prohibits, however, dealing with the copy in other ways and makes contracts that would prevent or restrict the making of a copy for the purpose stated above unenforceable.[68]

40 Finally, the Japanese statute contains an exception for the reproduction or adaptation of a work to the extent deemed necessary "the purpose of information analysis ('information analysis' means to extract information, concerned with languages, sounds, images or other elements constituting such information, from many works or other much information, and to make a comparison, a classification or other statistical analysis of such information."[69]

2. Designing Big Data/TDM exceptions

41 The examples in the previous paragraphs demonstrate a similar normative underpinning, namely a policy designed to allow TDM of data contained in copyright works. They disagree on the implementation of the policy, however. Based on those examples, the questions that policy-makers considering enacting an explicit TDM exception or limitation should include:

- Whether the exception applies to only one (reproduction) or all rights (including adaptation/derivation);
- Whether contractual overrides are possible;
- Whether the material used should be from a lawful source;
- What dissemination of the data, if any, is possible; and
- Whether the purpose of TDM is non-commercial.

42 The answers to all five questions can be grounded in a normative approach, but they should be set against the backdrop of the three-step test, which, as explained below, is likely to apply to any copyright exception or limitation.

43 Before taking a look at the five points in greater detail, it is worth recalling that there are other types of exceptions that might allow TDM in specific instances, such as general exceptions for scientific research and fair use.[70]

44 As to the first question, if allowing TDM is seen as a normatively desirable goal, then the right holder should not be able to use one right fragment in the bundle of copyright rights to prevent it. In an analysis of rights involved, Irini Stamatoudi came

62 Christophe Geiger, Giancarlo Frosio & Oleksandr Bulayenko, 'Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data' (2018) 49:7 EIPR 814, 818.

63 Copyright Act of 9 September 1965 (Federal Law Gazette I, p. 1273), as last amended by Article 1 of the Act of 1 September 2017 (Federal Law Gazette I p. 3346), art. 60d. Available at <https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html>.

64 Ibid.

65 Ibid.

66 Geiger et al. (n 51) 830.

67 Law No. 2016-1231§ for a Digital Republic and art. L122-5 of the Intellectual Property Code.

68 Added by the Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations 2014, 2014 No. 1372. Online <https://www.legislation.gov.uk/uksi/2014/1372/regulation/3/made>.

69 Copyright Law of Japan, art. 47*septies*, translated by Yukifusa Oyama et al., available at <http://www.cric.or.jp/english/clj/doc/20161018_October,2016_Copyright_Law_of_Japan.pdf>.

70 An example of the former may be found in arts. 5(3)(a) and 6(2)(b) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, O.J. L 167, 22/06/2001 P. 0010 – 0019('InfoSoc Directive').

to the conclusion that right fragments beyond reproduction and adaptation were much less relevant.[71] Still, it would seem safer to formulate the exception or limitation as a non-infringing *use*, as in section 107 (fair use) of the US Copyright Act for example.[72]

45 Second, for the same reason, contractual overrides should not be allowed. One can hardly see how they can be effective unless perhaps there was only one provider of TDM for a certain type of work. Even if a provision against contractual overrides was absent from the text of the statute, the restriction could be found inapplicable based on principles of contract law.[73]

46 Third, the lawful source element contained in French law is facially compelling. It seems difficult to oppose a requirement that the source of the data be legitimate. There are difficulties in its application, however. First, it is not always clear to a *human* user whether a source is legal or not; the situation may be even less clear for a machine. Second, and relatedly, if the source is foreign, a determination of its legality may require an analysis of the law of the country of origin, as copyright infringement is determined based on the *lex loci delicti*—and this presupposes a determination of its origin (and foreignness) to begin with. Perhaps a requirement targeting sources that the user *knows or would have been grossly negligent in not knowing* were illegal might be more appropriate.[74]

47 The last two questions on the list above are somewhat harder. Dissemination of the data, if such data includes copyright works, could be necessary among the people interested in the work. German law makes an exception for a "limited circle of persons for their joint scientific research", and "third persons for the purpose of monitoring the quality of scientific research."[75] This is a reflection of a scientific basis of the exception, which includes project-based work by a limited number of scientists and monitoring by peer reviewers. This would not allow the use of TDM to scan libraries of books and make snippets available to the general public, as Google Books does, for example. An interpretation of the scope of the exception might depend on whether the use is commercial, which in turn might vary according to the definitional approach taken: is it the commercial nature of the *entity* performing the TDM that matters, or the specific use of the TDM data concerned (i.e., is that specific use monetized)?

48 As of early 2019, the EU was considering a new, mandatory TDM exception as part of its digital copyright reform efforts.[76] Article 3, which contains the proposed TDM exception, has been the focus of intense debates. The September 2018 (Parliament) version of the proposed TDM exception maintains the TDM exception for scientific research proposed by the Commission but adds an optional exception applicable to the private sector, not just for the benefit of public institutions and research organisations.[77] Members of the academic community have criticised the narrow scope of the Commission's proposed exception, which the Parliament's amendments ameliorated.[78] The European Copyright Society opined that "data mining should be permitted for non-commercial research purposes, for research conducted in a commercial context, for purposes of journalism and for any other purpose".[79]

49 One should note, finally, that when a technological protection measure or "lock" such as those protected by art. 11 of the 1996 WIPO Copyright Treaty, is in place preventing the use of data contained in copyright works for TDM purposes, the question is whether a TDM exception provides a "right" to perform TDM and thus potentially a right to circumvent the TDM or obtain redress against measures designed to restrict it.[80] This might apply to traffic management (e.g., throttling) measured used to slow the process down. Those questions are worth pondering, but they are difficult to answer, especially at the international level.[81]

71 Stamatoudi (n 32) 262.

72 The US Copyright Act (17 USC s 107) reads in part as follows: "the fair use of a copyrighted work ... is not an infringement of copyright".

73 See for example Lucie Guibault's detailed analysis of the possible application of the German *Sozialbinding* principle in this context. Lucie M.C.R. Guibault, *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright* (Kluwer Law International, 2002) 224-225.

74 This language echoes footnote 10 (to art. 39(2)) of the TRIPS Agreement (n 1).

75 See n 54.

76 Geiger at al. (n 51) 832-33.

77 The Parliamentary version and the Commission's proposal are compared in amendments 64 and 65 of the document 'Amendments adopted by the European Parliament on 12 September 2018 on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market' (COM(2016)0593 – C8-0383/2016 – 2016/0280 (COD)) (1), online: <https://bit.ly/2SS3HYA>.

78 See e.g. Martin Senftleben, 'EU Copyright Reform and Startups – Shedding Light on Potential Threats in the Political Black Box' (undated), at p. 9. Online: <https://bit.ly/2kiJgFq>.

79 European Copyright Society, General Opinion on the EU Copyright Reform Package, 24 January 2017. Online: <https://bit.ly/2k2k3jD>.

80 WIPO Copyright Treaty, 20 Dec. 1996.

81 For a brief discussion, see Geiger at al. (n 51) 836-838.

3. Application of the Three-Step Test

50 The three-step test sets boundaries for exceptions and limitations to copyright rights.

51 The original three-step test is contained in art. 9(2) of the Berne Convention. Its purpose is to allow countries party to the Convention to make exceptions to the right of reproduction (1) "in certain special cases", (2) "provided that such reproduction does not conflict with a normal exploitation of the work", and (3) "does not unreasonably prejudice the legitimate interests of the author".[82] The test was extended to all copyright rights by the TRIPS Agreement, with the difference that the term "author" at the end was replaced with the term "right holder".[83]

52 The test was interpreted in two panel reports adopted by the World Trade Organization's Dispute-Settlement Body.

53 The first step ("certain special cases") was interpreted to mean that "an exception or limitation must be limited in its field of application or exceptional in its scope. In other words, an exception or limitation should be narrow in quantitative as well as a qualitative sense".[84] The Study Group discussed the possible inclusion of the test in the Berne Convention before the 1967 (Stockholm) revision had opined that the test should require that any exception to the right of reproduction be "for clearly specified purposes".[85]

54 The normative grounding to justify a TDM exception is fairly clear. Indeed, exceptions and limitations have already been introduced in major jurisdictions. A well-justified exception or limitation with reasonable limits and a clear purpose is likely to pass the first step.

55 The second step (interference with normal exploitation) was defined as follows. First, exploitation was defined as any use of the work by which the copyright holder tries to extract/maximize the value of her right. "Normal" is more troublesome. Does it refer to what is simply "common", or does it refer to a normative standard? The question is particularly relevant for new forms and emerging business models that have not, thus far, been common or "normal" in an empirical sense. At the revision of the Berne Convention in Stockholm in 1967, the concept was used to refer to "all forms of exploiting a work, which have, or are likely to acquire, considerable economic or practical importance".[86] In other words, if the exception is used to limit a commercially significant market or, a fortiori, to enter into competition with the copyright holder, the exception is prohibited.[87]

56 Could a TDM exception be used to justify scanning and making available entire libraries of books still under active commercial exploitation? The answer is negative, as this would interfere with commercial exploitation. For books still protected by copyright *but no longer easily available on a commercial basis*, the absence of active commercial exploitation would likely limit the impact of the second step, however, subject to a caveat. Some forms of exploitation are typically done by a third party under license and do not need any active exploitation *by the right holder*. For example, a film studio might want the right to make a film out of a novel no longer commercially exploited. That may in turn generate new demand for the book. This is still normal exploitation. One must be careful in extending this reasoning too far, for example, and assume that every novel will be turned into a movie.

57 TDM is quite comparable to the not adaptation of a novel to the big screen. Its purpose is *not* to convey the same or similar expressive creativity via a different medium. TDM is looking, if anything, for *ideas* embedded in copyright works. Because Big Data corpora used for TDM are necessarily composed of large numbers of works and other data, the TDM function cannot be performed if licensing work by work is required. This is also differs in the case of a film adaptation, a scenario in which it seems reasonable to expect that the author (or her representative) and the film producer might negotiate a license.

58 One way to pass the second step would be for a TDM exception to allow limited uses that do not demonstrably interfere with commercial exploitation, such as those allowed under the German

82 Berne Convention (n 11) art. 9(2).

83 TRIPS Agreement, art. 13. The test is now used as the model for exceptions to *all copyright rights* in TRIPS (art. 13); Articles 10(1) and (2) of the WIPO Copyright Treaty (20 December 1996); Article 16(2) of the WIPO Performances and Phonograms Treaty (also adopted on 20 December 1996); Article 13(2) of the Beijing Treaty on Audiovisual Performances (24 June 2012); and Article 11 of the Marrakesh Treaty to Facilitate Access to Published Works for Persons who are Blind, Visually Impaired or Otherwise Print Disabled (27 June 2013). Interestingly, in TRIPS, it is also the test for exceptions to industrial design protection (art. 26(2)) and patent rights (art. 30).

84 WTO Report of the Panel WT/DS160/R of 15 June 2000 on United States – Section 110(5) of the US Copyright Act, para 6.109 (emphasis added and citations omitted). [hereinafter "panel report"]. The second case led to the following panel report: WT/DS114/R of 17 March 2000 on Canada – Patent Protection of Pharmaceutical Products.

85 Records of the Intellectual Property Conference of Stockholm: June 11 to July 14, 1967 (WIPO, 1971) 112.

86 Ibid, at 112.

87 Paul Goldstein, *International Copyright: Principles, Law, and Practice* (OUP 1998) 295.

statute. Another example is the use of "snippets" from books scanned by Google for its Google Books project, which was found to be a fair use by the US Court of Appeals for the Second Circuit. This matters not just as a matter of US (state) practice but because at least the fourth fair use factor ("the effect of the use upon the potential market for or value of the copyrighted work") is a market-based assessment of the impact of the use resembling the three-step test's second step.[88] The Second Circuit noted that this did not mean that the Google Books project would have *no* impact, but rather that the impact would not be meaningful or significant.[89] It also noted that the type of loss of sale created by TDM "will generally occur in relation to interests that are not protected by the copyright. A snippet's capacity to satisfy a searcher's need for access to a copyrighted book will at times be because the snippet conveys a historical fact that the searcher needs to ascertain."[90] In the same vein, one could argue that the level of interference required to violate the second step of the test must be significant and should be a use that is relevant from the point of view of commercial exploitation.

59 The third step (no unreasonable prejudice to legitimate interests) is perhaps the most difficult to interpret. What is an "unreasonable prejudice", and what are "legitimate interests"? Let us start with the latter. "Legitimate" can mean sanctioned or authorized by law or principle. Alternatively, it can just as well be used to denote something that is "normal" or "regular". The WTO dispute-settlement panel report concluded that the combination of the notion of "prejudice" with that of "interests" pointed clearly towards a legal-normative approach. In other words, "legitimate interests" are those that are protected by law.[91]

60 Then, what is an "unreasonable" prejudice? The presence of the word "unreasonable" indicates that *some level or degree* of prejudice is justifiable. Hence, while a country might exempt the making of a small number of private copies entirely, it may be required to impose a compensation scheme, such as a levy, when the prejudice level becomes unjustified.[92] The WTO panel concluded that "prejudice to the legitimate interests of right holders reaches an unreasonable level if an exception or limitation causes or has the potential to cause an unreasonable loss of income to the copyright holder".[93]

61 Whether a TDM exception is liable to cause an unreasonable loss of income to copyright holders is analytically similar to the second step of the test as interpreted by the WTO panels. It is not, however, identical: The owner of rights in a work no longer commercially exploited may have a harder case on the second step. It is not unreasonable, however, for a copyright holder, to expect some compensation for use of a protected work even if it is not commercially exploited. For example, the owner of rights in a novel may expect compensation for the republication by a third party or translation of the book. The major difference between the second and third step in this regard is that the third step condition may be met by compensating right holders. This would allow the imposition of a compulsory license for specific TDM uses that overstep the boundary of free use, for example to make available significant portions of, or even entire, protected works that are no longer commercially exploited. For example a TDM engine could find all works that fit a user's criteria (say, 20th century novels, in any language, where a murder by poison takes place and both Pontius Pilate and a cat play a prominent part in the plot).[94] Then the system could (a) make the text or part thereof available, against adequate compensation, especially if no e-book database existed; or (b) generate a translation or summary if the book, especially if no linguistic version of use to the searcher was available.[95]

E. Patents

I. The role of Big Data in patent disclosures

62 The interface between patents and Big Data is interesting on several levels.

63 First, TDM might be used in enhancing the use of patent information.[96] The "patent bargain" is basically a fair disclosure of an invention in exchange for a limited monopoly on its use,

88 The fourth fair use factor contained in the US Copyright Act (17 USC s 101) reads as follows: "the effect of the use upon the potential market for or value of the copyrighted work."

89 *The Authors Guild v. Google, Inc.* 804 F.3d 202 (2d Cir, 2015), cert. denied 136 S.Ct. 1658.

90 Ibid.

91 Panel Report, paras 6.223–6.229. In para. 6.224 the Panel tried to reconcile the two approaches: "[T]he term relates to lawfulness from a legal positivist perspective, but it has also the connotation of legitimacy from a more normative perspective, in the context of calling for the protection of interests that are justifiable in the light of the objectives that underlie the protection of exclusive rights".

92 Records (n 72) 1145–46.

93 Panel Report (n 71) para. 6.229.

94 The reader will have recognized the unlikely plot of Mikhail Boulgakov's masterpiece, *Master and Margarita*.

95 The application of both the Berne Convention Appendix (for developing countries) and the Marrakesh VIP Treaty might also be considered in this context.

96 See Dario Mastrelia, 'Patent information and technology transfer in the information society era: From the current scenario to new business ideas' (2018) 40:7 EIPR 460.

especially on a commercial basis.[97] Unfortunately, patent information is often mired in a difficult language known as "patentese", which obscures the informational function of published patents.[98] An AI-capable TDM system might be able not just to find but also to *interpret* useful information and facilitate technology transfers.[99] Relatedly, AI and patent information could be combined not just to interpret patent claims but also to determine their validity.[100]

64 AI applications in this field already go further, however, and the trajectory of their development leads to some potentially remarkable conclusions. First, existing AI-based systems using Big Data (e.g. databases of published patents and technical literature) allow patent applicants to maximize the exclusivity claimed in their patent applications by identifying material analogous to the invention that can also be claimed—essentially variations on the theme of the invention—thus potentially broadening its scope *beyond what the applicant actually invented*.[101]

II. Big Data and the future of innovation

65 This section is admittedly at the border between current technology and the future. Part of it is thus speculation based on how current AI systems using patent corpora and AI are likely to evolve. Various options are considered. Hopefully, the reader will find some of it useful.

66 The kind of claim-broadening system described above can be used for a different purpose, namely to *disclose* (*without* claiming patent rights) incremental variations on claims of existing patents, thus potentially preventing patenting of improvements and even derivative and incremental inventions in the future.[102] Are AI-generated disclosures of variations on existing inventions or incremental innovations sufficient to defeat novelty?[103] If massive disclosures through AI-systems of incremental variations on existing patents become common, patent courts and offices might be tempted—for both institutional and normative reasons—to limit the patent-defeating power of such disclosures, for example by insisting that they do not sufficiently enable or describe the invention, which would remain patentable, therefore, when an application is filed by a (human) person providing a more complete disclosure. More neutral outcomes might be obtained in higher courts.

67 The discussion of the role of Big Data-based AI systems in innovation disclosures can be taken up a level. As Yanisky Ravid and Liu note:

> *AI systems create a wide range of innovative, new, and non-obvious products and services, such as medical devices, drug synthesizers, weapons, kitchen appliances, and machines, and will soon produce many others that, had they been generated by humans, might be patentable inventions under current patent law.*[104]

68 There is little doubt that Big Data-based AI systems will innovate, that is, they will produce what one might call "inventions". Indeed, Google's AI system, known as DeepMind, already thinks it does and it has filed patent applications.[105] The first question to ask in this context is whether such inventions are patentable. The second is, what will the broader impact on innovation be?

69 As noted in the introductory part, Big Data-based AI systems are more likely to generate incremental innovations than pioneer inventions. They could so, however, at a pace of innovation that could eclipse any previous period in human history, causing an exponential increase over the (already very fast) pace of current technological change.

97 The obligation to disclose is reflected in art. 29.1 of the TRIPS Agreement. See also Katherine J. Strandburg, 'What Does the Public Get? Experimental Use and the Patent Bargain' [2004] Wisconsin. LR 81, 111-17.

98 Sean B. Seymore, 'The Teaching Function of Patents' (2010) 85 Notre Dame LR 621, 633–34.

99 See Mastrelia (n 83) 465. It may also be useful to recall that art. 7 of the TRIPS Agreement mentions that "the transfer and dissemination of technology, to the mutual advantage of producers and users of technological knowledge and in a manner conducive to social and economic welfare, and to a balance of rights and obligations".

100 See Ben Dugan, 'Mechanizing Alice: Automating the Subject Matter Eligibility Test of Alice v. CLS Bank' [2018] U Illinois J L Tech & Policy 33.

101 See Ben Hattenbach, Joshua Glucoft, 'Patents in an Era of Infinite Monkeys and Artificial Intelligence' (2015) 19 Stanford Technology LR 32, 35, describing a company called CLOEM using "brute-force computing to mechanically compose text for thousands of patent claims covering potentially novel inventions and also to generate defensive publications to prevent others from obtaining patent protection in the same field".

102 See Ryan Abbott, 'I Think, Therefore I Invent: Creative Computers and the Future of Patent Law' (2016) 57 Boston College LR 1079, describing "projects such as "All Prior Art" and "All the Claims" which attempt to use machines to create and publish vast amounts of information to prevent other parties from obtaining patents".

103 Though there is no formal international test, typically this would require that the disclosure provide enough information for a person skilled in the art to make or practice the invention. For a discussion (under US law) see Jennifer L. Kisko and Mark Bosse, 'Enablement and Anticipation' (2007) 89 J Patent & Trademark Office Society 144, 151.

104 Yanisky Ravid and Liu (n 9), 2219-2220.

105 Mike James, 'Google's DeepMind Files AI Patents', i-programmer (11 June 2018) <https://bit.ly/2ATh5or>.

One company active in the field markets itself as creating "commercially relevant inventions at high speed and with great diversity" and notes that "[h]undreds of patents based on *our inventions* have been filed by some of the best-known technology companies worldwide".[106] If this type of technology continues to grow, as it surely will, we could reach a *singularity of innovation*.[107] The notion of "singularity" became well-known after the publication of Ray Kurtzweil's famous 2006 book on the topic.[108] The singularity, according to Kurzweil, will be a reality when computers become more "intelligent" than humans.[109]

70 An innovation singularity would compel a fundamental rethink of the innovation incentive system. From a first to disclose (and patent) system, one might need to consider a "first to develop" system. Such a system would lead to a series of both doctrinal and normative questions, including: whether any period of exclusivity is essential and then how long; who can apply; what period of time do they have to actually develop; and then develop what (proof of concept, actually marketable product, etc.); to which territory does it apply, and the list goes on.

71 The future might not take a public domain path (through massive disclosures) and opt for a proprietary route instead. Big Data based "inventions" reflecting the deep learning ability of AI systems might deserve protection by patents *even if no discernible human contribution to the inventive process has taken place*. The forces that might restrict the scope of novelty-destroying disclosures mentioned in the previous paragraphs might push back against a public domain trajectory and help grant patents even if the broader scope of claims in applications is the product of claim-broadening algorithms. This would mean that claims added or broadened by a Big Data based AI system to a patent application (and possibly entire new applications) might have to be granted to a person (natural or legal) for inventions that the applicant does not actually possess and is very possibly unable to exploit. Whether this occurs, in turn, might depend on the ability of the AI system to explain its invention.[110]

72 The impact of such a scenario might depend on how the market would react. If owners of patent rights in inventions they cannot exploit license them to companies that can exploit them, then private ordering might solve the otherwise massive blocking effect. The blocking effect could become a patent troll's dream, however, allowing the capture of vast areas of incremental innovation and thus exponentially expanding the reach of trolls in this space.[111]

73 As with copyright "authorship", one might fairly ask whether there must be human inventorship for a patent to be granted. No definitive answer can be given under current law, and a full analysis is beyond the scope of this Article. Divergences of views have emerged.[112] One might add that this

106 <http://www.iprova.com/about-us/> (accessed 21 January 2019).

107 See Ryan Abbott, 'I Think, Therefore I Invent: Creative Computers and the Future of Patent Law' (2016) 57 Boston Coll LR 1079, 1079–80 ("A creative singularity in which computers overtake human inventors as the primary source of new discoveries is foreseeable").

108 Ray Kurzweil, *The Singularity Is Near* (Viking, 2006). It seems, however, that the notion originated earlier. For example, it can be found Vernor Vinge, 'The Coming Technological Singularity: How to Survive in the Post-Human Era' (Winter 1993) *Whole Earth Review* (online <https://edoras.sdsu.edu/~vinge/misc/singularity.html>).

109 See ibid. Vinge also discussed the idea that those computers might somehow become "aware".

110 Explanation in this context is sometimes referred to as dumbing it down for humans to understand the machine's "thinking", or explaining "to a lay audience in such a way that they can make use of such explanations." Sandra Wachter et. al., 'Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR' (2018) 31 Harvard J L & Tech. 841, 851.

The problem is that the best AI insights may be the ones that the machine is least able to explain. For example, if a Big Data based AI system was excellent at diagnosing a certain disease, explanation might not be possible, but then I suspect that in such a case the value of excellent diagnostic capabilities would outweigh the need for an explanation.

111 A patent is blocking if "if circumventing it (1) is not commercially practicable, or (2) will not produce a commercially viable product". Ian Simmons, Patrick Lynch, Theodore H. Frank, '"I Know It When I See It": Defining and Demonstrating "Blocking Patents"' (2002) 16 Antitrust 48, at 49.

As professor Robert Merges noted, "patent law's property rule, which requires a voluntary patentee-infringer bargain or an injunction against infringement, assumes that if a bargain would benefit both parties, they will reach one". Robert Merges, 'Intellectual Property Rights and Bargaining Breakdown: The Case of Blocking Patents' (1994) 62 Tennessee LR 75, 78. That assumption is questionable. However, the problem that AI might cause may also be solved (in part) by AI by facilitating contacts between potential licensor and licensee (Thanks to Florent Thouvenin (University of Zurich) for this insight).

112 In the United States, though the law seems to require human inventive activity, the Patent Office (USPTO) has reportedly granted 'several patents with nonhuman inventors, albeit not explicitly and not necessarily with their knowledge". Russ Pearlman, 'Recognizing Artificial Intelligence (Ai) As Authors and Inventors Under U.S. Intellectual Property Law' (2018) 24 Richmond J.L. & Technology 2, 23. Normatively, "[t]he concept of an inventor does not fit neatly into scenarios in which the invention emerges from random interactions between existing computer programs, repeated computer simulations using all possible scenarios, or other forms of data mining, perhaps with little or no direction or forethought on the part of the human operator". Liza Vertinsky & Todd M. Rice, 'Thinking About Thinking Machines: Implications of Machine Inventors for

presupposes that one actually *knows* whether a human or a machine is the "inventor". If the patent applicant does not need to provide proof of human invention, perhaps courts will require it later on in infringement proceedings and invalidate patents for lack of (human) inventorship.

74 The last question in this section is whether there can be patents on AI systems themselves. International patentability criteria are contained in art. 27 of the TRIPS Agreement. This provision leaves World Trade Organization (WTO) members a fair degree of flexibility in determining what constitutes an "invention", and then whether such invention is new, involves an inventive step (or is non-obvious) and is industrially applicable (or useful).[113] The European Patent Office (EPO) issued new Examination Guidelines (in force November 2018) noting that "[a]rtificial intelligence and machine learning are based on computational models and algorithms for classification, clustering, regression and dimensionality reduction, such as neural networks, genetic algorithms, support vector machines, k-means, kernel regression and discriminant analysis", and that ["s]uch computational models and algorithms are *per se* of an abstract mathematical nature, irrespective of whether they can be 'trained' based on training data".[114] In the United States, algorithms are also essentially unpatentable since the US Supreme Court's decision in *Alice v. CLS Bank,* which imposed a two-part test that most computer programs are unlikely to pass.[115] The focus is now on the machine: "If the novel feature is the use of a computer, the patent will likely be invalid, while if the novel feature is a better computer, the patent will likely be valid."[116] The role of patents in protecting algorithms thus seems fairly narrow going forward.

III. Localization and working requirements

75 There is a final point, arguably tangential but nonetheless potentially relevant, to be made in connection with patents and Big Data. In 1995, when the TRIPS Agreement entered into force, rules were meant to limit or eliminate the so-called working requirements in patent law, which were legal under previous international rules.[117] This requirement was seen, in a number of (mostly developing) countries as a part of the patent bargain.[118] A patent, as defined in TRIPS, is a right to exclude not conditioned on either availability or manufacture or other use of the patented invention in the territories where a patent is in force.[119] Prior to TRIPS, certain countries imposed a (local) working requirement to make sure that patented inventions would be available (and the technology used) in the country. The TRIPS rationale is, in short, that companies should be able to produce patented inventions wherever they believe it is more efficient and export to other territories. Local working requirements parallels the current clash between personal data protection and (free) trade.

76 This is relevant to Big Data because a common form of personal data protection is *data localization*.[120] Is the assumption that free trade is a desirable normative goal applicable here? Cross-border data flow limits seem to be a pushing back against free trade.[121] This indirectly imposes a local "working requirement" on AI corpora containing personal data. If IP law is prologue, free trade (i.e. free cross-border data flows) will win that debate.

F. Data Exclusivity

77 There is a right often closely associated with patents for pharmaceuticals, namely the right of data exclusivity.[122] This is the right to prevent certain

Patent Law' (2002) 8 Boston Univ J Science & Tech L 574, 586.

113 See Carlos M. Correa, 'Public Health and Patent Legislation in Developing Countries' (2001) 3 Tulane J Technology and Intellectual Prop 1, 8-9.

114 European Patent Office, 'Guidelines for Examination' (Nov. 2018), sec. 3.3.1. Available at <https://www.epo.org/law-practice/legal-texts/html/guidelines2018/e/g_ii_3_3_1.htm>.

115 *Alice Corp. Pty. Ltd. v. CLS Bank Int'l* (2014).134 S. Ct. 2347, 2354-55.

116 Fabio E. Marino & Teri H. P. Nguyen, 'From Alappat to Alice: The Evolution of Software Patents' (2017) 9 Hastings Science & Tech LJ 1, at 28.

117 TRIPS entered into force on 1 January 1995. The principal set of substantive patent rules before TRIPS were contained in the Paris Convention for the Protection of Industrial Property, of March 20, 1883, last updated in Stockholm (1967), art. 5A.

For a discussion of the working requirement, see Bryan Mercurio & Mitali Tyagi, 'Treaty Interpretation in WTO Dispute Settlement: The Outstanding Question of the Legality of Local Working Requirements' (2010) 19 Minnesota J Intl L. 275, 279-288.

118 See Katherine J. Strandburg, 'What Does the Public Get? Experimental Use and the Patent Bargain' (2004) Wisconsin LR 81.

119 TRIPS (n 1), arts. 27(1) and 31.

120 For a (critical) discussion of national data localization practices, see Bret Cohen, Britanie Hall, Charlie Wood, 'Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy' (2017) 32 Antitrust 107.

121 See Svetlana Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"'? (2018) 17:3 World Trade Rev 477.

122 For a fuller discussion of this interface, see Daniel Gervais, 'The Patent Option' (2019) 20 North Carolina J L & Tech (forthcoming), draft available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3266580>.

forms of use of clinical trial data generated to obtain marketing approval for certain pharmaceuticals and chemical products. A basic data exclusivity right is contained in TRIPS.[123] More extensive protection is contained in post-TRIPS (in the so-called "TRIPS-Plus") agreements.[124] There is a concern that such protection might prevent the use of TDM tools, which is seen as a negative development because "it is the collected clinical trial data, and their ability to provide a large and comprehensive dataset, that are highly valuable, not the specific health and safety outcome proven by those data."[125]

78 This right is directly relevant. As discussed in the previous section, patents may become more difficult to obtain due to massive Big Data –based AI disclosures of possibly new incremental innovations. For example, such a system could conceivably disclose new molecules and predict their efficacy. In such a case, it would be near impossible to patent the drug unless patented by the user of the AI "inventor". If it was patented by the AI inventor, then that person's consent could be required to test the new molecule. In both cases the company investing in the testing might not own a patent on the molecule and find it hard to justify the expense of generating clinical test data. The data exclusivity right might fill that void. The right is, however, of limited application beyond the pharmaceutical and agrochemical fields.

G. Trade Secrets and Confidential Information

79 Let us end our *tour d'horizon* with the protection of confidential information, including the subset of confidential information known as trade secrets. Trade secrets and confidential information laws, and contracts, can be used to enable the orderly disclosure of information.[126] That protection is reflected in the TRIPS Agreement.[127] This type of protection of secrets information is compatible with, and often based on, legislation such as the Trade Secrets Directive and a host of national laws.[128]

80 What is the area of application of trade secret law to Big Data? Cristina Sappa analysed the application of trade secret law to data gathered via the Internet of Things (IoT).[129] She suggested three areas which seem to be worthy of further study.

81 First, "within the IoT realm, as in any other business, trade secrets are used to protect information to which access is traditionally limited thanks to (among others) confidentiality clauses or non-disclosure agreements."[130] Thus, trade secret and confidential information law—in this case with the support of contract law—could be used to protect data acquired for purposes of TDM.[131] Trade secret law typically works far better for business information than private data.[132] One might indeed expect the default contracts may not adequately protect the users or consumers—though privacy or consumer protection laws may impose limits on contractual freedoms that include minimum guarantees of confidentiality.[133]

82 Secondly, the protection of confidential information could apply to non-trivial "data coming from a machine-to-machine process".[134] One commentator suggested that "trade secrets, rather than database *sui generis* rights, are the most interesting and flexible property right for coping with the challenge of customer data appropriation in the new, collaborative economy 3.0".[135] For example, if a corpus of Big Data was processed to generate a database of correlations between persons and their preferences (but let us assume that such a database does not or no longer contains the data used to generate the correlations), the new corpus of correlations and insights derived from such correlations may well be protected as a

123 TRIPS Agreement (n 1) art 39(2).

124 See Peter K. Yu, 'Data Exclusivities in the Age of Big Data', Texas A&M Univ School of Law Legal Studies Research Paper-Series No. 18-08, at 5-8. Available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3133810>.

125 Ibid 4.

126 See Mark Lemley, 'The Surprising Virtues of Treating Trade Secret ad IP Rights' (2008) 61 Stanford LR 311.

127 TRIPS Agreement (n 1) art. 39.2.

EU law defines a trade secret as "valuable know-how and business information, that is undisclosed and intended to remain confidential" generated by businesses and non-commercial research institutions that "invest in acquiring, developing and applying know-how and information which is the currency of the knowledge economy and provides a competitive advantage". Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, recital 1.

128 Ibid.

129 Cristiana Sappa, 'What Does Trade Secrecy Have To Do with the Interconnection-Based Paradigm of the Internet of Things?' (2018) 40:8 EIPR 518.

130 Ibid 521.

131 TRIPS Agreement (n 1) art. 39.2.

132 Pamela Samuelson, 'Privacy as Intellectual Property?' (2000) 52 Stanford LR1125, 1151-70.

133 This would of course include the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.)

134 Sappa (n. 113) 523.

135 Gianclaudio Malgieri, '"Ownership" of Customer (Big) Data in the European Union: Quasi-Property As Comparative Solution?' (2016) 20 J Internet L 3.

trade secret or a database where it exists. Moreover, its use may no longer be limited by the personal data protection that applied to the raw data.

83 Thirdly, Sappa suggests we should consider the "possibilities of welfare gains by third parties, since this regime applying to *knowledge commons* such as the IoT enables spillovers, and therefore its presence may not necessarily be perceived as a bad thing."[136] Excessive restrictions on access to lock-in effects by major data gathering entities might have negative welfare impacts warranting governmental intervention in "data--driven platform markets characterized by strong network and lock--in effects--and in new technological contexts that might otherwise be ripe for competitive innovation."[137]

H. Conclusion

84 This article reviewed the application of IP rights to Big Data. In most cases, AI software is protected by copyright. Copyright's traditional role is otherwise in tension with the creation and use of Big Data corpora, however. The nature of the non-relational (noSQL) databases typical of Big Data corpora implies that such corpora are unlikely to be protected by copyright or by the EU sui generis rights in databases. Misappropriation (tort-based) protection might fill the gap, especially for data generated by AI systems that has high but short-lived value (e.g. in the FinTech sector).[138] Exceptions for Text and Data Mining are probably required to allow TDM using corpora of literary and artistic works, such as texts and images and video. Such exceptions are likely to continue to emerge in more jurisdictions around the world.

85 The questions concerning patents are not easy to answer. AI systems can be used to expand patent applications, but they can also be used to "guess" future incremental innovation and disclose them. Whether that disclosure will be interpreted by patent offices and courts as novelty-defeating is an open question. Whether AI-inventions— with no direct human input—are patentable is a matter under discussion as of this writing.

86 The article also reviewed data exclusivity and trade secrets. The latter might protect correlations and insights generated by AI systems, even if those are based on deep learning including the processing of protected personal data. This might generate tension between personal data protection and IP. The former might fill gaps in patent protection but only in areas where it applies (essentially chemical and pharmaceutical products).

87 In sum, the interfaces between Big Data and IP are about finding ways to adapt IP rights to allow and set proper parameters for the generation, processing and use of Big Data. This includes an analysis of how Big Data may infringe IP rights. There is also an issue of rights *in* Big Data, however. Courts and legislators have years of questions to answer on both constraints in and protection of Big Data.

136 Ibid.

137 Kenneth A. Bamberger & Orly Lobel, 'Platform Market Power' (2017) 32 Berkeley Tech. LJ 1051, 1089.

138 See European Commission, "Consultation document. FinTech: A more competitive and innovative European Financial Sector", 2017, available at <https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf> (last accessed 15 December 2018).

Lawfulness for Users in European Copyright Law

Acquis and Perspectives

by **Tatiana Eleni Synodinou***

Abstract: This article analyses the emerging dynamics of the concepts of lawful user, lawful use, and lawful access in European Copyright law. It aims to demonstrate that these concepts, which are part of the EU copyright law acquis, have the potential to provide a fair solution to the controversies regarding the "rights" and "duties" of users in European copyright law. The article proposes to establish a legislative dynamic definition of lawful use in European Copyright Law. The concept must be clarified and given a broad meaning in order to cover both uses which are authorized by the right holders, but are also not restricted by law, by taking into account the legal ideals of fairness and reasonableness. This change must be accompanied by the recognition of all copyright exceptions as jus cogens and the establishment of effective procedural mechanisms to safeguard the enjoyment of lawful users' rights.

Keywords: Copyright law; lawful user; lawful use; lawful access; lawful source; copyright exceptions; fairness; reasonableness; good faith; users' rights

Recommended citation: Tatiana Eleni Synodinou, Lawfulness for Users in European Copyright Law: Acquis and Perspectives, 10 (2019) JIPITEC 20 para 1.

A. Introduction

"When law can do no right,

Let it be lawful that law bar no wrong:

Law cannot give my child his kingdom here,

For he that holds his kingdom holds the law"[1].

1 Would a modern Shakespeare write about copyright law? In a modern version, one would say "because the author holds the means to control access to the work, he holds the copyright law". Traditionally, copyright law is exclusively author-oriented, and users' freedoms are seen as some narrow-interpreted restrictions, justified in specific circumstances. There is no general concept of lawful or fair use of work of mind.

2 Lawfulness and fairness could, at first sight, be seen as antagonistic concepts in copyright law. Lawfulness is generally seen as a restriction in the sense that the use of a copyright-protected work could be made only on the grounds of a specific legal basis. On the other hand, fairness is perceived as an enabling concept, because it presupposes a balancing between the interests of the right holders and users, which would ideally result in a reasonable outcome with no unjustified adverse effects on both parties.

3 Exploring the concept of lawfulness of use and specifically researching the status of "lawful user" in European copyright law could be considered as heresy. Copyright law doctrine classically perceives

* Associate Professor, Law Department, University of Cyprus.

1 (King John, 3.1.189), Constance to Cardinal Pandulph.

the use of copyright-protected works through the prism of exclusive control of the work by the copyright holder and it is characterized by the absence of the user.[2] Public interest is satisfied by the establishment of strictly defined exceptions or limitations to copyright. Moreover, exceptions or limitations are not traditionally considered as rights of the end-users.

4 The absence of the concept of the "user" in copyright law is also linked to another issue: the fundamental copyright premise that the mere use of works is free[3] and the traditional disinterest of copyright law in personal uses which do not have a commercial nature. Fifty years ago, copyright law rarely concerned itself with uses that were not both commercial and public,[4] while people believed that they were free to use copyright-protected works for non-commercial purposes.[5] In line with this approach, since controlling access to and use of copyright-protected works by private users was not a realistic goal, copyright holders have mainly focused on controlling reproductions and communications to the public that have a commercial nature.

5 However, the digital era changed this paradigm and it is now possible to control access to and use of works by private users. The dematerialization and the disappearance of the tangible copy is a defining feature of the digital environment. In this context, the need to access a tangible copy of an intellectual creation in the analogue world has been replaced by access to the work itself. Consequently, the intrinsic value of information resides much more in its use than in its acquisition or possession.[6] In this context, traditional users' liberties come under siege, since the growing dependence on digital content, accompanied by stronger copyright protection, has led to a narrowing of freedom of use.[7] Accordingly, it has become extremely difficult to identify permissible use and exercising exceptions may require some serious brainwork.[8]

6 The thesis that it is necessary to safeguard copyright users' interests or rights[9] has effectively emerged as a reaction and a necessary counterbalance to the growing asymmetry between the widespread control of right holders over copyright-protected works and the ambiguous restricted scope of copyright users' freedoms. In light of the above, the concepts of the "use" and of the "user" of copyright-protected works have obtained an autonomous status in European copyright legislation and case law through the corresponding concepts of lawful use, lawful user, and lawful access.[10]

7 This article analyses the emerging dynamics of the concepts of lawful user, lawful use, and lawful access in European Copyright law. It aims to demonstrate

2 Synodinou T., 'The Lawful User and a Balancing of Interests in European Copyright Law' (2010), IIC: 819-843. · Cohen J., 'The place of the user in copyright law' (2005) 74 Fordham L. Rev 347-374.

3 Westkamp G., 'Temporary Copying and Private Communications-the Creeping Evolution of Use and Access Rights in European Copyright Law'(2004) Geo. Wash. Int'l. LR: 1057.

4 Litman J., 'Lawful Personal Use (Symposium: Frontiers of Intellectual Property)' (2007) Tex. L. Rev. 85, no. 7: 1871-920; Litman J., 'The Exclusive Right to Read', (1994) 13 CARDOZO ARTS & ENT. L.J. 29, 35; Pamela Samuelson, 'Freedom of Expression in Historical Perspective', (2003) 10 J. INTELL. PROP. L. 319, 326.

5 Litman, J., 'Lawful Personal Use (Symposium: Frontiers of Intellectual Property), op.cit., p. 1873.

6 Dusollier S., 'Incidences et réalités d'un droit de contrôler l'accès en droit européen' in: Le Droit d'auteur: un contrôle de l'accès aux œuvres?', (2000) Cahiers du CRID n° 18, p. 25-52.

7 Elkin Cohen N., 'Copyright in the Digital Ecosystem, A User Rights Approach', in: Okediji R. (ed.) *Copyright Law in an Age of Limitations and Exceptions*, (Cambridge University Press, 2017), p. 133.

8 Janssens M. C., 'The issue of exceptions: reshaping the keys to the gates in the territory of literary, musical and artistic creation', in: Derclaye, E.(ed.), *Research Handbook on the Future of EU Copyright*, (Edward Elgar,2009), p. 317-318.

9 See, for instance: Litman J. 'Readers' Copyright', (2011) J. Copyright Soc'y 58, no. 2: 325-53; Niva Elkin-Koren, 'Making Room for Consumers Under the DMCA', (2007) 22 Berkeley Tech. L. J. 1119; L. Ray Patterson, Stanley W. Lindberg, *The Nature of Copyright: A Law of Users Rights*, (Athens, Georgia: University of Georgia Press, 1991); Carys C., 'Globalizing User Rights-Talk: On Copyright Limits and Rhetorical Risks' (2017), Articles & Book Chapters, <http://digitalcommons.osgoode.yorku.ca/scholarly_works/2666>; Liu J., 'Copyright Law's Theory of the Consumer', (2003) 44 B.C. L. REV. 397; Geiger C., Schönherr F., 'Defining the Scope of Protection of Copyright in the EU: The Need to Reconsider the Acquis regarding Limitations and Exceptions' (2012) in: Synodinou T. E. (ed.) 'Codification of EU Copyright Law: Challenges and Perspectives' (Kluwer), pp. 133-167; Mazziotti G., *EU Digital Copyright Law and the End-User* (Springer, 2008); Chapdelaine P., 'The Ambiguous Nature of Copyright Users' Rights', (2013) 26 INTELL.PROP.J. 1, 5; Dusollier S., 'The Relations between Copyright Law and Consumer's Rights from a European Perspective' (2010), European Parliament Publication, Available at SSRN: <https://ssrn.com/abstract=2127736>. The importance of establishing a "fair balance" between copyright protection and users' interest is also mentioned in the recital 31 to the Directive 2001/29, which states the following: "*A fair balance of rights and interests between the different categories of rightholders, as well as between the different categories of rightholders and users of protected subject-matter must be safeguarded*". For a recognition of the need to safeguard user interests by the CJEU, see, for instance: Case C-145/10, *Eva-Maria Painer v Standard VerlagsGmbH and Others*, ECLI:EU:C:2011:798, where it is stated in par. 134 that the quotation exception "*...is intended to strike a fair balance between the right to freedom of expression of users of a work or other subject-matter and the reproduction right conferred on authors.*"

10 Analogous developments have taken place worldwide. For the emblematic recognition of exceptions as users' rights in Canada, see: *Canadian Ltd. v. Law Society of Upper Canada* [CCH] 2004 SCC 13.

that these concepts, which are part of the EU copyright law acquis, have the potential to provide a fair solution to the controversies regarding the "rights" and "duties" of users in European copyright law. In the state of the art, exceptions to Copyright law are analyzed and interpreted either through the scope of the three steps test,[11] or with reference to externalities such as freedom of expression. It is proposed in this article that the emerging concept of lawfulness should play a substantial role in the conceptual delimitation of the copyright exceptions. The article argues that lawfulness and fairness of use in copyright law should not be considered as antagonistic but as mutually complementary elements of an EU dynamic concept of "lawful use". It further proposes the establishment of a taxonomy of lawful use in European copyright law, which would be based on the consolidation and further development of the existing acquis and principles of lawful use, as the latter have emerged via the case law of the Court of Justice of the European Union (CJEU).

8 The article is divided into three parts. The first part (B.) will examine the piecemeal legislative birth of the concepts of lawful user and of lawful use and the variant interpretations of these notions by the CJEU. The second part (C.) will explore the adjacent, but not identical, emerging concept of lawful access, which was introduced in the rhetoric of the EU copyright digital single market package. Finally, the third part (D.) will bring to light aspects of the silent consolidation and expansion of these concepts by the CJEU through the establishment of a prototype of a lawful and responsible user of copyright-protected works on the Internet.

B. The origins and dynamics of the concept of lawful use in European copyright law

9 The concept of "lawful user" made its first appearance in the Computer Programs Directive.[12] The Directive has introduced the notion, but paradoxically does not establish a clear terminology and does not use an identical term for defining the person who is entitled to enjoy the exceptions. In this context, the term "lawful acquirer of the program" or descriptive definitions such as the "person having a right to use the computer program" or the "person having a right to use a copy of a computer program" are used indiscriminately to determine the person who can lawfully invoke the application of copyright exceptions.[13]

10 The same expression reappears five years later in the Database Directive.[14] In this case, the person who can claim the application of the exceptions established by that Directive is defined consistently as the "lawful user of a database". Even though the two Directives do not use exactly the same term, the meaning of the concept in both Directives has to be perceived as identical. This interpretation seems to be implicitly confirmed by the Report published by the Commission on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs.[15] As stated in the Report, Articles 6 and 8 of the Database Directive (Directive 96/9/EC), which use the term "lawful user", were modelled along the lines of Article 5 (1) of the Computer Programs Directive. In any case, since the CJEU has not expressly dealt with this question, the issue will have to be addressed in a future consolidation or codification of the EU copyright *acquis*.

11 From a copyright policy point of view, the introduction of the concept of "lawful user" in those two Directives constitutes the expression of a new perception of the delimitation of copyright monopoly, characteristically of a paradigm shift. It is the first time ever that the individualized entity of the user of copyright-protected works is recognized

11 From the vast bibliography see: Geiger C., Gervais D. J., Senftleben M., 'The Three-Step-Test Revisited: How to Use the Test's Flexibility in National Copyright Law' (2014), American University International Law Review, Vol. 29, No. 3, pp. 581-626. Available at SSRN: <https://ssrn.com/abstract=2356619> or <http://dx.doi.org/10.2139/ssrn.2356619>; Senftleben, M., 'The International Three-Step Test A Model Provision for EC Fair Use Legislation', (2010) 1 JIPITEC 67, para. 1; Griffiths J., 'The 'Three-Step Test' in European Copyright Law - Problems and Solutions' (2009), Queen Mary School of Law Legal Studies Research Paper No. 31/2009. Available at SSRN: <https://ssrn.com/abstract=1476968>. See also: Geiger C., Hilty R., Griffiths J, Suthersanen U., 'Declaration A Balanced Interpretation Of The "Three-Step Test" In Copyright Law', 1 (2010) JIPITEC 119 para 1; Hilty R., 'Declaration on the "Three-Step Test": Where do we go from here?', 1 (2010) JIPITEC 83, para. 1.

12 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, OJ L 122, 17.5.1991, p. 42–46. The Directive has meanwhile been codified. See: Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs (Codified version) OJ L 111, 5.5.2009, p. 16–22.

13 Synodinou T. (supra n.1).

14 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77,27.3.1996, p. 20–28.

15 Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the implementation and effects of Directive 91/250/EEC on the legal protection of computer programs, Brussels, 10.04.2000 COM (2000) 199 final.

as an autonomous subject who is entitled to exercise certain legal prerogatives in the form of mandatory copyright exceptions. Indeed, the introduction of the concept of "lawful user" carries great symbolism, but it would have remained a purely theoretical advance if the lawful user's capacity to enjoy the use of copyright-protected works was not safeguarded or guaranteed.

12 Indeed, effective means to secure a proper balance of interests in copyright law is to take into account the general interest through specific mechanisms of recognition of the users' interests inside copyright law, such as through the establishment of users' rights which could be enforced in courts.[16] In this context, another unique feature of both Directives is that they establish some of the exceptions in favor of lawful users as mandatory, both in the sense that Member States shall provide for those exceptions and, more significantly, in the sense that these exceptions cannot be overridden by contractual terms. Specifically, Article 9 of Directive 91/250/EC states that any contractual provisions that limit or abrogate the right to create a back-up copy of a computer program, to observe, study and test the program and to decompile the program in order to achieve interoperability shall be considered as null and void.[17] Article 15 of Directive 96/9/EC also declares the binding nature of some exceptions. Any contractual provision contrary to Articles 6 par. 1 and 8 of the Directive shall be treated as null and void. Assigning a mandatory nature to exceptions or limitations to copyright injects a new perspective into copyright exceptions. This development could be seen as an indirect recognition of the category of "user rights" as an essential counterbalance to copyright protection. So, in addition to the concept of "lawful use", a new category of "legal prerogatives" also emerges: the "rights of the lawful user".

13 In 2001, the adjacent concept of "lawful use" appears in the Information Society Directive.[18] The Directive does not define the lawful user as the sole beneficiary of copyright exceptions. However, the mandatory temporary copy exception provided for by Article 5 par. 1 presupposes either acts of reproduction whose sole purpose is to enable transmission by an intermediary on a network between third parties, or lawful use to be made of a work or other subject matter. Even though the "lawfulness" of the use is not directly assessed in relation to the user's status as it is in the Software and the Database Directives, but in relation to the purpose of the act of reproduction,[19] the concepts of "lawful user" and of "lawful use" in the three Directives must be deemed to have the same meaning and the same function.

14 While the Software Directive and the Database Directive did not provide a definition of the "lawful user",[20] Recital 33 of the Information Society Directive defines "lawful use" broadly as any use which is authorized by the right holder or not restricted by law. There are two alternative criteria for assessing the "lawfulness" of the use. Either such use is authorized by the right holder (either expressly or implicitly if a work is made freely available through a website without any terms and conditions governing its use) or it is not restricted by law. In that sense, even though it is not entirely clear, it appears that a use would be lawful not only if it is based on a copyright exception or limitation,[21] but also on other legal grounds outside the purview of copyright law. Especially with regard to the assessment of lawful use on the grounds of copyright exceptions, it strongly depends on the possibility of neutralizing copyright exceptions by technological protection measures (TPMs) and contractual agreements. Concerning the enforceability of exceptions against TPMs, Directive 2001/29 chose to respond under an umbrella solution in Article 6 (4), which gives great freedom to Member States to adopt appropriate measures for safeguarding the enjoyment of copyright exceptions,[22] while this provision does not apply if the work is made available via on-demand services on agreed contractual terms.[23] Specifically, EU copyright legislation has

16 Geiger C., 'Copyright as an Access Right, Securing Cultural Participation Through the Protection of Creators' Interests' in R. Giblin, K. Weatherall (eds.) *What if We Could Reimagine Copyright?*, (Canberra, ANU Press, 2017), pp. 73-109; Max Planck Institute for Innovation & Competition Research Paper No. 15-07, available at SSRN: <https://ssrn.com/abstract=2643304>. See also: Burell R. and Coleman A., *Copyright Exceptions: The Digital Impact* (Cambridge University Press, 2005) 279; Riis T. and Schovsbo J., 'User's Rights, Reconstructing Copyright Policy on Utilitarian Grounds' (2007) European Intellectual Property Review 1.

17 See Article 8 of Directive 2009/24/EC (codified version of Directive 91/250), supra n.3.

18 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, Official Journal L 167, 22/06/2001 P. 0010 – 0019.

19 Dussolier S., 'Droit d'auteur et protection des œuvres dans l'univers numérique, Droits et exceptions à la lumière des dispositifs de verrouillage des œuvres' (2005) Larcier, Bruxelles, p. 449.

20 For possible interpretations, see: Vanovermeire V., 'The concept of the lawful user in the database directive', (2000) IIC, Vol. 31, p. 63-81; Dusollier S., 'L'utilisation légitime de l'œuvre: un nouveau sésame pour le bénéfice des exceptions en droit d'auteur?' (2005) Communication-Commerce Electronique (11), pp 17-20; Aplin T., 'Copyright Law in the Digital Society: The Challenges of Multimedia', (2005), Hart Publishing, p. 181.

21 Van Eechoud M., Hugenholtz P. B., Van Gompel S., Guibault L., Helberger N., 'Harmonizing European Copyright Law' (2009), Wolters Kluwer, Kluwer Law International, p. 116.

22 Bechtold, S., 'Information Society Directive, art. 6', in: Dreier Th., Hugenholtz, P.B. (eds.), 'Concise European Copyright Law' (2006), Kluwer Law International, p. 391.

23 Article 6 (4) of Directive 2001/29/EC of the European

an ambiguous approach on this issue. Regarding the thorny issue of the tension between exceptions and overriding contractual terms, Directive 2001/29 did not provide a clear answer. Recital 45 states that "the exceptions and limitations referred to in Article 5(2), (3) and (4) should not, however, prevent the definition of contractual relations designed to ensure fair compensation for the rightholders insofar as permitted by national law". As Guibault highlights, this has led to somehow conflicting interpretations. Some commentators argue that the limitations of Articles 5(2) to 5(4) can be overridden by contractual agreements, while others consider that the ability to perform legitimate uses that do not require the author's authorization is a factor that can be considered in the context of contractual agreements regarding the price.[24] Consequently, while certain exceptions might be safeguarded against TPMs in national copyright laws under the ambivalent conditions set by Article 6 par. 4 of Directive 2001/29, the question of the prevalence of copyright exceptions over contracts, or vice-versa, has been left mainly to the discretion of the Member States. An approach favoring a general prevalence of copyright exceptions over contractual clauses emerged in the *Verwertungsgesellschaft Wort (VG Wort)* cases,[25] where the CJEU appears to support the view that Member States generally have a choice over whether or not to allow exceptions to be overridden by, limited by, or otherwise dependent on contract terms. However, where contract or license terms are not expressly allowed by domestic copyright laws to limit the scope of an exception, the default position is that the exception will prevail over any rights holder authorization.[26] Whether this approach would become a prevailing principle in European copyright law remains to be seen, while in the meantime the question has only been harmonized for specific copyright exceptions.

15 Consequently, it appears that a use would be lawful on the grounds of a copyright exception or limitation, provided that this exception has not been contractually forbidden, unless European or national copyright law has established, either expressly or implicitly (by not expressly allowing contract or license terms to limit the scope of an exception), this exception as being resistant to contractual agreements.

16 The CJEU was called upon to interpret the prerequisite of "lawful use" laid down in Article 5 par. 1, in the *Infopaq II*, *Football Association Premier League* and the recent *Filmspeler* cases. As will be demonstrated, the CJEU's stance in relation to the concept of lawful use is ambivalent, because while at first it embraced a flexible approach - which appears to comply with Recital 33 of the Information Society Directive - more recently it restricted its scope by linking lawfulness to the author's consent and by establishing lawful access (interpreted as accessing the work via a "lawful source") as a prerequisite for subsequent lawful use.

17 In point of fact, the Court first adopted a broad construction of the concept of "lawful use", with reference to Recital 33 of the Information Society Directive.[27] In *Infopaq II,*[28] the Court confirmed that the specific authorization of the copyright holder is not required for asserting that the use is lawful. The Court held that the drafting of a summary of newspaper articles, even though it was not authorized by the copyright holders, was not restricted by the applicable legislation and the use could not be deemed unlawful. Similarly, in its judgment of 4 October 2011 in *Football Association Premier League,*[29] the Court was called upon to analyze whether the temporary copy exception could apply to the ephemeral acts of reproduction which were taking place upon the mere reception of satellite broadcasts by television viewers. It held that the picking up of such broadcasts and their visual display in a private context did not constitute an act restricted by the legislation and that such reception was to be considered lawful in the case of broadcasts from a Member State, when brought about by means of a foreign decoding device. In this context, the notion of lawfulness can therefore be defined as a specific application of the notion of good faith.

18 However, in the recent *Filmspeler* case,[30] the CJEU affirmed that the temporary copy exception of Article 5 par. 1 of the InfoSoc Directive cannot

Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

24 Guibault L., 'Relationship between copyright and contract law' in: Derclaye, E.(ed.), *Research Handbook on the Future of EU Copyright,* (Edward Elgar,2009), p. 529.

25 Cases C-457/11 to C-460/11, *Verwertungsgesellschaft Wort (VG Wort) v Kyocera and Others (C-457/11) and Canon Deutschland GmbH (C-458/11) and Fujitsu Technology Solutions GmbH (C-459/11) and Hewlett-Packard GmbH (C-460/11) v Verwertungsgesellschaft Wort (VG Wort)*, ECLI:EU:C:2013:426.

26 See par. 37 of VG Wort, op.cit. : "*Where a Member State has decided, pursuant to a provision in Article 5(2) and (3) of Directive 2001/29, to exclude, from the material scope of that provision, any right for the rightholders to authorise reproduction of their protected works or other subject-matter, any authorising act the rightholders may adopt is devoid of legal effects under the law of that State.*"

27 Seville C., *EU Intellectual Property Law and Policy,* (Edward Elgar, Cheltenham, 2016) p. 75.

28 *Case* C-302/10, *Infopaq International A/S v Danske Dagblades Forening,* [2012], ECLI:EU:C:2012:16, paras 44 and 45.

29 Cases C-403/08 and C-429/08, *Football Association Premier League Ltd and Others v QC Leisure and Others and Karen Murphy v Media Protection Services Ltd*, ECLI:EU:C:2011:631, par. 170 to 172.

30 Case C-527/15, *Stichting Brein v Jack Frederik Wullems*, [2017], ECLI:EU:C:2017:300.

be relied on by users of Kodi boxes, and thus of multimedia players on which there are pre-installed add-ons, which modify the settings and allow the Kodi box user to have access to private servers on which copyright-protected works have been made available to the public without the right holders' consent. Even if the content is streamed to the device, a technical and temporary copy of the work is still held in the device's memory. The CJEU firmly rejects the application of the exception of temporary reproduction, since it is clear that these settings do not correspond to a lawful use. On the contrary, the temporary reproductions on the multimedia players are made in the course of an obviously illegal use, since the users of such devices are deliberately accessing a free and unauthorized database of protected works.[31]

19 Consequently, the users of the device are not lawful users and they are also infringing copyright law, because no copyright exception can be invoked in their favor in relation to the reproductions made. This stance taken by the CJEU is not surprising; since the seminal *ACI Adam* case,[32] it would be impossible for users to invoke the private copy exception, due to the lack of a lawful source of the copy. As the Court stated, to accept that such reproductions may be made from an unlawful source would encourage the circulation of counterfeit or pirated works, thus inevitably reducing the volume of sales or of other lawful transactions relating to protected works, with the result that a normal exploitation of these works would be adversely affected. In line with the *ACI Adam's* argumentation, the CJEU in *Filmspeler* has also closed to users the escape route of the temporary copy exception. In order to arrive at this conclusion, the CJEU takes into account the *mens rea* of users of Kodi boxes, who deliberately access a free and unauthorized database of protected works, in order to conclude that they cannot rely on the temporary copy exception, because the temporary acts of reproduction take place in the context of a clearly illegal use.

20 From the above, it appears that the CJEU has opted for a flexible definition of the notion of "lawful use" based on the equally broad formulation of Recital 33 of the Information Society Directive, in the sense that a lawful use could also be any use which is not restricted by law, and therefore any use that can rely on copyright exceptions. However, as the *Filmspeler* judgment shows, the assessment made of the "lawfulness" of use on the grounds of a copyright exception is holistic, in the sense that the status of the user's knowledge in relation to the legality of the source of the copy of the work, which is accessed and used, is also taken into consideration.

21 In this context, the lawfulness of use for end-users depends on two interrelated criteria: a) their access to the work via a lawful source; and b) their knowledge in relation to the lawfulness or unlawfulness of this source. This approach is pragmatic because it takes into consideration the informational asymmetry in relation to the assessment of the lawfulness of the source of a copyright protected work, which is used on the grounds of a copyright exception. If only the first criterion, which is an objective one, were to apply, this would make it impossible for users to invoke copyright exceptions every time they access the work via an unlawful source, regardless of whether they are reasonably in the position to know or assume the unlawfulness of the source. In this context, the second criterion, which is subjective, would enable users who are not in a position to know or to logically assume the unlawfulness of the source, to still invoke copyright exceptions and be regarded as lawful users.

22 As will be shown, this line of reasoning has been consolidated by the CJEU in the hyperlinking cases (*Svensson*, *Bestwater* and especially *GS Media*). Furthermore, the question of the "lawful source" has dynamically reappeared recently, through the analogous concept of lawful access. The latter has emerged as a new trend in the EU Digital Single Market Copyright Package, though in variant forms, while the nature of the relationship between lawful access and lawful use is not clear (C.).

C. "Lawful access" in the Digital Single Market Copyright Package: a new trend?

23 The concepts of lawful access or lawful use must not be confused with the concept of lawful user. In this case, lawfulness is attached to the act, not to the person. The concept of "lawfulness" is also present in the recently adopted Directive on Copyright in the Digital Single Market. Specifically, "lawful access" to works or other protectable subject-matter is a prerequisite for enjoyment of the text and data-mining exceptions.[33] The prerequisite of "lawful access" is not something new in the Digital Single Market Package, since Article 6 (4) of the Directive 2001/29 referred to the associated concept of "legal access".[34] When referring to "lawful access" as a

31 Ibid, par. 69.

32 Case C-435/12, *ACI Adam BV and Others v Stichting de Thuiskopie and Stichting Onderhandelingen Thuiskopie vergoeding,* [2014], ECLI:EU:C:2014:254.

33 Articles 3 and 4.

34 "6. 4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take

condition for enjoyment of the exception, the text closely follows the model of the UK text on the data-mining exception[35] and not the criterion set in the French text on the data-mining exception,[36] which covers reproductions from "lawful sources" (material lawfully made available with the right holders' consent).[37]

24 From the wording of the provision, it appears that lawfulness of access is a prerequisite for enjoyment of the exceptions as lawful use. Nonetheless, the text of the Directive does not define what "lawful access" is. Some indications are to be found in Recital 14 of the Directive, where it is explained that lawful access to copyright-protected content occurs, for example, when researchers have access through subscriptions to publications or open-access licenses. Furthermore, it is noteworthy that lawful access comprises also access to works which are freely available on the Internet.[38] Nonetheless, there is no indication whether lawfulness of access is to be assessed purely objectively or also by taking into consideration other factors, such as the presumed state of mind of the user in relation to the lawfulness of the source of the work. Consequently, a crucial question is to determine the relationship between "lawful use" and "lawful access".

25 First, the two concepts could be differentiated chronologically: it could be argued that lawful access refers only to the initial access to the work via a lawful source. So, "lawful access" to the work is a first checkpoint of the lawfulness of the subsequent user's acts. The underlying idea is that there cannot be lawful use of the work or the database without initial lawful access to it. The Proposal, however, remains silent on whether "lawful access" should only be interpreted as having access to the work with the consent of the author or other right holder, or whether there might be other legal grounds for having lawful access to the work.

26 On the other hand, it could also be argued that lawful access and lawful use should be perceived as the necessary complementary steps accompanying the act of use as a whole. In this sense, "lawful use" encompasses both access to the work and all uses made of it, either simultaneously or subsequently to accessing it. This approach has two advantages. Firstly, it consolidates the various existing terminologies found in the piecemeal EU copyright legislation (lawful acquirer,[39] person having a right to use a computer program,[40] lawful user,[41] lawful use,[42] legal access,[43] lawful access).[44] Secondly, instead of evaluating the lawfulness of the user's acts in the form of two steps (access, other uses), it promotes a holistic approach to the lawfulness of users' acts, which could enable more flexibility, but also injects an element of responsibility with regards to the users' acts *vis-à-vis* copyright protected works.

27 Accordingly, lawful use should be endowed with a broad meaning. In the case of the text and data-mining exception this would mean that the exception could be enjoyed by every person who can use the work or the database, either on the grounds of a contract or license (in which case the license granted to the research institution will necessarily cover use by researchers), but also when their use is not prohibited by law. In this context, it would have been preferable to use the term "lawful use" in the text on the data-mining exception too, since the latter has been broadly defined and consolidated in CJEU case law; at least regarding the temporary copy exception established by the Information Society Directive.[45] However, such an interpretation could possibly be put forward by the CJEU if it is called on in the future to decide on relevant questions.

28 It is also noteworthy that the text on the data-mining exception of Article 3 is mandatory, since any contractual provision contrary to that exception will be unenforceable. The guarantee covering the exception against contractual clauses certainly strengthens the position of users, who can enjoy the

appropriate measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned".

35 Copyright, Designs and Patents Act 1988, § 29A (UK).

36 Art .38 of the Law No. 2016-1231 for a Digital Republic added paragraph 10 to Art.L122-5 and paragraph 5 to Art. L 342-3 of the Intellectual Property Code (Code de la propriété intellectuelle, CPI).

37 Geiger C., Frosio G., Bulayenko O., 'The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market-Legal Aspects, In depth Analysis for the JURI Committee. European Parliament, E 604.941' (2018), p. 17.

38 However, the exception of Article 4 is not applicable if the the use of works and other subject matter has been expressly reserved by their rightholders in an appropriate manner, such as machine readable means in the case of content made publicly available online. See: Art. 4, par.3.

39 Article 5 (1) of Directive 91/250/EEC on the legal protection of computer programs.

40 Article 5 (3) of Directive 91/250/EEC on the legal protection of computer programs.

41 Articles 6, 8 and 9 of Directive 96/9/EC on the legal protection of computer programs.

42 Article 5 (1) of the Directive 2001/29 on the legal protection of computer programs.

43 Article 6 (4) of the Directive 2001/29 on the legal protection of computer programs.

44 Recital 14 and Articles 3 and 4 of the Directive on Copyright in the Digital Single Market.

45 Geiger C., Frosio G., Bulayenko O., (2018), p. 24.

exception as a reinforced legal prerogative akin to a "user right". This is also in line with the reasoning of the Software and the Database Directives, where only "lawful users" can enjoy copyright exceptions. However, conversely this stance also embodies a more restrictive approach to enjoyment of the exception,[46] since as the European Copyright Society has pointed out, it makes the exception subject to private ordering. Indeed, the exception can effectively be denied to certain users by a right holder who refuses to grant "lawful access" to works or who grants such access on a conditional basis only.[47] So the concept will act restrictively if the condition of "lawful access" is interpreted in such a way that it will always depend on the terms of a contract or license. This is the reason why it is imperative to consolidate the terms of "lawful access" and "lawful use" into a single EU autonomous legal concept (that of "lawful use") and to define it flexibly.

29 The Digital Single Market Copyright Package also introduced another mandatory copyright exception in the Portability Regulation,[48] which entered into force in April 2018. Specifically, Article 3(1) introduces an obligation for an online service provider to enable a subscriber to access and use the online content service when temporarily present in other Member States. Furthermore, Article 5 provides that any contractual provisions, including those existing between holders of copyright and related rights, those holding any other rights relevant to the use of content in online content services and service providers, as well as between service providers and subscribers, which are contrary to Articles 3(1) and 4, shall be unenforceable. Even though it is not expressly classified as a "lawful user's right", the obligation of portability established by the Regulation takes the form of a personal right in favor of a user/consumer. Indeed, the portability privilege presents the two essential features of a lawful user's right. Firstly, it is not established generally in favor of the public, but in favor of a specific and distinct legal subject: the subscriber-consumer of an online content service who, on the basis of a contract for the provision of an online content service with a provider, may lawfully access and use such a service in his Member State of residence. Secondly, like the software and database lawful user's rights and the text and data-mining exception of Article 3, portability is fully guaranteed against opposing contractual terms and cannot be overridden by the contractual will.[49]

30 Nonetheless, unlike the concept of "lawful use" in the Information Society Directive, the concept of the "lawful user" who can claim the portability right is defined narrowly in the Portability Regulation as the subscriber to the online content service. Consequently, beneficiaries of the portability privilege are the only persons who have been contractually granted the right to use the service. This is also explained in Recital 15 of the Portability Regulation. According to this provision, "This Regulation should apply to online content services that providers, after having obtained the relevant rights from right holders in a given territory, provide to their subscribers on the basis of a contract, by any means including streaming, downloading, through applications or any other technique which allows use of that content. For the purposes of this Regulation, the term contract should be regarded as covering any agreement between a provider and a subscriber, including any arrangement by which the subscriber accepts the provider's terms and conditions for the provision of online content services, whether against payment of money or without such payment. A registration to receive content alerts or a mere acceptance of HTML cookies should not be regarded as a contract for the provision of online content services for the purposes of this Regulation".

31 The restrictive definition of "lawfulness" in this case corresponds to the reality of the transactions of such services, which are normally provided against payment. In this context, the entire edifice of the portability mechanism is modelled on the case where a subscription contract exists, and therefore all the necessary checks on the user's Member State of residence are based on information provided through the subscription contract. Consequently, the concept of "lawfulness" takes on a very specific meaning and has to be distinguished from the broader concept of "lawful use" contained in the Software, Database and Information Society Directives, as well as the notion of "lawful access" of the text and data-mining exceptions.

D. The implicit consolidation and expansion of the concept of "lawful use" in the CJEU's case law

32 The concept of "lawful user" was expressly recognized in sectoral EU copyright law Directives (the specific cases of software and databases) and the temporary copy exception of the Information Society Directive, while the adjacent concept of

46 Dusollier S., 'L'utilisation légitime de l'œuvre : un nouveau sésame pour le bénéfice des exceptions en droit d'auteur?' (2005) 11 Communication-Commerce Electronique, pp 17-20, at 18.

47 European Copyright Society, 'General Opinion on the EU Copyright Reform Package', (2017).

48 Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market OJ L 168, 30.6.2017, p. 1–11.

49 Synodinou T (2016), p. 14.

"lawful access" is a criterion for enjoyment of the text and data-mining exception in the Directive in the Digital Single Market.

33 However, the appearances of these concepts are sporadic and inconsistent. In this context, even though the emergence of "lawful use" has a significant symbolic value, it still remains marginal in EU copyright legislation.

34 Nonetheless, the CJEU seems to have taken on the task of implicitly expanding and further elaborating the concept. As has been demonstrated in *ACI Adam*,[50] the CJEU introduced lawfulness of access to the work as a prerequisite for lawful use when affirming that the benefit of the private copy exception concerns only reproductions made from "lawful sources".[51] The Court takes a firm stance and considers that the application of the private copy exception is not possible under EU copyright law, basing its argumentation solely on the unlawful nature of the source, which is interpreted by reference to the three steps test. The CJEU does not give a precise definition of what constitutes an "unlawful source", but it bases its argumentation mainly on the three steps test. In this context, the prerequisite of the lawful source appears to be emancipated from the specific private copy context and takes on the broader dimension of "lawful access". Since the CJEU did not expressly link its line of reasoning to the private copy exception, it could be deduced that the same reasoning could apply to all copyright exceptions. This could imply a general underlying principle that only lawful users can claim the application of copyright exceptions.[52]

35 It is noteworthy that the assessment of "lawfulness" is strictly linked to the source of the copy and does not take into consideration the end-user's knowledge in relation to the unlawfulness of the source of the copy. As a result, end-users cannot claim the application of the private copy exception for illegal downloads. In this sense, lawfulness differs from the principle of good faith. The CJEU does not take its reasoning further to officially declare that end-users are not lawful users and are, therefore, copyright infringers. Nonetheless this is implied, even though for practical reasons and due to privacy concerns, individual users who download material from unlawful sources are not expected to face legal action.[53]

36 In the subsequent *Copydan* judgment,[54] the CJEU was more explicit regarding the conditions governing the "lawful source". In the Court's view, the focal point for assessing the lawfulness of the source is the right holder's consent. As the Court stated, reproductions made using unlawful sources are those which are made from protected works that are made available to the public without the right holder's consent.[55] The lawfulness of the use (the making of a private copy in this case) is therefore conditional upon the way the source of the copy was made available to the public. If the work was made available to the public with the right holder's consent, the source is lawful and its use by the end-user is lawful too. By doing so, the CJEU embodies in its reasoning a logic of exclusive control of the uses of copyright-protected works and of copyright exceptions by private ordering. It will be fairly straightforward to ascertain when the end-user has acquired a copy of the work or has lawfully accessed the work as a service on the basis of a license/contract concluded directly between the right holder and the user. There will, however, be grey areas if a work is made available without rights holders clearly indicating which acts are authorized.

37 Based on the finding that the lawfulness of the source is assessed according to whether the work was made available with or without the right holder's authorization, the CJEU further elaborated on the lawfulness of linking the activities of users of copyright-protected works. First, in *Svensson*[56] and *Bestwater*,[57] the CJEU held that when an author published or authorized the publication of her work on a website without any technical restrictions, it is presumed that authorization was granted to all Internet websites to access this work via hyperlinking or framing. As the CJEU noted "..., it must be held that, where all the users of another site to whom the works at issue have been communicated by means of a clickable link could access those works directly on the site on which they were initially communicated, without the involvement of the manager of that other site, the users of the site managed by the latter must be deemed to be potential recipients of the initial communication and, therefore, as being part of the public taken into account by the copyright holders when they authorised the initial communication". Consequently, the lawfulness of hyperlinking is dependent on the presumed consent of the author or right holder who, in the absence

50 Case C-435/12, *ACI Adam BV and Others v Stichting de Thuiskopie and Stichting Onderhandelingen Thuiskopie vergoeding,* [2014], ECLI:EU:C:2014:254.

51 Ibid, par. 39.

52 Lucas A., Lucas- Schloetter A., Bernault C., 'Traité de la propriété littéraire et artistique' (2017), LexisNexis, supra n.9, p.390, n 400.

53 Quintais J.P., de Leeuw A., 'No more downloading from unlawful sources?' (2014) Kluwer Copyright Blog. Available via <http://copyrightblog.kluweriplaw.com/2014/05/12/no-more-downloading-from-unlawful-sources/>.

54 Case C-463/12, *Copydan Båndkopi v Nokia Danmark A/S*, [2015], ECLI:EU:C:2015:144.

55 Ibid, par. 74.

56 Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB*, [2014], ECLI:EU:C:2014:76.

57 Case C-348/13, *BestWater International GmbH v Michael Mebes and Stefan Potsch*, [2014], ECLI:EU:C:2014:2315.

of any technical restrictions of access to the work, is supposed to have authorized the communication of the work to all Internet users. This has also been further affirmed in the case of *Soulier and Doke,*[58] where the CJEU held that in a situation in which an author had given prior, explicit and unreserved authorization for the publication of his articles on the website of a newspaper publisher, without making use of technical measures restricting access to these works from other websites, that author could be regarded, in essence, as having authorized the communication of these works to the general Internet public.

38 This objective approach of the concept of the public is broad, but still has its own limits. If the work is communicated to the public lawfully but without the author's consent by a user on the basis of a copyright exception, then third parties, such as search engines, which provide a link to the work, are not directly covered by the Svensson principles. This is because the fact that it is impossible for the author to prohibit use due to the prevalence of a copyright exception (where the author cannot by law prohibit specific uses) is not legally equivalent to the positive act of granting authorization or consenting to use.[59] However, the exceptional significance of hyperlinking for the Internet function could result in reversing this line of thinking, as for instance was the case in Germany, where despite GS Media's presumption of knowledge for profit-making linkers, the German Federal Court of Justice held that such a presumption would not apply to search engines and for links displayed by search engines, because of the particular importance of these subjects to the functioning of the Internet. Consequently, the Court concluded that Google had not infringed the claimant's copyrights by displaying thumbnails of and links to photographs publicly available on the Internet without the right holder's consent.[60]

39 The CJEU's approach raises some additional questions in relation to what kind of restrictions the author should impose in order to avoid being presumed to have given his consent for communication of the work to all Internet users. Are contractual restrictions equivalent to technical restrictions, such as a "paywall overlay"? If a right holder adds a disclaimer below the work of mind, stating that linking to this work is not authorized, could it be possible that a potential link is not infringing copyright? In *Renckhoff,*[61] the CJEU concluded that the lack of warnings, disclaimers (and presumably other contractual restrictions of access) does not have any legal impact on the application of the right of communication to the public. This is relevant both for professionals and for normal, non-professional users, who do not have any profit-making intention to make primary communications of copyright-protected works to the public. The CJEU does not give an answer to the effect of contractual restrictions on the Svensson principle of free linking to content lawfully made accessible on the Internet without any technological access restrictions. Does a non-professional linker who does not have any profit-making intention have to diligently search for the existence of such contractual restrictions before linking? Although it could be risky to arrive at general conclusions, the significant level of importance that the CJEU attached to hyperlinking for the proper functioning of the Internet and for the exercise of online freedom of expression, could militate against such an approach.

40 Subsequently, in the *GS Media* case,[62] the prototype of a "responsible linker" complements the CJEU's previous stance in relation to "lawful use" and to "unlawful sources". In *GS Media*, the Court takes a further step forward and sets the criteria governing a-user's liability for copyright infringement, and specifically for the violation of the "making available right". The confirmation of the concept of "lawfulness" of the source/access in relation to the making available right is a strong indication that this concept is recognized by the CJEU as having a horizontal application, since it cuts across both the right of reproduction and the right of communication to the public and also copyright exceptions. The Court's reasoning is divided into two parts. Firstly, an assessment is made as to whether the work was made available with or without the right holder's authorization. If the work was made available without the right holder's consent, then the user's liability depends on whether he knew or ought to have known that the work was made available without the right holder's consent.

41 In the same way as a person who makes a private copy of a copyright-protected work from an unlawful source, a person who provides a link to copyright-protected content, which has been made accessible without the right holders' authorization, cannot be considered as a lawful user of the work. In the CJEU's reasoning, a linker is not a lawful user of a copyright-protected work if that person knew or ought to have known that the hyperlink

58 Case C-301/15, *Marc Soulier and Sara Doke v Premier ministre and Ministre de la Culture et de la Communication* [2016], ECLI:EU:C:2016:878.

59 See for such an approach : Varnerot, V., 'La gestion collective du droit de reproduction et de représentation des œuvres d'arts visuels par les services automatisés de référencement d'images', Communication- Commerce Electronique (1) 2018, p. 11.

60 Bundesgerichtshof, I ZR 11/16 - Preview III.

61 Case C-161/17, Land Nordrhein-Westfalen v Dirk Renckhoff, [2018], ECLI:EU:C:2018:279.

62 Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others*, [2016], ECLI:EU:C:2016:644.

he posted provides access to a work illegally placed on the Internet. Specifically, for profit-making linking activities, that knowledge is presumed.[63] In so doing, the CJEU's reasoning introduces elements of extra-contractual liability law into the core of copyright law, and thereby significantly alters the orthodox stance that copyright is established as an exclusive property right, the infringement of which does not take into account the *mens rea* of the infringer.[64] Indeed, in the CJEU's view, the question is no longer simply that of whether, objectively speaking, an act of communication to the public occurred: the assertion of the existence of the act itself is connected to subjective elements, such as the intention of the potential infringer's direct or constructive knowledge. This change is necessary in the online environment, where it is not possible for end-users who do not have a direct contractual relationship with the right holder to investigate and safely prove that the work is made available to the public without the author's consent.

42 The end-user's constructive knowledge has to be assessed with reference to the prototype of the objective standard of the *bonus pater familias*, the "reasonable person", such as this concept is established in the law of obligations of each Member State (such as the common law concept of "the man on the Clapham omnibus" or the French law standard of the *"homme avisé"*).[65] In this context, for example, a reasonable and prudent person would not have expected to access the latest Hollywood movie for free via an Internet link, and therefore lawful use will not occur if she/he further provides the link to the public. Similarly, the deliberate act of advertising the accessibility of copyright-protected works which were made available on the Internet without the copyright holders' consent, is an undeniable factor which reverses any argument in favor of the good faith of the person who provides the links.[66]

43 While in such a flagrant case, it would be fairly easy to ascertain the unlawfulness of the use, more complex situations will certainly arise where the unlawfulness of the source/access will not be clear. This is the case when, for example, a work was placed on the Internet with the author's consent, but with a contractual prohibition on making it further available which is not mentioned on the relevant website from which the end-user accessed the work, and without any technological barriers to accessing the work. Even though in such a case, it would not have been possible for a reasonable person to be aware of the contractual prohibition, the dependence of the assessment of the user's liability on complex legal reasoning would certainly be a deterrent factor against the use of the work. As the CJEU has not specifically defined the prototype of the "reasonable user", this assessment will have to be made on the basis of the variant relevant national legal standards.

44 It seems that for the CJEU, the delicate delineation between "lawful" and "unlawful" use will be decided on the grounds of the fundamental *"fraus omnia corrumpit"* legal principle. A manifestly illicit act (an unlawful source/access, the making available of the work without the right holder's authorization) is enough to contaminate the entire chain of reproductions and communications to the public of copyright-protected works, and even to rule out the application of copyright exceptions and limitations. Unless the use has been authorized, only those acting responsibly and in good faith could avoid liability and be considered as lawful users. Furthermore, there is a significant differentiation regarding the burden of proof of knowledge that the work was made available without the right holder's consent. The knowledge is presumed in the case of professional users (such as professional linkers), while the right holder carries the burden of proof for ordinary end-users who use the works in the context of a non-profit activity.

45 Indeed, a higher standard of care is generally expected from professionals in a specific field. So, while it is not absurd to pretend that online newspapers check whether the content they link to is authorized, no one could ever think that private users could always check and be aware of the legal status of the content they link to.[67] Nonetheless, the distinction in practice will not always be straightforward. The *GS Media* decision does not define the criteria which will be used to assess the profit-making activity (whether the link itself should generate profit, whether the website as a whole is 'for profit', whether the fact that the person creating the link is a commercial party is sufficient for the purpose of the 'for profit' criterion).[68] Furthermore, the dichotomy between the "professional" (profit-seeking) and "non-professional" linker is an artificial one, where both profit-seekers and amateur information providers are formally protected equally by freedom of

63 Synodinou T., 'Opinion, Decoding the Kodi Box: to link or not to link ?' (2017), EIPR (12), pp. 733-736.

64 Dormont S., 'L'arrêt GS Media de la Cour de Justice de l'Union européenne : de précisions en distinctions, l'hyperlien lui fait perdre son latin...' Communication Commerce Electronique (2)' (2017), p. 17.

65 For the concept of "responsible person" in the common law of negligence, see: *Blyth v. Birmingham Waterworks* [1856] 11 Exch 781 · *Hall v. Brooklands Auto-Racing Club* [1933] 1 KB 205.

66 *Filmspeler*, supra n.18, par. 50.

67 Bellan A., 'Compared to Svensson, GS Media is not that bad after all' (2016) Available via <http://ipkitten.blogspot.com/2016/10/compared-to-svensson-gs-media-is-not.html>.

68 Lokhorst G., 'GS Media in the National Courts: Fresh Issues on the meaning of for profit', (2017) Available via <http://copyrightblog.kluweriplaw.com/2017/01/17/gs-media-national-courts-fresh-issues-meaning-profit/>.

expression, under Article 10 of the European Convention on Human Rights. It is also questionable whether this distinction is compatible with the Berne convention, but it is worth mentioning that the concept itself is not a novelty in European Media law. For instance, in the Pihl[69] case, the ECtHR ruled that a non-profit blog operator is not liable for defamatory users' comments in case of prompt removal upon notice. The process of ascertaining the profit-making nature of the activity has to take into consideration the particularities of the Internet. In this context, financing by means of advertising revenues linked to the website's traffic appears on the face of it to fall within the scope of profit-making activities.[70]

46 Moreover, another question is whether and to what extent the lack of knowledge or of negligence of a user with a non-profit activity could generally be used as a decisive factor for denying her/his liability. Indeed, the issue at stake is that of whether the findings of the *GS Media* case as regards individual non-professional users could be applied more generally in relation to the reproduction and/or communication to the public of copyright-protected works which are accessible on the Internet with no technical constraints. The Advocate General Campos Sánchez-Bordona, in his Opinion on the *Renckhoff* case,[71] clearly favored such an approach. The case concerned the posting by a pupil, on a school's website, of a photograph which had been published on another website with the author's consent and was freely accessible on the Internet. In the Advocate General's view, even though this case has to be distinguished from the *GS Media* case (which involved the question of hyperlinks to protected works that were freely available on another website without the copyright holder's consent), the reasoning in the *GS Media* case concerning the subjective component of the behavior of persons with no profit motive could be extrapolated, *mutatis mutandis*, to the *Renckhoff* case. Indeed, it may be difficult, "in particular for individuals", to ascertain whether the copyright holders of works on the Internet have consented to their works being posted on the site concerned. On the basis of the foregoing, the Advocate General had opined that neither the pupil nor the school had communicated the photograph to the public. On the other hand, it was suggested that there will be communication to the public where the copyright holders give notice that the work to which access is being provided has been "illegally placed on the Internet" or where access to the work is provided in such a way that users of the website on which it is posted can "circumvent the restrictions taken by the site where the protected work is posted or where the author has notified the person seeking to publish his photograph on the internet that he does not give his consent".

47 However, the CJEU did not follow the Advocate General's Opinion.[72] By clearly distinguishing this case from *GS Media*, it held that the posting by the pupil of the photograph required a new authorization by the author. As the CJEU stressed: "unlike hyperlinks which, according to the case-law of the Court, contribute in particular to the sound operation of the internet by enabling the dissemination of information in that network characterised by the availability of immense amounts of information, the publication on a website without the authorisation of the copyright holder of a work which was previously communicated on another website with the consent of that copyright holder does not contribute, to the same extent, to that objective".[73]

48 Furthermore, for the Court to hold that the posting on one website of a work previously communicated on another website with the consent of the copyright holder does not constitute making available to a new public, would amount to applying an exhaustion rule to the right of communication. Lastly, it is irrelevant that the copyright holder did not limit the ways in which Internet users could use the photograph, since the enjoyment and the exercise of the right of communication to the public may not be subject to any formality.[74] The CJEU safeguarded the preventive and exclusive nature of copyright. It appears that the objective to establish a high level of protection for authors does not permit a liberal interpretation of the rights of the author in a way that the knowledge or the negligence of the users is taken into account in order to deny users' liability when assessing whether they have communicated a copyright-protected work to the public. On the other hand, in the specific case of links, given their significant contribution to the sound operation of the Internet by enabling the dissemination of information, a more lenient approach is possible.

49 The CJEU's stance in *Renckhoff* is in line with its previous findings in the *Vcast* case, where the lawfulness of the users' acts has also been approached restrictively, by taking into account the whole context of their access to copyright-protected works.[75] In the view of the Court, the users

69 ECHR, Rolf Anders Daniel PIHL against Sweden, 9 March 2017, app no 74742/14.

70 See the "Pirate bay" case: Case C-610/15, *Stichting Brein v Ziggo BV and XS4All Internet BV*, [2017], ECLI:EU:C:2017:456.

71 Opinion of the Advocate General Campos Sánchez-Bordona delivered on 25 April 2018, Case C-161/17, *Land Nordrhein-Westfalen v Dirk Renckhoff*, [2018], ECLI:EU:C:2018:279.

72 Case C-161/17, *Land Nordrhein-Westfalen v Dirk Renckhoff*, [2018], ECLI:EU:C:2018:279.

73 Ibid, par. 40.

74 Ibid, par. 36.

75 Case C-265/16, *VCAST Limited v RTI SpA,* [2017], ECLI:EU:C:2017:913.

of a broadcast digital recording mechanism cannot invoke the private copy exception in order to justify access to content that is hosted in the cloud by the recording service. Provided that the same content can be accessed by various users who subscribed to the service, the issue of lawfulness of use must be analyzed not only in light of the application of the right of reproduction, but also in light of the right of communication to the public.[76] In this context, even when online access could be permitted by an exception to the right to reproduction, the issue of the lawfulness of the user's access has to be examined broadly, in conjunction with the possible application of other rights, such as the right of communication to the public.

50 Consequently, in *Renckhoff* the CJEU closed the door to a possible application of extra-contractual liability evaluations when assessing lawfulness of use in relation to whether an act of the user falls within copyright monopoly because it has been communicated to the public without the author's consent. However, the CJEU did not examine whether the *GS Media* line of reasoning could find some application in relation to the assessment of lawful use on the basis of copyright exceptions and limitations. Indeed, *Renckhoff* should not be perceived as precluding the lawfulness of the users' acts on the grounds of copyright exceptions in general terms. In the present case it was clear that the essay with the photo was uploaded onto the school's website, while the possible application of the educational exception was not raised by the domestic court. The application of the educational exception was therefore not examined by the CJEU, which focused only on whether an act of communication to the public, with or without the author's consent, took place. As stated in para. 42 of the judgment, "it suffices to state that the findings set out in paragraph 35 of the present judgment, relating to the concept of 'new public', are not based on whether the illustration used by the pupil for her school presentation is educational in nature, but on the fact that the posting of that work on the school website made it accessible to all the visitors to that website".

51 Even though the use was deemed unlawful, because it did not lie outside the scope of the right of communication to the public, the *Renckhoff* case does not preclude that the use might have been considered lawful on the grounds of the educational copyright exception. It is noteworthy that the argument has also been discussed in the ALAI Opinion on this case,[77] where it was stated that in relation to the assessment of lawful use by way of illustration for teaching, the crucial question, from the viewpoint of the Berne Convention (Article 10(2)), is whether communication on a website that is accessible to all Internet users and is not restricted solely to the school community, can still be characterized as use by way of illustration for teaching and whether such use is compatible with fair practice. The ALAI Opinion concludes that communication of a work on a website open to everyone, even if it is made by a school, doubtless exceeds the scope of a broadcast by way of illustration for teaching. Therefore, article 10(2) cannot justify it. However, it has also been argued that communication on a school's website with more restricted access might prove to be perfectly compatible with the Convention's norms.

52 In this context, the *Renckhoff* case does not answer the question of whether the unlawful nature of the source, or more broadly unlawful access to a copyright-protected work, contaminates all subsequent uses, and thus necessarily neutralizes lawful use on the grounds of copyright exceptions as well. This is because in *Renckhoff,* the work was made available to the travel website without any technical restrictions, with the author's consent. Therefore, the source of the photo on the Internet was lawful, even though the author's consent was contractually limited to use on the travel website. Since the educational exception could apply if the photo was made available with more restricted access, it can be deduced that the existence of contractual restrictions, which constitute in *personam* limitations regarding the use of the photograph other than on the travel website, would not have been a sufficient legal basis for rendering uses based on copyright exceptions unlawful. In this context, *Renckhoff*, like *Svensson*, implicitly promotes an "*in rem"* approach to the effect of the author's consent, in the sense that the presence of the work on a website without any technical restrictions and with the author's consent, could not exclude the lawful use of this work on the grounds of a copyright exception.

53 Certainly, there is no answer to the question of whether the existence of express contractual restrictions on the travel website, in the form of a disclaimer issued by the right holder or the licensee (the travel website's owner) would render use of the photograph on the grounds of copyright exceptions unlawful. In this case, the user's access to the work via the website containing the disclaimer would be seen as an implied acceptance by the user of the terms and conditions of access mentioned in the disclaimer. Could a contractual restriction of this type in relation to how much or what part of a work

76 Jougleux P., 'Access to works protected by copyright law' in Synodinou T. (ed), 'Pluralism or Universalism in international copyright law' (Kluwer Law International, Alphen aan den Rijn, Netherlands: Wolters Kluwer, forthcoming in 2019).

77 Opinion on case Case C-161/17, *Land Nordrhein-Westfalen v Dirk Renckhoff*, [2018], ECLI:EU:C:2018:634, Available at: <http://www.alai.org/en/assets/files/resolutions/180529-opinion-land-nordrhein-westfalen-en.pdf>.

can be quoted or used for illustration purposes for teaching, render a use that does not respect those conditions unlawful? Here again comes the question of enforceability of copyright exceptions against contractual restrictions and the possible scope and specifically the effect of these restrictions regarding works found without any technical restrictions on the Internet. The CJEU dealt with this question in the *Ryanair* case only in the specific context of a database that was not protected under the terms of the Database Directive, either by copyright or by the sui generis right, and held that the author of such a database is not prevented from laying down contractual limitations on its use by third parties. It was furthermore concluded that the author or producer of such a database is not obliged to safeguard a minimum level of free use of the database content for the users, such as the right for a lawful user to extract and reuse an insubstantial part of the database content for any reason, even for commercial purposes.

54 Furthermore, the contractual method of delimiting the use of information has its own inherent limits. The principle of privity of the contract (or the principle of the relative force of obligations in civil law countries) precludes the imposition of contractual obligations on third parties. So, where a copyright-protected work accessed by the user via a website with contractual restrictions which restrict or neutralize copyright exceptions is further disseminated on the Internet, the author or the website's right holder cannot invoke these restrictions against third parties who did not access the work via the website on which it was published with these restrictions, but accessed it from other sources where the restrictions were not mentioned. This is, however, applicable only in relation to copyright exceptions which have been established as *ius cogens* by European copyright law or by domestic copyright laws.

55 Leaving aside the complex issue of unlawfulness of use due to contractual restrictions, the basic question still remains of whether users can invoke copyright exceptions when they have accessed the work via an unlawful source, such as where the photograph had been uploaded to the travel website without the author's consent. As the law stands now, there is no straightforward answer. The unlawfulness of the source/access would normally render copyright exceptions unacceptable as a basis for lawful use - as has already been clarified first in *ACI Adam* and later in *GS Media* - in relation to hyperlinks pointing to works which have been made available to the Internet without the author's consent. Accepting the contrary would somehow result in "laundering" the unlawfulness of the source/access via the mechanism of copyright exceptions. However, even though it is limited to hyperlinking, *GS Media* has also shown that there is a difference between the status of responsibility to be expected from non-commercial and from for-profit users. Knowledge of the unlawfulness of the source is presumed in the case of for-profit users, while the right holder carries the burden of proof for ordinary users who use the works in the context of a non-profit activity. The importance of hyperlinking for freedom of expression on the Internet, combined with the technicalities of this mode of communication (lack of control of the source of the work, since the linker is pointing and recommunicating an existing communication) was crucial in reaching this conclusion.

56 Could a similar line of reasoning apply in relation to the assessment of lawfulness of use on the grounds of copyright exceptions as well? In our view, this should not be excluded with reference to *Renckhoff,* since the latter did not deal with this question, but simply excluded the CJEU's hyperlinking line of reasoning only in relation to the assessment of whether a communication to the public took place with or without the author's consent and not in relation to the assessment of lawfulness of use on the grounds of copyright exceptions. Certainly, there is no "one size fits all" approach to all copyright exceptions. Firstly, in some cases, such as for example in the case of the exception of quotation,[78] the lawfulness of the source has been expressly established by law as a condition for enjoyment of the exception. This was also highlighted recently by AG Spuznar in his Opinion on the *Spiegel Online* case, where the necessity of the prerequisite of the lawfulness of the first publication of the work being quoted was firmly stated because it safeguards the author's moral right

78 See Article 10 of the Berne Convention: "(1) It shall be permissible to make quotations from a work which has already been lawfully made available to the public, provided that their making is compatible with fair practice, and their extent does not exceed that justified by the purpose, including quotations from newspaper articles and periodicals in the form of press summaries." See also Article 5(3)(d) of the Directive 2001/29 that authorizes Member States to allow: "quotations for purposes such as criticism or review, provided that they relate to a work or other subject-matter which has already been lawfully made available to the public, that, unless this turns out to be impossible, the source, including the author's name, is indicated, and that their use is in accordance with fair practice, and to the extent required by the specific purpose". As it is mentioned by Rosati, "quotation has been regarded by some as a 'right' (rather than an 'exception') because the language of Article 10(1) of the Berne Convention appears to require Member States to authorize quotations of copyright works". See: Rosati E., 'Non-Commercial Quotation and Freedom of Panorama: Useful and Lawful?', (2017) JIPITEC 8 4. For such an approach see: Goldstein P., Hugenholtz P.B., 'International copyright. Principles, law, and practice', (OUP:2013), p. 391; Tawfik M. J., 'International Copyright Law: W[h]iter User Rights?', in Michael Geist (ed.), *In the Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 66.

of divulgation.[79] The assessment of the lawfulness of the source in the event of quotation, but also possibly in other cases of copyright exceptions, the basis for justification of which is freedom of expression, deserves a special analysis through the prism of fundamental rights. Indeed, the prerequisite of the lawfulness of the source in this case functions as a safeguard for protection of the author's freedom of expression regarding the decision on whether and when the work should be released to the public, which in copyright law is guaranteed through the author's moral right. It is noteworthy that this is expressly recognized by AG Spuznar in his Opinion on *Spiegel Online*, where it is stressed that the author's exclusive control over his own work is based both on protection of the author's personality (moral right) and on his/her freedom of expression. This enhanced focus on the fundamental rights basis of copyright when it comes to the protection of the author's moral interests has the potential to assert moral rights as a powerful limitation on the dissemination of copyright-protected works on the grounds of copyright exceptions in European copyright law. This is also in line with the CJEU's findings in *Deckmyn*, where the legitimate interest of authors in ensuring that their works are not associated with a racist and discriminatory message has been recognized by the CJEU.[80] The prerequisite of the lawfulness of the source in the quotation exception, both in Berne and in Article 5 of Directive 2001/29, should however, be interpreted broadly in the sense that what is important is that the first divulgation of the work to the public was made with the author's consent or under a compulsory license, regardless of the means of divulgation (it does not have to be a "lawful published work" within the meaning of article 3 (3) of the Berne Convention)[81] and, presumably, of possible further contractual restrictions on it. Since the underlying idea is that it should be the author's decision as to whether, and if so when, he or she wants to render the work public,[82] if the author consented to publication of the work on an Internet source, such as on a website or on a public profile on a social media account, the condition of lawfulness of the source should normally be met for subsequent uses of the work on the basis of the quotation exception.

57 Furthermore, the unlawfulness of the source should not in any case render a use that is based on copyright exceptions unlawful and, as a result, lead to the user being held liable for copyright infringement. The fact that it may be impossible – or at least extremely difficult – to know or presume that the source is unlawful, especially in the case of sources found online, should be taken into consideration as part of a holistic assessment of the user's liability. In this context, there should be cases of lawful non-commercial use of a copyright-protected work accessed via an unlawful source, provided that, in line with *GS Media's* underlying principle, the user could not reasonably have been in a position to know or assume the non-manifest unlawfulness of the source of the work. Conversely, uses from a manifestly unlawful source would not qualify as lawful use, even for non-commercial users, unless there is a specific background which renders the specific use lawful, such as if use on the grounds of the exception is absolutely necessary to safeguard freedom of expression.[83] However, according to the *GS Media* principles, this benefit would not apply to the use of unlawful sources of copyright-protected works for news reporting, parody or quotation by media professionals who operate on a commercial/profit-making basis, since their knowledge of the sources' unlawfulness will be presumed.

58 Is it possible to include in European copyright law a horizontal analysis of the non-commercial user's state of mind in relation to lawfulness of the source of the work that is being used on the grounds of a copyright exception, even in cases such as the exception of quotation, where the lawfulness of the source is a criterion directly imposed by the Berne Convention and EU Copyright law? Provided that this assessment is made in relation to the user's liability and not in relation to the scope of copyright protection (rights and exceptions) such as the latter is defined in international copyright law, the introduction into European copyright law of such an exemption-from-liability clause - in favor of non-commercial users who could not reasonably be in a position to know or presume that a source of a work that they use on the basis of copyright exceptions is unlawful - would be possible. Clauses which alleviate copyright users' liability are not completely unknown in copyright legislation,[84] although these

79 Case C-516/17, *Spiegel Online GmbH contre Volker Beck*, Opinion (2019), ECLI:EU:C:2019:16, par. 55.

80 Case C-201/13, *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others*, ECLI:EU:C:2014:2132, par. 31.

81 Ricketson S., Ginsburg J., 'International Copyright and Neighbouring Rights, The Berne Convention and Beyond', (2005) Vol. I, (OUP), p. 785, 786.

82 Lewinski V., Walter M., 'Information Society Directive, Article 5', in Lewinski V., Walter M., 'European Copyright Law, A Commentary' (OUP, 2019), p. 1049.

83 Case C-516/17, *Spiegel Online GmbH contre Volker Beck*, Opinion (2019), ECLI:EU:C:2019:16.

84 See for instance Article 13 (6) of the Cypriot copyright law 59/1976, where it is provided that : "(6) At any time in an action for copyright infringement right it is proved or admitted that - (a) there was an infringement, but (b) at that time the defendant was unaware of, but had no good reason to believe that the he work to which the claim relates is copyright protected, the claimant shall not be entitled under this Article to any compensation from the defendant for the offense but shall be entitled to the benefits derived from the infringement irrespective of the granting or not of

clauses are often applicable only when calculating the amount of damages or other sanctions imposed on the infringer. This clause would be part of a dynamic concept of lawful use which consolidates and further advances the existing acquis on lawful use and lawful source/access.

59 In fact, "lawful use" should be perceived as a flexible concept which allows a comprehensive evaluation of the user's acts by taking into account both fairness and reasonable expectations of responsibility. Hitherto, the CJEU's piecemeal elaboration of the concept of lawful use has established its perimeter in a one-dimensional format only, by focusing mainly on the restrictive dimension of lawfulness and not on its inherent enabling dynamic. However, lawfulness could also be interpreted openly, in a way that ensures that legal norms such as reasonableness and fairness are also taken into account via a variety of legal mechanisms both inside and outside the scope of copyright law. It is noteworthy that in his Opinion in the *Spiegel Online* case, AG Szpunar argued that the courts might intervene in exceptional circumstances to safeguard a fundamental right (freedom of expression in this case), even in the absence of a specific corresponding exception (when the "essence of a fundamental right" is at stake), since it is within the competence of the legislator to strike a fair balance between copyright and other fundamental rights.[85] This finding should not be seen only as a restriction, but as a hint that it is within the competence of the EU legislator to shape the general perimeter of "sensitive" copyright norms associated with flexible and fundamental rights under a taxonomy of lawful use.

60 This presupposes the consolidation and restructuring by the EU legislator of the core of the concept of lawful use, which now appears amorphous. This dynamic definition should consolidate the existing acquis on the lawfulness of use through the elaboration of a definition of lawful use which is sensitive to fundamental rights, accompanied by a catalogue of examples of categories of lawful use.[86] Under such an approach, the problematic of lawful source/lawful access (gained by contract or thanks to other legal grounds within copyright, such as exhaustion and copyright exceptions) should be seen as part of a comprehensive assessment of the lawfulness of the user's act and of the user's liability. This holistic assessment should be made on the basis of two mutually complementary pillars: a) by means of a fundamental rights' analysis of copyright norms[87] combined with the application of abstract legal principles embodying elements of fairness and of natural justice, such as interpreting and performing a contract/license of use in accordance with good faith or analogous legal concepts such as "unconscionability" in common law jurisdictions;[88] or b) by assessing the users' behavior on the grounds of established principles of extra-contractual liability in line with the *GS Media* logic and by introducing an exemption-from-liability clause in favor of non-commercial users who could not reasonably be in a position to know or presume that the source of a work that they used on the basis of copyright exceptions was unlawful.

61 In this sense, the comprehensive approach could be used not only to broaden the concept of lawful use and to avoid unjust effects but could also function in the opposite direction as an inner restriction on lawful use itself, in case of misuse. Good faith and fair practice could be used as criteria to judge whether lawful use really is lawful or whether it still remains lawful. This, in turn, would result in losing the option of invoking the rights of the lawful user under certain specific circumstances. For instance, a lawful acquirer – such as a purchaser of a copy of a software package who stores a back-up copy of the software on an insecure server to which everyone has free access – is offering other users of the server, either intentionally or by negligence, the possibility to reproduce the program. This user is violating the principle of good faith and abusing the right

any other remedy under this Article".

85 See on this point: GeigerC. and Izyumenko E., 'Freedom of Expression as an External Limitation to Copyright Law in the EU: The Advocate General of the CJEU Shows the Way' (2018), European Intellectual Property Review.; Centre for International Intellectual Property Studies (CEIPI) Research Paper N°2018-12. Available at SSRN: <https://ssrn.com/abstract=3293735> or <http://dx.doi.org/10.2139/ssrn.3293735>.

86 For this approach, see: Synodinou T., 'Who is lawful user in European copyright law? From a variable geometry to a taxonomy of lawful use', in: Synodinou T., Jougleux Ph., Markou Ch., Prastitou Th. (eds.), 'EU Internet law in the digital era', Springer (forthcoming in 2019).

87 For Hugenholtz, the fair balance of copyright with other fundamental rights, such as freedom of expression, the right to privacy or the right to conduct business, would be a source for flexibility in European Copyright Law that is alongside the existing structure of well-defined limitations and exceptions. See: Hugenhlotz P. B., 'Flexible Copyright, Can the Author's Rights Accommodate Fair Use?', in: Okediji R (ed.)., *Copyright Law in an Age of Limitations and Exceptions*, (Cambridge University Press,2017), p. 287-289. For the "fair balance" of copyright with other fundamental rights in the CJEU's case law, see: Griffiths J., 'Constitutionalising or Harmonising? The Court of Justice, the Right to Property and European Copyright Law' (2013) 38 European Law Review 65-78. Available at SSRN: <https://ssrn.com/abstract=2217562>.

88 As Waddams notes, "Good faith, unconscionability and reasonable expectations are concepts that sound somewhat similar, and the terms are sometimes used together to signify (usually with approbation) what might be summarised as a flexible approach to contract law, avoiding rigid rules, and emphasising justice in the individual case, even at the cost of stability and predictability". See: Waddams S. M., 'Good Faith, Unconscionability and Reasonable Expectations', (1995) 9 Journal of Contract Law, p.58.

to make a back-up copy of the program and could also be deemed to be in breach of his duty of care. Consequently, even if the initial lawful acquisition of the copy of the computer program has made him a lawful user, his use could still not be considered as lawful under these specific circumstances.

62 Additionally, the core of "lawful use" is intrinsically connected to the broader question of the recognition and effective protection of users' interests in European copyright law. The user of copyright-protected works has gradually emerged as a new norm in the CJEU's case law.[89] In this context, in *UPC Telekabel*,[90] the CJEU stressed the need to safeguard Internet users' right to lawfully access information when Internet service providers adopt measures to bring an end to a third party's infringement of copyright. As Geiger notes, the Court in *Telekabe*l, "clearly adopted the language of users' rights as a counterbalance to the disproportionally extensive enforcement of copyright".[91] It is noteworthy that this is the first time that the CJEU gives a more concrete substance to users' rights by accompanying them with a procedural safeguard, since, as the Court states, national procedural rules must provide a possibility for Internet users to assert their rights before the court once the implementing measures are known.[92] A user could therefore address a complaint to the court that the specific blocking method chosen affects his/her fundamental rights.[93] However, the scope of these rights is still imprecise. Shall this *locus standi* principle apply exceptionally only in the case of general injunctions, such as those provided by Austrian law in the *UPC Telekabel* case, or should it be extended to all blocking injunctions, even the specific ones that are issued by the courts?

89 See, for instance: Case C-117/13, *Technische Universität Darmstadt v Eugen Ulmer KG ('Ulmer')*, [2014], par. 43 · Case C-201/13, *Deckmyn*,[2014] (CJEU, Judgment of the Court (Grand Chamber) of 3 September 2014, par. 26.

90 Case C-314/12*UPC Telekabel Wien GmbH v Constantin Film Verleih GmbHand Wega Filmproduktionsgesellschaft mbH ('UPC Telekabel')* [2014], Judgment of the Court (Fourth Chamber) of 27 March 2014).

91 Geiger C., 'Copyright as an Access Right, Securing Cultural Participation Through the Protection of Creators' Interests' in R. Giblin, K. Weatherall (eds.) *What if We Could Reimagine Copyright?,* (Canberra, ANU Press, 2017), pp. 73-109; Max Planck Institute for Innovation & Competition Research Paper No. 15-07. Available at SSRN: <https://ssrn.com/abstract=2643304>.

92 Synodinou T., 'Intermediaries' liability for on line copyright infringement in the EU: evolutions and confusions' (2015) 31 Computer Law and Security Review, 57-67.

93 Savola P., 'Website blocking in copyright injunctions: a further perspective' (2014). Available at: <http://the1709blog.blogspot.com/2014/03/website-blocking-in-copyright.html>; Savola, P. 'Proportionality in Fundamental Rights Conflicts in National Measures Implementing EU Law' (2014). Available at SSRN: <http://ssrn.com/abstract=2432260> or <http://dx.doi.org/10.2139/ssrn.2432260>.

63 The effective safeguarding of lawful users' rights necessarily presupposes a number of structural changes in the copyright ecosystem, both at a substantial and at a procedural level. First, copyright exceptions should be established as real lawful user's right in the sense that they are *jus cogens* that cannot be overridden by technological protection measures (TPMs) and by contracts. This change must be accompanied by the introduction of procedural mechanisms, such as the establishment of *locus standi* of lawful users to bring a claim before a court against the neutralization or restriction of copyright exceptions, and the establishment of out-of-court redress mechanisms for the settlement of these disputes. This is also the path that has been taken by Article 17 (former Article 13) of the Directive on Copyright in the Digital Single Market, where it is provided that various mechanisms shall be established by the Member States in relation to the effective enjoyment of copyright exceptions by users of the services offline providers. First, an obligation is imposed on online service providers to establish complaint and redress mechanisms in order to safeguard the effective enjoyment of quotation, criticism, review and parody. Furthermore, Member States should also ensure that users have access to out-of-court redress mechanisms for the settlement of disputes, which should allow these to be resolved impartially. Users should also have access to a court or other relevant judicial authority in order to assert the use of an exception or limitation to copyright rules.

E. Conclusion

64 The concept of lawful use could be seen as an oxymoron in EU copyright law. On the one hand, it is used as a means for restricting the use of copyright-protected works, in the sense that there is a trend towards only lawful users being able to avoid liability for copyright infringement when accessing or using works. On the other hand, the effective enjoyment of copyright exceptions has hitherto been safeguarded only for lawful users, since lawful users are the only ones who enjoy exceptions in terms of user rights, which cannot be overridden by contract. The two facets of the concept of "lawful user" are organically interlinked. Indeed, the concept of "lawful user" makes sense if, in addition to being subject to obligations, the lawful user also possesses certain rights, in the sense that copyright exceptions are mandatory.

65 The concept of "lawful use" first made its appearance in sectoral EU copyright legislation in relation to information goods. It also appeared sporadically in various EU copyright provisions in the field of copyright exceptions. Even though the concept is

marginal in EU copyright legislation, the CJEU has implicitly consolidated the concept of "lawful use" and expanded its application in relation to the main economic rights granted by copyright law for all categories of works.

66 The EU law principle of legal certainty is based on the fundamental premise that those who are subject to the law must know what the law is in order to be able to plan their actions accordingly, so that they can have legitimate expectations, otherwise they will regard the law as arbitrary.[94] In this context, it is vital to favor a dynamic definition of the concepts of "lawful user" and of "lawful use" in European copyright legislation. This definition shall consolidate the existing acquis on the lawfulness of use through a taxonomy of lawful use. This taxonomy could be based on a broad definition of lawful use accompanied by a catalogue of examples.[95] The concept must be clarified and given a broad meaning in order to cover both uses which are authorized by the right holders, but are also not restricted by law, by taking into account the legal ideals of fairness and reasonableness. This change must be accompanied by the recognition of all copyright exceptions as *jus cogens* and the establishment of effective procedural mechanisms to safeguard the enjoyment of lawful users' rights

67 In the author's view, the dual function of the concept, which acts both as an enabling and as a restrictive clause, has the potential to provide an enhanced calibration of the interests of both copyright holders and users.

94 Tridimas T., *The General Principles of EC Law* (OUP, Oxford 2000), p. 163.

95 For this approach, see: Synodinou T., 'Who is lawful user in European copyright law? From a variable geometry to a taxonomy of lawful use', in: Synodinou T., Jougleux Ph., Markou Ch., Prastitou Th. (eds.), 'EU Internet law in the digital era', Springer (forthcoming in 2019).

A FRAND Regime for Dominant Digital Platforms

by **Mathew Heim and Igor Nikolic***

Abstract: Dominant digital platforms are under increased scrutiny by regulators around the world, notably competition authorities. Much of the discussion focuses on market access and contestability. However, many doubt whether traditional competition law enforcement can, by itself, be an adequate solution to the challenges posed by dominant digital platforms. Instead, a broader regulatory solution could be devised to ensure effective competition and to provide access to critical platforms or access to data. On the premises that regulation is warranted, this paper considers whether a Fair, Reasonable and Non-Discriminatory (FRAND) access regime could be a solution to ensure effective competition, while maintaining the incentives of dominant platforms to innovate. The paper shows that, beyond the application of FRAND in the competition law context, the European Union institutions have consistently used the FRAND regime to ensure access to critical infrastructure or inputs. The FRAND regime has been applied in EU legislation such as standardisation, chemicals, electronic communications framework, public sector information, research framework, vehicles emissions, payment services, credit rating agencies and benchmark regulations. It has proved itself to be a flexible and pragmatic tool, able to apply to different market dynamics and bottlenecks. Drawing out the common elements of this European FRAND access regime, the paper considers how it could be applied as a regulatory solution for dominant digital platforms.

Keywords: Access; competition law; data sharing; digital platforms; digital single market; FRAND; interoperability

Recommended citation: Mathew Heim and Igor Nikolic, A FRAND Regime for Dominant Digital Platforms, 10 (2019) JIPITEC 38 para 1.

A. Introduction

1 The European Commission is considering what role competition policy may play in addressing concerns linked to the market power of digital platforms.[1] The question is apposite, given that digital platforms can grow – and have grown – to significant scale and their market position, exacerbated by network effects, may soon appear unassailable. The impact of dominant digital platforms can also be felt on adjacent and downstream markets, whether as a result of multi-sided markets or possible leveraging. Yet applying traditional competition law doctrines to evolving technology markets raises a host of challenges for regulators.

2 In addition to more "classic" competition concerns, new issues, not traditionally within the competition policy space, are increasingly being voiced. These issues include the following: the importance of data as the fuel of the new economy; privacy and data protection; media plurality; and democratic health or the like.

* Mathew Heim, Tanfield Chambers, is also Senior Adviser to 4iP Council. Dr. Igor Nikolic is Assistant Professor at Tilburg University. This paper was drafted with the support of 4iP Council and expands on a scoping paper submitted to the European Commission on Sept. 29th, 2018 by 4iP Council entitled *A FRAND regime for dominant digital platforms? Contribution by 4iP Council to the European Commission's workshop on Shaping Competition Policy in the Era of Digitisation*. The opinions expressed in this paper are those of the authors and do not necessarily represent the opinions of 4iPCouncil nor its members.

1 See <http://ec.europa.eu/competition/scp19/>.

3 At the same time, the European Commission is also considering how to build a strong European policy that would leverage the data economy, artificial intelligence, the internet of things, blockchain and other key enabling elements to Europe's digital future,[2] in which competition enforcement may play a secondary role.[3] Classic competition enforcement is therefore but one of the tools available to policymakers in addressing some of the issues raised by dominant digital platforms.

4 This paper explores how European policy and legislation has addressed issues of access to critical goods or services in the past, in order to provide inspiration to the ongoing debate.

B. Summary

5 This paper reviews some of the practices of the European Union (EU) institutions when seeking to ensure access to critical infrastructure or inputs, whether through enforcement or regulation, and which can serve as inspiration to the European Commission in considering how to address dominant digital platforms. We focus on one particular access regime, that can be set up either *ex ante* or applied as an *ex post* remedial solution in order to enable fair-trading conditions between digital platforms and users. Ensuring trading between a dominant digital platform and others on Fair, Reasonable and Non-Discriminatory (FRAND) basis might be a very useful option, given that FRAND is a commonplace, flexible and proven mechanism that is relied on in both commercial agreements and regulation.

6 This paper starts from the position that dominant digital platforms will likely face regulation in one form or another.[4] The aim of the paper is to show that, on that assumption, the FRAND access regime has shown itself to be a flexible tool for managing platforms and could be applied as a safe harbour or a regulatory solution to dominant digital platforms.

7 The paper is structured as follows. We first review competition law issues surrounding the conduct of dominant digital platforms. Second, we look at the applicability of FRAND access principles in relevant competition cases. We then review the FRAND access concept applied in some key EU legislation governing standardisation; chemicals; electronic communications framework; public sector information; research framework; vehicles emissions, payment services; credit rating agencies and benchmark regulations. This is not a forensic review of European FRAND-based legislation but seeks instead to capture the principal examples thereof. Finally, we summarise some of the essential elements of the European FRAND regime before concluding.

C. Issues surrounding the application of competition law in regulating the conduct of dominant digital platforms

8 How to assess the effects of dominant digital platforms on competition and what, if anything, should be done is subject to an ongoing debate in the literature and policy circles.[5] The fundamental issue is that dominant digital platforms effectively create an ecosystem lock-in. This may be either because competition is often "for" the market not "on" the market, or because the platform functions as *de facto* gatekeeper to an ecosystem, pulling in service or content suppliers, intermediaries, customers or consumers.[6]

2 See European Commission, *Building a European Data Economy* (Communication) COM (2017) 9 final; European Commission, *Towards a common European data space* (Communication) COM (2018) 232 final; European Commission, *Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services* (Communication) COM (2018) 238 final 2018/0112 (COD); European Commission, *Artificial Intelligence for Europe* (Communication) COM(2018) 237 final. See also Begona Otero, *Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?*, 4iP Council, December 2018. Available at: <https://www.4ipcouncil.com/application/files/8315/4394/1658/Evaluating_the_EC_Private_Data_Sharing_Principles.pdf>.

3 For example, in its *Proposal for an online intermediation services Regulation* the European Commission acknowledges a lacuna in addressing "unilateral potentially harmful trading practices" by digital platforms that are not necessarily competition law infringements and which European competition law may therefore not address.

4 As Cremer put it, "*Given their societal importance, there will be strong regulations of platforms*". See Jacques Cremer presentation at ICLE/University of Leeds Annual Competition Law Conference 25 October 2018, Washington DC.

5 For example, the US Federal Trade Commission is currently looking at "the identification and measurement of market power and entry barriers, and the evaluation of collusive, exclusionary, or predatory conduct or conduct that violates the consumer protection statutes enforced by the FTC, in markets featuring "platform" businesses." See <https://www.ftc.gov/news-events/press-releases/2018/06/ftc-announces-hearings-competition-consumer-protection-21st>. See also the inquiry by the Australian Competition and Consumer Commission into the market power of digital platforms e.g. <https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry>. See also Khan, Lina, Amazon's Antitrust Paradox (January 31, 2017). Yale Law Journal, Vol. 126, 2017.

6 See US Senator Mark Werner's observation regard: "certain technologies serve as critical, enabling inputs to wider technology ecosystems, such that control over them can be leveraged by a dominant provider to extract unfair terms

9 Where the platform's role is central to the ecosystem and certain players are locked-in, the market position of a platform may be practically impossible to challenge. Nevertheless the question remains whether new players or new ecosystems can create effective competitive constraints on the platform or whether some competitive pressure needs to be maintained through regulation, in order to ensure that actors within the ecosystem have access to critical elements of the platform, especially to enable continued competition in secondary or associated markets.

10 Regulators around the world face a challenge to create a satisfactory framework to ensure fair access of consumers and users to digital platforms supporting an environment for innovation and competition in dynamic markets. After many years of exploration, including some enforcement decisions, there is no consensus on some critical issues, ranging from simple taxonomy, to the more complex issue of market definition; tipping points that connote-market power; the extent dominant platforms can distort competition; the welfare costs of intervention; or the difficulty of designing effective *ex post* remedies.[7] Enforcers continue to face difficulties in fitting classic competition analysis to this paradigm, yet as noted by Coyle "... without a greater degree of consensus about how to analyze competition in digital platform markets, including methodologies for empirical assessment, it will be impossible for the relevant authorities or courts to do anything other than feel their way along on a case by case basis".[8]

11 Is the existing competition assessment toolkit sufficient to catch abusive "dominant" digital platforms or does it need to be expanded? Tirole notes "With rapidly changing technologies and globalization, traditional regulatory tools have become less effective, causing competition policy to lag" and "Policymakers and regulators around the world must face the fact that the reasoning behind traditional competition measures is no longer valid".[9] Coyle suggests that rather than focusing on prices and consumer switching behaviour or traditional market definition, antitrust authorities should favour a wider assessment of the platform's market ecosystem, focusing "on the scope for disruptive technological innovation and the dynamic consumer benefits of investment".[10] Yet others question calls for a broadening of the consumer welfare standard. As Melamed & Petit note: "Unless critics intend to make antitrust law a general tool for attacking all sorts of inequalities in size, power and wealth unrelated to market competition, they will not be able to improve antitrust law by abandoning the [consumer welfare] standard in platform markets in particular and across industries in general."[11] To borrow a phrase from Fox, this debate is nothing less than a battle for the soul of competition law.[12]

12 Another aspect is whether the competition law system is able to play a part in addressing societal concerns created by supra-dominant platforms which, through their sheer size, have such a seismic impact on whole economies and even democracies. Should the "bigness" of the handful of "mega" platforms even be a concern of competition law? Should the standard of consumer welfare be expanded beyond the "classic" consumer to capture, for example, the individual as a data subject, as an employee or even a voter? Should data (or subset thereof) be considered an essential input, or should some dominant platforms be considered an essential facility?

13 If current competition law approaches contain inadequacies in addressing problems associated with dominant digital platforms, some suggest that legislation could be used to define new thresholds (e.g. user base, size, lock in) above which "certain core functions/platforms/apps would constitute 'essential facilities', requiring a platform to provide third party access on fair, reasonable and non-discriminatory (FRAND) terms and preventing platforms from engaging in self-dealing or preferential conduct".[13] In addition, legislation or regulation could ensure access to critical technology by requiring that dominant platforms maintain

---

from, or otherwise disadvantage, third parties". See White Paper, *Potential Policy Proposals for Regulation of Social Media Technology Firms* (2018) available at: <https://regmedia.co.uk/2018/07/30/warner_social_media_proposal.pdf>.

7 See Melamed, Doug and Petit, Nicolas, *The Misguided Assault on the Consumer Welfare Standard in the Age of Platform Markets* (October 30, 2018) Available at SSRN: <https://ssrn.com/abstract=3248140> or <http://dx.doi.org/10.2139/ssrn.3248140> (reviewing the debate).

8 See Diane Coyle, *Practical competition policy implications of digital platforms*, Bennett Institute for Public Policy working paper no: 01/2018, March 2018. At <https://www.bennettinstitute.cam.ac.uk/media/uploads/files/Practical_competition_policy_tools_for_digital_platforms.pdf>.

9 See Jean Tirole, *Regulating the disrupters*, Livemint, 1 January 2019 at <https://www.livemint.com/Technology/XsgWUgy9tR4uaoME7xtITI/Regulating-the-disrupters-Jean-Tirole.html>.

10 Coyle (2018), p 12. See footnote 9. See also Bamberger, Kenneth A. and Lobel, Orly, *Platform Market Power* (November 20, 2017). 32 Berkeley Technology Law Journal 1051 (2017); San Diego Legal Studies Paper No. 17-311; UC Berkeley Public Law Research Paper. Available at SSRN: <https://ssrn.com/abstract=3074717>.

11 Melamed & Petit (2018), p 42. See footnote 7.

12 Eleanor M. Fox, *The Battle for the Soul of Antitrust*, 75 Calif. L. Rev. 917 (1987).

13 Senator Mark Werner, White Paper, *Potential Policy Proposals for Regulation of Social Media Technology Firms* (2018). See Footnote 7.

Application Programming Interfaces (APIs) for third party access, thus achieving interoperability, under FRAND terms. However, even some who argue that the consumer welfare standard should be broaden acknowledge that competition law should not be used to make every successful platform a utility.[14]

14 It should be unnecessary to consider the "essential facilities" doctrines broadly. In elaborating coherent rules for emerging platforms that may reach a tipping point (and be conferred with the special responsibility that comes with market power), *ex ante* "remedies" can be devised to ensure that lock in does not occur. The issue only really arises when considering what should be done with existing "mega-platforms" and whether, after recognising a problem, a remedy can be fashioned that addresses various tensions of proportionality, effectiveness, as well as practicality, that are rooted in commercial reality.

15 This paper therefore explores existing practices relating to FRAND access in European law and policy as a possible practical framework to address situations where digital platforms are either found to be dominant or where platforms may wish, *ex ante*, to adopt a reasonable and pragmatic solution, in order to avoid allegations of market power or its abuse - and therefore forestall regulatory scrutiny.

16 The next sections will describe and analyse the applicability of FRAND access framework in EU competition law and legislation.

D. FRAND in the Context of Competition Law & Policy

I. Competition Policy and FRAND

17 The concept of "fair, reasonable and non-discriminatory" access is increasingly used by competition authorities as a "good faith" notion, applied as a competition law remedy to ensure the supply of a particular product or the access to specific infrastructure.[15] In particular, FRAND access remedies in competition cases have been used in both abuse of dominance and merger review cases and across a range of sectors.

18 From a theoretical perspective, it could be argued that Article 102 TFEU already embraces a FRAND-based notion; it eschews excessive prices[16] while promoting access and non-discrimination obligations,[17] as required under the "special responsibility" of dominant firms.[18] FRAND-based access remedies have been used in Article 102 TFEU compulsory licensing cases,[19] yet this does not mean that a compulsory licensing remedy should be broadly imposed on dominant digital platforms (unless exceptional circumstances can be established). We will see that European competition law already has some experience in applying FRAND-based access remedies, where the European Commission has sought to ensure market access but did not want to engage in setting precise prices or terms.[20]

14 Tim Wu, *Taking Innovation Seriously: Antitrust Enforcement if Innovation Mattered Most*, (2012), Antitrust Law Journal No. 2.

15 For instance, in the context of the *Microsoft* case the European Commission determined that Microsoft's operating system APIs was an essential input that Microsoft could not abusively refuse to license and required a FRAND-based access remedy. See also Case T-201/04, *Microsoft v. Commission*, 2007 E.C.R. II-3601, para 193. See also paras. 808 et seq. and para. 1231 and 1261. Petit notes that "... the 2018 Google Android case is a repeat of the 2004 Microsoft case, suggesting consistent support to the idea of keeping technology platforms open". See Petit, Nicolas, Competition Cases Involving Platforms: Lessons from Europe (October 17, 2018). Available at SSRN: <https://ssrn.com/abstract=3285277>), p.5.

16 A non-FRAND rate under the terms of contract law or as a regulatory solution cannot be automatically equated to exploitative abuse under competition law, which is of a higher threshold. See for example Case M.7995 *Deutsche Borse/London Stock Exchange Group*, para 106.

17 Article 102(c) TFEU. See also Melamed & Petit (2018). See footnote 7.

18 On special responsibilities of dominant firms see Case 322/81 *Nederlandsche Banden Industrie Michelin (Michelin I)* v *Commission* [1983] ECR 3461, paragraph 57; Case T-83/91 *Tetra Pak* v *Commission (Tetra Pak II)* [1993] ECR II-755, paragraph 114; Case T-111/96 *ITT Promedia* v *Commission* [1998] ECR II-2937, paragraph 139; Case T-228/97 *Irish Sugar* v *Commission* [1999] ECR II-2969, paragraph 112; and Case T-203/01 *Michelin* v *Commission* (*Michelin II*) [2003] ECR II-4071, paragraph 97. CaseC-209/10 *Post Danmark A/S v Konkurrencerådet*, EU:C:2012:172, paragraphs 21-23.

19 See e.g. Joined cases C-241/91 P and C-242/91 P, *RTE & ITP v Commission* [1995] ECR I-743, Case 418/01, *IMS Health v NDC Health*, [2004] ECR I-5039 and Case T-201/04, *Microsoft Corp. v Commission*, [2007] ECR II-3601. See for example European Commission decision of 21 December 1988 in case IV/31851 Magill TV Guide, para 27: "Accordingly the only remedy possible in the present case is to require ITP, BBC and RTE to supply each other and third parties on request and on a non-discriminatory basis with their individual advance weekly programme listings and to permit reproduction of those listings by such parties .... If they choose to supply and permit reproduction of the listings by means of licenses, any royalties requested by ITP, BBC and RTE should be reasonable".

20 FRAND competition remedies, like all regulatory measures, should also satisfy the principle of proportionality (See for example Case C-180/96 United Kingdom v Commission, I2265, para 96). Given that the FRAND regime is based on fairness and reasonableness, that it adopts commercial practices and imposes obligations of good faith on all parties, it is likely that the FRAND regime is limited to what is needed to address concerns, is the least onerous measure, and is proportionate to the aim envisaged. See also Cyril Ritter, *How Far Can the Commission Go When Imposing Remedies for Antitrust Infringements?*, Journal of European Competition Law & Practice, 2016.

19 There have now been a number of merger review cases in Europe where parties have agreed to adopt a FRAND-based behavioural remedy to ensure that existing market players or new entrants are placed in a position where they can effectively compete with the merged company.[21] The FRAND access remedy has been qualified as an "appropriate benchmark"[22] in a merger review and applied by different jurisdictions across diverse sectors, such as medical equipment, television broadcasting, music streaming licensing, payment processing, gas networks, flight search, missile systems, technology platforms and herbicides.[23] Lessons can therefore be drawn from cases where FRAND-based remedies have been accepted to address input foreclosure concerns by ensuring access to critical "must have" inputs (considered essential for third parties to compete effectively with the merged entity), including ensuring that customers are supplied on the same or similar terms to the merged entity's own business.

20 European competition authorities have specifically addressed the issue of ensuring interoperability between device interfaces or communications protocols, associated software and data management systems. In *Newscorp/Telepiù* access to platform APIs was ensured on FRAND terms, so far as was necessary to allow downstream pay-TV providers to develop interactive services compatible with the decoders and software used by the combined entity's platform's customers.[24] In *Siemens/Drägerwerk,* royalty free FRAND commitments were given to ensure continued interoperability between medical equipment platforms and hospital data management systems, including making available and maintaining all existing and future interfaces and communications protocols.[25] In *Worldline/Equens* the merging parties agreed to license on FRAND terms to payment network service providers (NSPs) within Germany key card and payment processing software, as well as the source code for the Poseidon software and the ZVT protocol, on which most German point of sale terminals run.[26]

21 It is worth noting that in *Worldline/Equens,* additional "flanking" commitments were offered to ensure that the FRAND remedy was effective. These include effectively capping software maintenance fees for 10 years; ensuring additional costs (e.g. maintenance services were also under FRAND terms); that NSPs' access would be prioritised over Worldline's PaySquare in case of shortage; including new modules and upgrades at no additional cost; that NSPs would have access to Poseidon source code for internal business use, in return for a one-off price-regulated fee; to place governance of the ZVT protocol with an external, independent not-for-profit, entity that would represent all market participants; that the Licensing Trustee would have access to all of Worldline licenses, contracts, pricing and invoicing conditions enabling it to effectively review the commitments, and that NSPs could seek more favourable terms if the Licensing Trustee considered PaySquare had advantageous terms; and set up a fast-track dispute resolution mechanism. Finally, as a compliance tool, a material breach of the remedies would result in NSPs having access to the source code free of charge.[27]

22 The *Newscorp/Telepiù* remedy is also worth further comment. During the Commission's investigation, third parties expressed concerns that the applicable European regulatory framework, which required those operators to offer access of digital television services on a FRAND basis to all broadcasters,[28] might not be sufficient to constrain likely foreclosure by Newscorp in the Italian pay-TV market.[29] The

21 The European Commission is by no means alone in its reliance on the FRAND principle in merger remedies. Competition authorities around the world are increasingly accepting FRAND-based remedies in a merger context including the US Department of Justice review of *Google/ITA* (2011), the US FTC review of Northrop *Grumman/Orbital* (2018), the decision of the Competition Commission of India and of MOFCOM of China in *Bayer/Monsanto* (2018), the decision of the South African Competition Tribunal in Dow/DuPont (2017) and the Japan FTC in *ASML/Cymer* (2012).

22 See *Liberty Global/De Vijver Media,* COMP/M.7194 (2015), para. 655. "...[T]he Commission considers that the reference to 'fair, reasonable and non-discriminatory terms' is the most appropriate benchmark to for the terms to which various types of TV distributors will be entitled under the commitments". See also paras. 624-5, and 672.

23 See cases referred to in footnotes 22, 23, 25-27. See also PRSfM/STIM/GEMA COMP/M.6800. where the joint venture partners agreed that the joint venture would offer key copyright administration services to other collecting societies on FRAND terms, when compared to the terms offered to the individual members of the joint venture. Also, access to physical infrastructure have been assessed as an essential input in: Hellenic Petroleum/British Petroleum Hellas SA, HCC 465/VI /2009. The Hellenic Competition Commission (HCC) imposed a FRAND commitment on Hellenic Petroleum (ELPE) whereby ELPE would grant access to third parties (wholesalers) to its storage facilities/depots in Crete under FRAND terms. See also *Contribution of Greece to the Roundtable on Remedies in Merger Cases* held by the OECD's Competition Committee (Working Party No.3 on Co-operation and Enforcement), June 2011. DAF COMP(2013)11, 30 July 2012.

24 *Newscorp/Telepiù,* COMP/M.2876 (2004).

25 *Siemens/Drägerwerk,* COMP/M.2861 (2013), para 154.

26 *Worldline/Equens,* COMP/M.7873 (2016). See also <http://europa.eu/rapid/press-release_IP-16-1462_en.htm>.

27 See also Paul McGeown, EU Merger Control 2016: *Behavioral Remedies, No Longer Taboo,* The Antitrust Report, LexisNexis, May 2017.

28 Notably the implementation of then Directive 95/47/EC, the Directive on Television Transmission Standards, and Directive 2002/19/EC, the old 'Access Directive' (see Section V.(f) below).

29 *Newscorp/Telepiù,* para 121 identifying specific concerns

European Commission found that cooperation with and by Newcorp or its subsidiary, NDS, was critical to enter the Italian pay-TV market. Most interestingly, the European Commission found[30] that given the technical difficulties for pay-TV operators both using a different CAS to NDS or implementing Simulcrypt obligations within a short period of time, it created a complete dependence on the combined entity from the technological viewpoint.[31] Newscorp's control of the technical platform would give it the possibility and the incentive to set the standard for the accepted level of "intra-platform" competition. The European Commission therefore imposed measures to effectively compel Newscorp to comply with the existing FRAND rules found within the legislative framework. In that context, while a monitoring trustee was appointed to ensure compliance with the remedies, disputes related to the licensing terms fall to be adjudicated to the Italian Communications Authority, the national regulatory authority responsible for safeguarding the implementation of the regulatory framework. *Newscorp/Telepiù* therefore agreed to allow access to the API so far as necessary to develop interactive services compatible with the decoders used by the Combined Platform's customers.[32]

23 In sum, the FRAND regime has now been applied by competition authorities in Europe (and indeed further afield) to ensure access to products and services across a range of sectors. FRAND access commitments have proved particularly useful and are the least intrusive remedies, where there is no adequate regulatory framework in place that addresses underlying competitive concerns.[33]

24 Competition law can therefore continue to ensure intra- and inter-platform competition by promoting access to critical inputs using a tried-and-tested regime that ensures a balance of interests, guaranteeing equality of arms in negotiations, minimising impact of regulatory intervention, and basing remedies on existing sector practices. Indeed, in setting out some lessons to be drawn from European competition cases involving platforms, Petit observes that while EU technology policy is premised on *ex ante* regulation, antitrust enforcement appears to effectively act as a "fact finding exercise or as a regulatory kick starter seconded by regulatory propositions, notably as relates to online platform regulation."[34]

25 Competition law policy is an important complement to broader European policy measures, but competition policy should not be primarily driven through cases: such an approach has significant flaws. First, imposing FRAND access as a merger remedy is opportunistic and dependent upon having a notifiable merger to begin with. If there is no relevant merger review where a FRAND access regime can be considered, alternative instruments should be considered to provide guidance to undertakings. In any event, FRAND access remedies would be merger-specific and could not necessarily be applied as a universal solution to dominant digital platforms across similar markets. The same can be said for other competition enforcement measures. Second, in non-merger cases, substantive competition law investigations are inherently slow. They typically last for several years during which market developments may often render any remedy too late to address pressing competitive concerns. In addition, enforcement cases are also fact-specific and companies under investigation should be confident that their case will not be "hijacked" for policy-making purposes. Finally, if cases end up in commitment decisions, any FRAND access remedy may provide little precedential value for other companies. Consequently, competition law remedies should be complemented by broader policy measures. There is therefore something to be said for a more structured competition approach to FRAND, especially given the jurisprudence already developed by the European Commission.

26 Competition law and national competition authorities may have a role to play in providing more structural guidance to companies. As Tirole notes, "rapidly changing technologies and globalization, traditional regulatory tools have become less effective, causing competition policy to lag", which requires more agile policies to be developed including "soft law" instruments.[35] From a competition perspective, formal guidance could well be useful where platforms risk creating silos

regarding technical services for pay-TV, and in particular conditional access systems being the likelihood that the new entity grant access to the NDS technology for CAS to potential new entrants under unfair terms and conditions; and that the new entity obstruct the entry of alternative pay-TV platforms with a different CAS system from that of NDS, leading to a virtual monopoly, in view of the fact that NDS would become the only CAS used in Italy.

30 *Newscorp/Telepiù,* para 140.

31 "A number of respondents in the market investigation have gone as far as considering NDS technology as a sort of 'essential facility' for the Italian pay-TV market". See *Newscorp/Telepiù,* para 124.

32 *Newscorp/Telepiù* Commitments, Part II, para 11.5.

33 FRAND remedies also address regulatory efficiency concerns as they are also self-policing, as a FRAND regime grants a clear cause of action before the courts to third parties harmed by exclusion or non-FRAND terms, as well as possible *ex post* regulatory actions under Article 102 (and what that would imply for remedies for findings of exclusion).

34 See Petit (2018). See footnote 15.

35 See Jean Tirole, Regulating the disrupters, Livemint, 1 January 2019, at <https://www.livemint.com/Technology/XsgWUgy9tR4uaoME7xtITI/Regulating-the-disrupters-Jean-Tirole.html>.

or proprietary ecosystems, locking out alternative players. A good example relates to the connected car, which will generate data of driver and passenger behaviour and experiences, automotive diagnostics, driving and road conditions that will feed into services related to driving and linked services. To what extent should the platforms controlling the accessing of this data seek to avoid walled-gardens or silos? While platforms should assess the risk themselves, guidance from the European Commission would be welcome if only to delineate scope of action.[36] There is sufficient jurisprudence in European law for the European Commission to provide guidelines on FRAND access regimes in relation to dominant digital platforms. This would not only help to ensure that binding access regimes are adopted *ex ante*, but could provide guidance to companies considering offering commitments to address competition concerns under Article 9 of Regulation 1/2003.

II. Competition Policy and "Standardisation FRAND

27 Patents essential for practicing a technology standard (Standard Essential Patents or SEPs) have recently been in focus, regarding the applicability of the EU's competition law to access to these patents. Technical standards can broadly be categorised as collaborative, when they are developed within the framework of Standard-Development Organisations (SDO), or *de facto*, when they are developed outside of any institutional framework of SDOs and achieve broad market acceptance to effectively become a standard on the market. Competition law in Europe has taken a FRAND-based approach to essential patents related to both collaborative and *de facto* standards.

28 FRAND licensing commitments, in the context of technical standards, are intended to ensure widespread access to a standard for implementers while, at the same time, providing adequate rewards and incentives to technology developers. Although FRAND commitments are voluntarily given by SEP owners to SDOs, the European Commission views that the existence of a FRAND policy will place the SDOs, and their contributing members, within the safe harbour of Article 101 TFEU.[37] Complying with the FRAND safe harbour means that there is, in principle, no need to undertake the often-complex task of assessing market power or dominance of SEP owners.

29 A FRAND commitment may also have an important impact on the availability of injunctive relief which, if granted by a court, may deny the infringer access to that standard. In the *Huawei v ZTE*,[38] the Court of Justice of the EU (CJEU) considered whether a SEP owner found to be dominant had abused that dominant position where it sought an injunction for the infringement of its SEP, to which a FRAND commitment had been made. The Court held, amongst other things, that a competition law defence could be raised by an infringer of an SEP against a request for an injunction, where a dominant SEP holder had not followed certain steps, including making a FRAND offer.[39] Following those steps creates a safe harbour for the SEP holder when requesting an injunction. However, the Court also set out certain steps that the infringer has to follow if they were to be able to avail themselves of such a defence. As a result, the Court set out a negotiating process that, where followed, should lead to a FRAND outcome. What *Huawei v ZTE* shows is that, in the event of a dispute, where both parties follow the steps required of them, access on a FRAND-basis is ensured and third parties are not unduly excluded on the basis of proprietary rights. It also shows, at a high level, that the Court built its decision around the FRAND commitment.

30 In the context of *de facto* standards, the German Bundesgerichtshof permitted a competition law defence to be raised where a patent infringer was not able to get a FRAND-like licence to a patent in a *de facto* standard, even where a FRAND commitment had not been made expressly or required by regulation.[40]

36 See Wolfgang Kerber, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, 9 (2018) JIPITEC 310 para 1.

37 European Commission *Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements*, (Communication) OJ C11, 14 January 2011. See para 279. In addition, the European Commission's *Technology Transfer Guidelines* go somewhat further, suggesting that FRAND commitments should be included in patent pools' self-assessment, whether or not these pools were licensing SEPs.

38 See *Huawei Technologies Co. Ltd v ZTE Corp., ZTE Deutschland GmbH*, Case C170/13, 16 July 2015, available at <http://curia.europa.eu/juris/document/document.jsf?docid=165911&doclang=en>.

39 See *Huawei v ZTE* para 54 of the CJEU ruling: "It follows that, having regard to the legitimate expectations created, the abusive nature of such a refusal may, in principle, be raised in defence to actions for a prohibitory injunction or for the recall of products. However, under Article 102 TFEU, the proprietor of the patent is obliged only to grant a licence on FRAND terms."

40 On the facts before it, the court clarified that the compulsory licence defence against the request for injunctive relief was only possible when the alleged infringer has made an offer to the patent proprietor that the patent proprietor could not reject without being anticompetitive, and behaves as if the patent proprietor had already accepted his offer. See Orange Book Standard, KZR 39/06, (Bundesgerichtshof—BGH, May 6, 2009).

31 In conclusion, EU competition law promotes licensing of SEPs on FRAND terms both by providing a safe harbour under Article 101 TFEU to SDOs, which have policies requiring FRAND commitments from their members and by ensuring a balanced path, based on good faith behaviour, to resolving SEP licensing disputes that would result in a FRAND agreement.

E. European Legislation, Regulation, Policies and FRAND

32 The notion of access on FRAND terms has also been used by the European legislature well beyond competition law. In pursuing public policy objectives, FRAND-based access has been applied across different sectors as a means of ensuring that critical inputs are made available for market participants. This creates a further useful source of European authority for the contention that the FRAND regimes is a suitable access remedy.

I. FRAND in the context of Standardisation Regulation

33 As mentioned, FRAND is a widely used notion in the context of licensing patents that are essential to practicing a technology standard. The FRAND commitment is voluntarily given by a technology contributor to an SDO. At its highest level, the FRAND commitment exists to ensure access to patented essential technologies on terms that are fair and reasonable for both licensor and licensee in order to, firstly, guarantee the uptake of new technologies and its wide diffusion, and secondly, encouraging valuable technology contributions to be made to standardisation efforts (thus encouraging further incentives to innovate in future standardisation).[41] The FRAND regime therefore seeks to balance competing interests of different players and making standardisation an attractive enterprise for all kinds of business models. Depending on the jurisdiction, a FRAND commitment is usually an enforceable defence under contract law or other principles such as quasi-contract, estoppel and in some instances antitrust law.[42]

34 Standards are a typical example of the creation of an innovation platform, done openly and transparently. As Tsilikas noted: "Collaborative standardization under the auspices of [SDOs] has, thus far, a remarkable record of breakthrough technological achievements, high-quality, cutting-edge standards, vibrant follow-on innovation in the implementation of standards and open, competitive upstream and downstream markets. Standardization in wireless telecommunications is driven by an inexorable dynamic: more innovative standards, services and products increase consumer demand and increased consumer demand calls for more investment in R&D, more innovation and better-performing interoperability standards."[43]

35 Core to that openness and transparency is the access to essential technology through the FRAND regime. The FRAND regime has empirically led to hugely successful results, ensuring both broad access to and wide dissemination of advanced technologies.[44]

36 What the precise rights and obligations are that the FRAND regime creates depends on the intention of the parties (usually set out in the SDO's IPR policy) and the specificities or usual practices of the particular industry.[45] The flexibility of the FRAND commitment has led it to be broadly adopted by SDOs across the board, notably the formal EU standardisation

41 See the European Commission, *Setting out the EU approach to Standard Essential Patent* (Communication), COM(2017) 712 final, 29 November 2017. Moreover, SDOs typically follow certain principles established by the World Trade Organisation that ensure that an SDO is business neutral. See more on the principles, such as openness, consensus based, transparency, and impartiality at Fredrik Nilsson, *Appropriate base to determine a fair return on investment: A legal and economic perspective on FRAND*, GRUR Int. 2017, 1017.

42 National SEP litigation tends to focus mainly on non-competition elements, see for example *Huawei v. Unwired Planet*, [2017] EWHC711(Pat) and the Court of Appeal review of that decision [2018] EWCA Civ 2344 or the repository of post-*Huawei v ZTE* national case law at <https://caselaw.4ipcouncil.com/>.

43 Tsilikas, Haris, *Collaborative Standardization and Disruptive Innovation: The Case of Wireless Telecommunication Standards* (May 17, 2016). Max Planck Institute for Innovation & Competition Research Paper No. 16-06. Available at SSRN: <https://ssrn.com/abstract=2783372>.

44 For example, between 2005 and 2013, the average mobile subscriber cost per megabyte decreased 99 percent, mobile network infrastructure costs were reduced by 95 percent, and 4G networks were able to transfer data 12,000 times faster than 2G networks. See Boston Consulting Group, *The Mobile Revolution*, January 2015. According to GSMA by 2025 5G networks are likely to cover one-third of the world's population. See more at <https://www.gsma.com/futurenetworks/technology/understanding-5g/5g-innovation/>.

45 There are international SDOs that do not use the exact expression "FRAND" in their IPR policies yet achieve the same result. SAE International, for example, is a US-based organisation that, inter alia, develops voluntary consensus-led standards covering aspects of design, construction, performance, durability, and promotes for commercial vehicle and automotive engineering. Within the context of patents in SAE's IPR policy, patents and patent applications can be included provided that SAE receive either a general disclaimer from the patent holder that they will not enforce any of their IP against implementers or that they state that "a license will be made available to all applicants without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination." See <https://www.sae.org/binaries/content/assets/cm/content/about/sae-ip-policy.pdf>.

bodies, ETSI and CEN/CENELEC, as well as numerous informal standards organisations.[46] As a result, this industry-led solution has been enshrined in the European Standardisation Regulation,[47] and broadly promoted in European standardisation policy,[48] as part of the regulatory framework around standards development and dissemination.

37 Indeed, the European Commission's recent FinTech Action Plan notes that that "An EU-wide FinTech market will not reach its full potential without the development of open standards that increase competition, enhance interoperability and simplify the exchange of and access to data between market players".[49] Implementing such interoperability can be done through *ad hoc* interfaces, which raises efficiency and competition issues, or interoperability standards for the whole market on the basis of the principles within the European Standardisation Regulation which, as noted above, seeks to ensure effective access through FRAND terms.

38 As a final note, the negotiation framework devised by the CJEU in *Huawei v ZTE* could provide inspiration for other non-SDO situations. In *Huawei v ZTE* the CJEU required the holder of the essential input to set out clearly what the input consisted of as well as its price, where upon the customer, having all the elements necessary to take a decision, has to accept to negotiate and diligently agree to the offer or make a reasonable counter offer.[50] Such a process is attractive as a policy solution, but it has to be acknowledged that the system was devised in the event of an inability by the parties to reach agreement and on the basis that one party had already committed to allow access to some of its technologies on FRAND terms. It cannot be used as a procedural straight jacket, as parties could well reach agreement outside of such a process.[51]

II. The Regulation for the Registration, Evaluation, Authorisation and Restriction of Chemicals

39 The Regulation for the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)[52] creates a FRAND-like access framework for sharing previously submitted reports and data between companies. In particular, it creates a framework whereby the holder of this critical information (entities that have previously registered particular chemicals) and a potential registrant "make every effort to ensure that the costs of sharing the information are determined in a fair, transparent and non-discriminatory way".[53] It is notable that REACH echoes a central tenet in *Huawei v ZTE*, where the European Court imposes obligations on both licensor and potential licensee to seek agreement in good faith. REACH also provides for rules on cost-sharing (notably where there is no agreement found between the parties), as well as a dispute resolution mechanism, while respecting access to courts.

40 In considering data sharing requirements, Drexl notes that REACH contains certain features "that could be used as guidance for similar legislation in other fields".[54] These include: (i) the public interest

46 Tim Pohlman, Knut Blind, *Landscaping Study on Standard Essential Patents* (2016) p. 36 (finding that 68% of all declared SEPs are licensed under FRAND terms, while the remaining 32% do not specify licensing conditions); Justus Baron & Daniel Spulber *Technology Standards and Standard Setting Organisations: Introduction to the Searle Center Database* (2018) 27 *Journal of Economics & Management Strategy* 462 (studying IPR policies of 37 SSO and find that 32 SSOs allow for FRAND licensing, with the remaining 5 SSOs require royalty-free licensing).

47 See the European Standardisation Regulation No 1025/2012, 25 October 2012, which seeks to create "an effective and efficient standardisation system which provides a flexible and transparent platform for consensus building between all participants" and requires that for technical specifications to fall under the Regulation they be covered by the FRAND regime, reflecting WTO norms.

48 See e.g. the European Commission, *Intellectual Property Rights and Standardization* (COM(92) 445 final), 27 October 1992; or the European Commission, *Digitising European Industry: Reaping the full benefits of the Digital Single Market*, (Communication), COM(2016) 180 final; or European Commission, *ICT Standardisation Priorities for the Digital Single Market* (Communication) COM(2016) 176 final of 19 April 2016; or the European Commission, *Setting out the EU approach to Standard Essential Patents* (Communication) COM(2017) 712 final, 29 November 2017.

49 European Commission, *FinTech Action plan: For a more competitive and innovative European financial sector* (Communication), Brussels, 8.3.2018 COM(2018) 109 final.

50 Claudia Tapia and Spyros Makris, *Negotiating SEP licenses in Europe after Huawei v ZTE: guidance from national courts*, Managing Intellectual Property, May 2018. Available at <https://www.4ipcouncil.com/application/files/1315/3018/6300/21-29_article_SEPs.pdf>.

51 In *Unwired Planet v. Huawei*, the Court of Appeal found that "We have come to the firm conclusion that the CJEU was not laying down mandatory conditions at [70] of its judgment such that non-compliance will render the proceedings a breach of Article 102 TFEU..." [2018] EWCA Civ 2344, para 269.

52 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (Text with EEA relevance).

53 See REACH Article 27(3) and 30(1).

54 Josef Drexl, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, 8 (2017) JIPITEC 257.

in creating the access regime; (ii) a framework of contractual negotiations favouring "a pro-market solution over direct government intervention";[55] (iii) a concrete base for calculating compensation, relying on the cost for undertaking the relevant study; (iv) a mechanism for dispute resolution "that enables the public interest to prevail and that provides sufficient legal certainty for the parties when they assess whether it makes sense to depart from that rule".[56] One particularly interesting aspect in looking to REACH as inspiration for FRAND-based access regimes is that the public interest is broader than ones that traditionally have resulted in compulsory licensing regimes.

41 Further, as Drexl notes, the REACH framework relies on bilateral commercial negotiations to determine the conditions for a pro-competitive solution.[57] While the REACH legislation does not engage in price-setting, which is so difficult for a legislature to get right, REACH does provide cost "metrics" in the event that no agreement can be arrived at; costs are limited to sharing the proportionate costs of information necessary to satisfy registration requirements.[58] Therefore legislation can provide guideposts to the parties in the event of a dispute, but the legislation need not get engaged in creating value homogeneity. These metrics are, however, specific to the scope of REACH related to the sharing of scientific studies and data and so are generally not applicable to other sectors.

III. European Electronic Communications Code

42 The recently adopted European Electronic Communications Code (EECC) provides updated EU-wide telecommunication rules.[59] It contains a number of provisions providing for access to and interconnection of electronic communication networks on terms that are fair, reasonable and non-discriminatory, or similarly-phrased terms.

43 For instance, the EECC allows National Regulatory Authorities (NRAs) to require operators to interconnect their networks and make their services interoperable;[60] provide access to wiring and cables facilities;[61] share passive infrastructure and conclude localised roaming access agreements.[62] Under all these scenarios, access and interconnection conditions must be objective, transparent, proportional and non-discriminatory. While such conditions are not further defined in the EECC and are to be further elaborated by NCAs, they substantively resemble a FRAND obligation.[63]

44 Moreover, in certain instances the EECC specifically allows NRAs to impose FRAND-based access obligations. For example, NRAs may require access on FRAND terms to cables and wiring beyond the first distribution point;[64] access to relevant facilities in order to ensure accessibility for end-users to digital radio and television broadcasting services;[65] and access to technical services enabling digitally-transmitted services to be received by viewers or listeners by means of decoders.[66] Additionally, holders of IP rights needed to access products and systems should ensure that licences to manufacturers of consumer equipment are on FRAND terms.[67]

45 Besides the above obligations that are applicable to all operators, a specific regulatory regime applies to operators found to have "significant market power" (SMP). Namely, NRAs may impose a number of obligations on such operators, such as the obligation of transparency, requiring operators to make public their terms and conditions for interconnection

55 Ibid. Drexl (2017), at para 180, also considers that a REACH-like access regime could also be implemented in situation where there is no additional public interest, arguing that this "would make sense if it is devised as a non-mandatory procedural framework for negotiations on access to information" and considers that the negotiation framework devised by the European Court in Huawei v ZTE "could especially be applicable for cases in which the holder of information publicly commits to grant access to data on FRAND terms".

56 Ibid. Drexl (2017), para 179.

57 Ibid. Drexl (2017), para 180.

58 See also the European Chemical Agency's Guidance on Data Sharing at <https://echa.europa.eu/documents/10162/23036412/guidance_on_data_sharing_en.pdf/545e4463-9e67-43f0-852f-35e70a8ead60>.

59 Directive (EU) 2018/1972 of 11 December 2018 establishing the European Electronics Communication Code, L 321/36.

60 EECC, Article 61.2.

61 EECC, Article 61.3, which is applicable if it can be shown that replicating these elements would be economically inefficient or physically impracticable.

62 EECC, Article 61.4.

63 One question arises as to why these provisions apply FRAND-like concepts of "objective, transparent, proportional and non-discriminatory", were as other sections of the Directive adopt the express FRAND conditions and whether these would be materially different. No reason is immediately forthcoming, although one explanation is that the term "objective, transparent, proportional and non-discriminatory" appears to have been included in the EEC, while FRAND wording was drawn from the old Access Directive (Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive), OJ L 108, 24.4.2002, notably Recital 10, Article 5.1.b and Annex I, Part I 2(b) and (c)).

64 EECC, Article 61.3 paragraph 2.

65 EECC, Article, 61.2.d.

66 EECC, Annex II.

67 Ibid.

and access, including information on pricing;[68] the obligation of non-discrimination treatment of other similarly situated companies;[69] or even the direct price control measures for interconnection and access.[70] The reasons for regulating operators with SMP is to ensure *ex ante* competition is maintained, when traditional *ex post* competition law remedies may not be sufficient nor adequate to safeguard effective competition in the telecommunications market.

46 The EECC therefore contains FRAND-based access regimes to networks, infrastructure and content. It is primarily managed by NRAs, who are best placed to assess the situation on the ground, given the nature of the markets. These access regimes are imposed in order to satisfy various public policy objectives, including ensuring full end-user connectivity, resolve infrastructure bottlenecks or safeguard *ex ante* competition, as an adjunct to *ad hoc* competition enforcement. The EECC thus shows that European legislation does not shy away from mandating access to critical infrastructure in order to satisfy broader policy objectives.

47 Interestingly, the EECC also includes an obligation to provide interoperability between "interpersonal communication services", which reach a significant level of coverage and user uptake.[71] This provision may arguably be used by NRAs to impose an obligation on widely used communication applications or social platforms to interoperate.[72] However, such regulatory interventions may be possible only where end-to-end connectivity is endangered and only to the extent necessary to ensure connectivity between end-users.[73] Nevertheless, this provision represents an evolution in providing a regulatory solution to ensuring interoperability between particular types of platforms that have a significant reach, though it may not be dominant in the competition law sense. The FRAND-based remedy is available to satisfy the broad public interest objectives found in the EECC, that include ensuring freedom of expression and information, as well as media pluralism, access to and take up of very high capacity networks and promotion of competition in the provision of electronic communications networks and associated facilities.[74]

IV. Public Sector Information Directive

48 Directive 2003/98/EC (amended by the Directive 2013/37/EU) on re-use of public sector information, introduces FRAND-based access conditions to enable access to such information.[75] Rather than referring expressly to the expression "fair, reasonable and non-discriminatory", the Directive fleshes elements to access public sector information including reasonable remuneration, non-discriminatory access and transparency, which are central elements to FRAND-based regimes.

49 In detailing the conditions for access to public sector information, the Directive sets out the following FRAND-based elements:

- Public sector bodies may charge fees for supplying and allowing access to the information. The principles governing charging under Article 6 note that "charges shall be limited to the marginal costs incurred for their reproduction, provision and dissemination".[76] However, the marginal cost default does not apply where public sector bodies are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks or, exceptionally, for documents for which the public sector body is required to generate sufficient revenue to cover a substantial part of the costs relating to their collection, production, reproduction and dissemination. Libraries, including university libraries, museums and archives are not bound by the marginal cost default, in order not to hinder their normal running.[77]

- Article 6 also sets out how total charges shall be calculated "according to objective, transparent and verifiable criteria to be laid down by the Member States. The total income of those

68 EECC, Article 69.

69 EECC, Article 70. See also Commission, 'Recommendation on Consistent Non-discrimination Obligations and Costing Methodologies to Promote Competition and Enhance the Broadband Investment Environment' 2013/466/EU (guide on interpreting the non-discrimination requirement in electronic communications legal framework).

70 EECC, Article 74.

71 EECC, Article 61.2.c.

72 See Wolfgang Kerber, Heike Schweitzer, 'Interoperability in the Digital Economy' (2017) 8 *JIPITEC* 39, 50-51.

73 EECC, Article 61.2.c.

74 EECC, Article 3.

75 Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information as amended by the Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013, 2003L0098 (consolidated text) (PSI Directive). The PSI Directive is currently under review and a proposal for new directive has been made, see: Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information (recast) COM/2018/234 final – 2018/0111 (COD).

76 See also Recital 22 of Directive 2013/37/EU. Recital 24 notes that the upper limits for charges set in the Directive are without prejudice to the right of Member States to apply lower charges or indeed no charges at all.

77 See Recital 23 of Directive 2013/37/EU.

bodies from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction and dissemination [where relevant the preservation and rights clearance], together with a reasonable return on investment. Charges shall be calculated in line with the accounting principles applicable to the public sector bodies involved." Of note is Recital 23 that acknowledges that, when calculating a reasonable return on investment, libraries, museums and archives can consider the prices charged by the private sector for the re-use of identical or similar documents.[78] Given the specific context of public sector data, the Directive can provide guide points on what elements to consider in calculating fees (which is admittedly easier than calculating fees for e.g. private sector R&D intensive innovation).

- The requirement for non-discrimination is further specified in order to ensure free exchange of information between public sector bodies when exercising public tasks, "whilst other parties are charged for the re-use of the same documents", including differentiated charging policy for commercial and non-commercial re-use.[79]

- The Directive requires that applicable conditions and the actual amount of those charges should be transparent (i.e. pre-established and public), including (on request) the calculation basis for charges and what factors should be taken into account in the calculation of charges for atypical cases.[80] This approach mirrors to some degree the behavioural aspect to FRAND licensing for SEPs set out in *Huawei v ZTE* and the European Commission's call for transparency and predictability in SEP licensing.[81]

- Highlighting the importance of broad access, the Directive notes that where public sector bodies allow for re-use of documents, conditions should not unnecessarily restrict possibilities for re-use. In particular, conditions should not be used to restrict competition,[82] and must be non-discriminatory for comparable categories of re-use (rather than users), notably where re-use also occurs by the commercial activities of public sector bodies.[83] Re-use is open to all potential actors and the Directive expressly prohibits the application of exclusive rights (except for the digitisation of cultural resources).[84]

V. Regulation Horizon 2020

50 The European Union's Framework Programme for Research and Innovation (Horizon 2020) is governed by Regulation 1290/2013,[85] that lays down the rules for participation and dissemination in Horizon 2020 over the years 2014-2020. In general, it can be said that the EU's "Horizon 2020" Framework Programme applies a FRAND-based model to enable access to the results of EU-funded projects, with the overarching principle for access being one of fairness and reasonableness. Article 48 of that Regulation covers access rights for exploitation and notes that, whether linked to access between project participants of the results or background information, or other, such access shall be granted under fair and reasonable conditions (subject to agreement).

51 The Commission's own Model Grant Agreements for the EU's "Horizon 2020" Framework Programme applies the model set out in the Regulation and, together with the Regulation provides an understanding of the EU's interpretation of FRAND access as a condition for accessing the results of European funded research.[86] It covers the rights of participants to the agreement ("beneficiaries" of funding) to have access under fair and reasonable conditions to each other's results (relevant background input held by participants prior to their accession to the project) that are needed for exploiting their own results.[87] Such access conditions apply where beneficiaries give each other access to the results needed for implementing their own tasks (or to other beneficiaries or affiliated entities).[88] In addition, there are options to require (when foreseen in the work programme) access to third parties for additional access rights for interoperability under fair and reasonable or royalty free conditions.[89]

78 Ibid.

79 See Recital 19 of the PSI Directive.

80 See Article 7 of the PSI Directive.

81 See Section V. a) above.

82 See Article 8(1) of the PSI Directive.

83 See Article 10 of the PSI Directive.

84 See Article 11 of the PSI Directive.

85 Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Regulation (EC) No 1906/2006. OJ L347/81, 20.12.2013.

86 See the H2020 Programme Multi-Beneficiary Model Grant Agreement of October 2017 at <http://ec.europa.eu/research/participants/data/ref/h2020/mga/sme/h2020-mga-sme-2-multi_en.pdf>.

87 Ibid, Article 25 (access is restricted if the beneficiary holding the background has notified others prior to signing the Agreement that access to its background is subject to legal restrictions or limits).

88 Ibid, Article 31.

89 Ibid, Article 31.6.

52 Article 2(1)(10) of the Regulation defines "fair and reasonable conditions" to mean "appropriate conditions, including possible financial terms or royalty- free conditions, taking into account the specific circumstances of the request for access, for example the actual or potential value of the results or background to which access is requested and/or the scope, duration or other characteristics of the exploitation envisaged".[90] This definition applies to all the access situations described above.[91]

53 It is notable that, no matter whether the access requirements relate to members of the consortium or their affiliates, whether for fulfilling their tasks, for exploiting their own efforts, or as relates to third parties (in relation to interoperability), the access regime remains the same. One can assume that "fair and reasonable" was considered by the legislature as flexible enough to deal with this broad range of interests and situations. For this reason, the definition implies that conditions can change depending on the circumstances of the request for access (i.e. the nature of the parties), as well as depending on the subjective nature of value or "other characteristics". Again, while not using the expression "FRAND", it can be assumed that the non-discriminatory aspect is included, as the definition specifically allows for differentiation where such a differentiation can be made.

VI. Vehicle Emissions Regulation

54 European Regulation (EU) 715/2007, relating to emissions from light passenger and commercial vehicles and access to vehicle repair and maintenance information, contains a FRAND-based information sharing regime. It imposes specific obligations on vehicle manufacturers to enable access to vehicle repair and maintenance information both to authorised and independent dealers and repairers.[92] Such access is on a non-discriminatory basis while permitting manufacturers to charge a "reasonable and proportionate fee".[93] However, the Regulation also notes that such fee is not reasonable or proportionate "if it discourages access by failing to take into account the extent to which the independent operator uses it", making it clear that the fee also needs to be in proportion to the importance of the information to the user as well as a reasonable value to the manufacturer.[94]

55 Although not using the exact "FRAND" wording, the Vehicle Emissions Regulation very much mirrors the FRAND intention of ensuring that fees are reasonable and non-discriminatory, while at the same time not discouraging access.

VII. Directive on Payment Services

56 The revised Directive on Payment Services in the Internal Market[95] of 25 November 2015 sets out that account servicing payment service providers, such as banks, must allow third parties to obtain real-time data relating to customers' accounts on a non-discriminatory basis (including without any discrimination in terms of charges, timing and priority).[96] Colangelo and Borgogno query whether banks can charge a fee for the access to front-end third-party providers and speculate that such compulsory access can be compensated, "as it happens, mutatis mutandis, with standard essential patents that are licensed under fair, reasonable and non-discriminatory ("FRAND") terms".[97] We agree that such access would be on the basis of FRAND principles, in accordance with the recognised commercial practices in the payment services field (rather than SEPs, *per se*). One can presume that where European regulation requires access to data and interoperability, such access must be on FRAND terms.

90 Regulation 1290/2013, Article 2(1)(10).

91 Ibid, Article 25(3). Note that under Article 31, a distinction is drawn between royalty-bearing and royalty free, as these two options are given. However, logic would dictate that "fair and reasonable" includes royalty free in the range of royalties (as expressly noted in the definition of Article 25(3)) and because there are usually other material terms and conditions in licensing agreements that should also be fair, reasonable and non-discriminatory.

92 Vehicle Emission's Regulation, Article 7(1).

93 Ibid.

94 Regulation (EC) 715/2007 of the European Parliament and of the Council on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information [2007] OJ L 171/1. See also Benoit Van Asbroeck Julien Debussche Jasmien César, *Building the European Data Economy & Data Ownership*, 1 January 2017. Available at <https://www.twobirds.com/en/news/articles/2017/global/data-ownership-in-the-context-of-the-european-data-economy>.

95 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

96 Ibid, Articles 64-68.

97 Colangelo and Borgogno, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*, Stanford-Vienna European Union Law Working Paper No. 35, 2018, <http://ttlf.stanford.edu>. Page 16

VIII. Credit Rating Agency Regulation

57 The European Regulation 462/2013 of 21 May 2013[98] amending Regulation No 1060/2009 on credit rating agencies included a FRAND-like requirement. As noted in recital 38, fees charged by credit rating agencies to their clients should not be discriminatory, although charging for the same type of service to different clients can be justified by a difference in the actual costs in providing this service. New Article 3(c) goes further in setting costs parameters by requiring credit rating agencies to ensure that fees are based on the actual costs of providing the service and cannot be affected by either the level of the credit rating issued nor on any other result or outcome of the work performed. It would be logical to assume that costs for developing better software etc. would be included in the "actual" cost of assessing a customer's credit rating. Otherwise the incentive to improve credit rating services would be affected. In addition, recital 33 imposes a transparency and oversight requirement, requiring credit rating agencies to disclose to the European Securities and Markets Authority their general policies and fees received from each of their clients, in order to allow for the effective supervision of the rules.

IX. EU Benchmarks Regulation

58 The pricing of many financial instruments and contracts rely on the accuracy of benchmarks. However, following the serious manipulation of LIBOR, EURIBOR and other benchmarks by various cartels[99] and the impact that the failure of critical benchmarks can have on market integrity, financial stability, consumers, the real economy, or the financing of households and businesses, the EU adopted the Benchmarks Regulation.[100] Specifically to mitigate the market power of critical benchmark administrators and bring discipline to the market, the Regulation contains a FRAND regime imposing, under Article 22, the obligation on administrators of critical benchmarks, including critical commodity benchmarks,[101] to take "adequate steps to ensure that licences of, and information relating to, the benchmark are provided to all users on a fair, reasonable, transparent and non-discriminatory basis".[102] This requirement is without prejudice to the application of EU competition law.

X. European Commission Policy Discussions for FRAND Access to Data

59 The Commission is already considering the possibility of sharing the access to data between businesses, with FRAND access being one of the considered models. In 2017 the Commission published a Communication entitled "Building a European Data Economy". In relation to access to data, the Commission explored the idea of applying a FRAND regime, whereby access to machine generated data would be granted against remuneration.[103] The Communication notes that: "A framework potentially based on certain key principles, such as fair, reasonable and non - discriminatory (FRAND) terms, could be developed for data holders, such as manufacturers, service providers or other parties, to provide access to the data they hold against remuneration after anonymisation. Relevant legitimate interests, as well as the need to protect trade secrets, would need to be taken into account. The consideration of different access regimes for different sectors and/or business models could also be envisaged in order to take into account the specificities of each industry. For instance, in some cases, open access to data (full or partial) could be the preferred choice both for firms and for society."[104]

98 Regulation (EU) No 462/2013 of the European Parliament and of the Council of 21 May 2013 amending Regulation (EC) No 1060/2009 on credit rating agencies Text with EEA relevance. OJ L 146, 31.5.2013, p. 1–33.

99 See e.g. Boot, Nuria and Klein, Timo and Schinkel, Maarten Pieter, *Collusive Benchmark Rates Fixing* (May 1, 2018). Tinbergen Institute Discussion Paper 2017-122/VII. Available at SSRN: <https://ssrn.com/abstract=3117398>.

100 Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds and amending Directives 2008/48/EC and 2014/17/EU and Regulation (EU) No 596/2014 (Text with EEA relevance). OJ L 171, 29.6.2016, p. 1–65. See Recital 35.

101 Ibid, Recital 38

102 See also, for example, the UK Financial Conduct Authority policy statement also requiring regulated benchmark administrators to grant access to and licenses to use benchmarks on a FRAND basis See PS16/4, February 2016. For example, para 1.9 states "In summary, our proposals required regulated benchmark administrators to grant access to and licences to use benchmarks on a fair, reasonable and non-discriminatory basis, including with regards to price. We proposed that such access should be provided within three months following a written request. We proposed that different fees should be charged to different users only where this is objectively justified, having regard to reasonable commercial grounds such as the quantity, scope or field of use requested. Our proposals also set out a list of non-exhaustive factors that we may consider in assessing whether the terms of access to a benchmark are FRAND".

103 European Commission, *Towards a common European data space* (Communication), COM(2018) 232 final.

104 Ibid, page 13.

60 The Communication highlights that a FRAND regime is business model neutral, recognising that data will have a value to the owner, while permitting both remuneration-based, as well as free access, and is flexible enough to take different sectorial interests and regulatory parameters (in this case anonymisation) into account. The Staff Working Document (SWD) accompanying the Communication acknowledges that inspiration can be found across a range of instruments, including some of those explored in the sections above.[105]

61 Following a public consultation, the Commission in 2018 published a Guidance on Sharing Private Sector Data in the European Data Economy.[106] It recommended companies to consider voluntarily granting access to non-personal data to other businesses and, when doing so, to adhere to certain principles related to transparency, respect to each other's commercial interests, to ensure undistorted competition, and minimise lock-in.[107] The Commission at least appears to recognise that the problems raised by big data and dominant digital platforms could be resolved by some form of data sharing requirement on principles that mirror notions protected by the FRAND regime.

F. The Nature of FRAND under European Law

62 We see FRAND-based access regimes applied by European legislation across multiple sectors and activities, fostering the sharing essential technologies or access to critical inputs in both regulated and unregulated sectors. These FRAND access regimes are imposed to promote various public interests relating to both private and public sector bodies. The nature of the entities that control the critical input is also varied. In some instances, the entities may possess or are likely to possess market power, in other instances the input is critical for market activity yet not necessarily critical to market access. In some instances, FRAND is applied in the context of disputes with particular steps in order to ensure access on reasonable terms. This shows the flexibility of the FRAND regime, which can apply to different players and in different circumstances.

63 The core elements of a FRAND regime can be summarised. At a high level, the purpose of the FRAND regime is to ensure broad and non-discriminatory access to the relevant input. Where legal relations need to be regulated, such access will often be though a license or similar agreement, but where access is guaranteed, a separate agreement may not be required. Its aim is to ensure the widest possible market access and use of the input, while avoiding lock-in, hold up, or foreclosure.

64 From the regulatory FRAND examples highlighted above, the Standardisation Regulation and EECC expressly refer to the term "fair, reasonable and non-discriminatory" while leaving the details of the arrangement to the market. The other examples use access regimes that are essentially identical to FRAND in all but the express wording, creating FRAND-based conditions of balance, reasonableness, non-discrimination and transparency. In fact, it is arguable that the FRAND regime used by the European institutions is a general principle and that a FRAND policy need not reflect those exact words, in that exact order, in order to achieve the same result. It would be difficult to argue that those laws that do not use the exact expression "FRAND" somehow grant access on a significantly different basis.

65 The various examples of European regulation each provide, to some degree, greater guidance on the detail FRAND-like regimes, displaying significant consistency across the board. In particular:

- **Fair & Reasonable balance:** Legislation covering REACH, the European Vehicle Emissions Regulation, the Public Sector Information Directive and the Horizon 2020 Regulation, provide parameters and guide points on calculating payment ("compensation", "income", "charge", "financial terms"), emphasising the balance between costs/investment over use/access and reflecting the different interests of the parties.

- **Transparency:** In addition, the Re-use of Public Sector Information Directive focuses on transparency of terms and conditions, including (on request) the calculation basis for the fee, mirroring *Huawei v ZTE* requirements for FRAND licensing of SEPs. In REACH and *Huawei v ZTE*,

105 European Commission Staff Working on the free flow of data and emerging issues of the European data economy. Accompanying the document. Communication Building a European data economy, 10.1.2017 SWD(2017) 2 final. A number of academics such as Drexl (footnote 56) or Daniel L. Rubinfeld & Michal Gal (see *Access Barriers to Big Data* (August 26, 2016). 59 Arizona Law Review 339 (2017). Available at SSRN: <https://ssrn.com/abstract=2830586> or <http://dx.doi.org/10.2139/ssrn.2830586>) also seized upon FRAND as a model to replicate in the data context. Van Asbroeck, Debussche & César (footnote 95) argue at p 85, that "Providing more favourable access conditions in case of sole-source databases could be a particularly interesting course of further analysis. It could also be examined whether some of the outstanding access to data issues could be solved by using open licences allowing for commercial re-exploitation and re-utilisation of the information on fair and non-discriminatory terms."

106 European Commission, *Guidance on Sharing Private Sector Data in the European Economy* (Communication), SWD(2018) 125 final.

107 Ibid, p.3.

both the holder of the critical input and the user have an obligation to find a fair and reasonable result.

- **Non-Discrimination:** In the Re-use of Public Sector Information Directive, public sector bodies will not discriminate if they grant free access to another public body fulfilling a public sector task, while commercial parties can be charged for the re-use of the same documents. The Horizon 2020 Regulation applies a "fair and reasonable" definition that enables differentiation where this can objectively be made (and it can therefore be assumed that non-discrimination is implicitly included).

- **Dispute Resolution**: In order to achieve the FRAND balance, there is an obligation on both parties to act in good faith. That is expressly set out in REACH, *Huawei v ZTE* framework for SEPs, and implied in Horizon 2020, which refers to fair and reasonable access being granted "subject to agreement". In the event of intractable disagreement, various forms of dispute resolution are available including the involvement or regulatory agencies, arbitration and mediation, but always preserving access to courts in the final instance.

66 Other notable points that underpin FRAND include: fostering access (the EECC focuses on the broad availability and variety of programming and services or Horizon 2020 access to research results); promoting key elements found in all FRAND frameworks (efficiency, competition, investment, innovation, consumer welfare); and favouring bilateral, market-based contractual negotiations over government intervention, within the parameters set out in the legislation.

67 Therefore, the review of FRAND access remedies in EU legislation shows that the public interest can underpin access regimes providing an *ex ante* framework which competition and regulatory policy can support, given the limitations of competition law in *ex post* market correction. While there are calls for *ex ante* common carrier or public utility regulation,[108] it is clear that well-articulated public interest criteria can be the basis of a FRAND regime, which will take a balanced, proportionate and pragmatic approach to the sharing of critical or important resources without the need for treating at least dominant platforms' activities as essential facilities or public utilities.[109]

G. The relevance of a FRAND access regime to dominant digital platforms

68 Having discussed the usability of FRAND access regimes in EU legislation and competition cases, the next issue to be assessed is its relevance for dominant digital platforms. A FRAND access regime can be useful in resolving issues both in relation to access to essential data and access to platforms. As seen, the application of competition law to ensure access to data considered essential for conducting business held by dominant platforms, may not be adequate to ensure full and timely access. Providing access to critical data on FRAND terms could be a way of fostering competition, but also protecting the interests and incentives to innovate digital platforms. Moreover, FRAND access can also be relevant in cases when dominant digital platforms refuse to provide access to its platform to rivals.

69 Calculating what precisely FRAND terms are may not be straight forward, and assessing "fair and reasonable" in the abstract remains complex.[110] There are numerous economic theories proposed for assessing the value for accessing technology, some of which purport to be FRAND-specific.[111] Not only do sectors and inputs differ (including, importantly, the legal regime governing them) but parties will have subjective notions of value, which is influenced by their different needs and incentives. This was recognised in the Horizon 2020 Regulation's

108 Khan (2017), page 797 et seq. See footnote 5.

109 "There is also a case for considering new ex ante regulatory tools to enhance the competitive process in digital platform markets: standards and interoperability, data portability, consumer transparency, and algorithmic pricing. In each of these, the challenge is translating well-established principles of competition analysis, law, and enforcement practice into the new domain of digital platforms". Coyle (2018), p. 17. See footnote 8.

110 Concerns about FRAND are often coloured by the very public disagreements over FRAND royalty rates for essential patents. See for example Denis Carlton, Allan Shampine, 'An Economic Interpretation of FRAND' (2013) 9 *Journal of Competition Law & Economics* 531(arguing for the use of *ex ante* incremental value of the patent before it was included in a standard); and Gregory Sidak, 'The Meaning of FRAND, Part I: Royalties' (2013) 9 *Journal of Competition Law & Economics* 931 (criticising the use of *ex ante* incremental value approach and suggesting the use of comparable licenses as a best indicator of a patent's market value). However, there are key distinctions between the regulation of FRAND regimes for digital platforms and the private ordering system under FRAND-based standardisation. First, the key input in standardisation (the technological specifications making up the standard and the patents that protect these essential technologies) are publicly available, so that it is therefore possible, and indeed usual practice, for the technology to be implemented before licensing terms are agreed. This can lead to gaming of the system with the SEP holder playing "catch up". However, in the context of regulated access, agreement on terms should occur before access is granted.

111 See Norman Neyrinck, *The Value of Intangibles – Remedies for Abuse of Refusal to License*, Working Paper. P. 45. Available at <http://www.emulation-innovation.be/wp-content/uploads/2013/09/Remedies-for-Abuse-of-Refusal-to-License-Norman-Neyrinck-22-11-2010.pdf>.

definition of "fair and reasonable conditions", accepting that conditions could change depending on the position of the parties; i.e. the circumstances of the access request, the nature of value of the input, or other characteristics. Having said that, metrics do have an important role to play in terms of transparency purposes, when the parties are not able to reach a compromise or where terms need to be determined by a third party. Such a third party, whether a regulator, court, arbitrator or mediator, will need to be informed by valuation principles and modelling.[112]

70 Assessing FRAND terms begins with an understanding of the nature of the input and relevant ecosystem. Some of the FRAND-based regulations are distinguished by the multiplicity of players involved in granting access to essential input that they control. One such example is REACH where we see common base formulae across product markets, applying per-tonnage fixed-fee price bands per substance.[113] Clearly each sector will have different considerations attached to them. FRAND metrics discussed for access to e.g. public data, publicly funded project results, standard essential technologies or access to API, are not interchangeable.

71 However, this paper shows that there are general principles that narrow down the discussion and concentrate the mind. Value considerations for access to dominant digital platform inputs are not impossible to explore. Looking at FRAND licensing commitments made by dominant platforms in merger cases, provides a useful insight into different means to assess FRAND.

72 For example, in *Worldline/Equens*, the remedies actually set out that the pricing of Poseidon licensing terms, which are structured around three main aspects, i.e. reference modules for which a price list is provided to NSPs to serve as a basis for bilateral negotiations; software maintenance fees, reference to a percentage of the license fee paid by NSPs (adjusted annually); and fees for ad hoc support services, set by reference to an hourly rate (adjusted annually). We therefore see that FRAND principles focus on providing transparent pricing, which can be the focus of negotiations and, where needed, adjudicated. The role of the Licensing Trustee is therefore a significant element, as is their need to have access to all of Worldline licenses in order to adjudicate on disputes. Nor does FRAND necessarily relate to the "price" of one input, but rather to all elements that are needed to ensure effective access, including maintenance, additional modules and upgrades. For this reason, the *Worldline/Equens* remedies also included various flanking commitments.[114]

73 In *Newscorp/Telepiù*, FRAND pricing for access to the API is to be determined by the lowest of the prices obtained when applying the two following principles: "(i) cost-oriented basis adopting where appropriate a long-run incremental costs approach and including a fair and reasonable contribution to the investment costs of set-top box roll-out and related infrastructure plus a reasonable return and (ii) relevant market values (where they exist) for comparable services."[115] It is notable that the Commission was willing to rely on two calculation methods: one economic model that factors both investment costs for implementation and return to the API holder; and one focusing on existing market comparables. However, rather than averaging out the rate, the policy choice was made to accept the lowest of the two.

74 One of the metrics that tends to have uniform acceptance and is reflected in both the *Worldline/Equens* and *Newscorp/Telepiù* remedies, is the use of comparable agreements or a track record of agreements. In the context of dominant digital platforms providing FRAND access, a question arises where there are no agreements that can act as precedent. The various FRAND metrics that can be considered cannot be divorced from the central question: "what can both parties live with?"[116]

75 Finally, it is also clear that FRAND cannot merely mean "cheap"; such an approach would disincentivise investment in developing innovative technology solutions and, perversely, condemn the most successful technologies to be less valuable. The FRAND regime reflects the balance between the importance of ensuring easy access to an input, while ensuring that the holder of the input is fairly remunerated. This means agreeing to a value that does not inhibit access but that also recognises, in addition to the value of technology, R&D costs,

112 What is clear is who chooses the metrics to use in order to determine the access terms, is as important as the metrics themselves. This narrows choices down in determining the terms themselves (usually the parties). But the oversight mechanism - who monitors the agreements and who adjudicates disputes (and their powers) - is equally critical in ensuring parties do not game the system.

113 See for example the European Chemical Industry Council (CEFIC) guidance for its Substance Information Exchange Forum at <https://cefic.org/app/uploads/2019/01/Fair-and-transparent-cost-sharing-in-SIEFs_REACHImpl_Legal.pdf>.

114 See footnote 26.

115 See footnote 24. Part II, para 11.6.

116 But it is also true that, depending on the circumstances and nature of the parties, the financial terms may be only one consideration. A FRAND regime includes within its notion of fairness and reasonableness royalty-free and other non-monetary considerations provided by the user for access, as well as important terms and conditions, which must be both fair, reasonable and non-discriminatory for access to the input.

risks taken, cost of capital etc. in order to incentivise future R&D projects.[117] Therefore the choice of the appropriate pricing methodology becomes a policy choice, as where to strike the right balance between fostering upstream or downstream innovation.[118]

H. Conclusion: A FRAND policy for Dominant Digital Platforms?

76 This paper has shown that there are numerous examples of the FRAND regime being used in European law, regulation and policy to ensure that critical inputs become or remain accessible to third parties. In fact, European regulation relating to access to critical inputs often appears to coalesce around FRAND access principles. A FRAND access regime would therefore have many benefits in addressing issues raised in markets where companies may play a gatekeeper function, such as digital platforms. Indeed, the FRAND regime has already guaranteed interoperability with broader ecosystems and third-party applications, as well as fair access to critical online platforms. At the same time, it allows fair compensation for the sharing of technology, thereby encouraging further investment in future innovation and competition in other markets. It can also be used to maintain APIs for third party access and can ensure access to data which is of great importance to a competitive and dynamic digitalisation of the European economy.

77 When elaborating policies related to digital platforms and/or data, the European Commission could seek inspiration from these sources. The FRAND regime is inherently flexible and indeed business-model neutral as it creates a level playing field between players on recognised commercial terms. Although the form that an access remedy should take depends on the nature of the input - both its physical nature (in this case non-tangible) and its legal nature - the FRAND regime side-steps many regulatory difficulties by creating an overarching model.[119] While public policy may set out various parameters for the sector input in question, terms and conditions of access, in their broadest sense, are left to bilateral market-based negotiations between participants in their particular market context with a dispute resolution or judicial backstop. In other words, FRAND enables the maintenance of competitive conditions, according to existing industry norms and practices, minimising disruptions and ensuring that regulatory solutions are as seamless and as limited as possible.

78 The implementation of a FRAND access regime may be voluntarily adopted *ex ante* by emerging digital platforms, before network effects become entrenched. Having in place access regimes to enable new entrants to compete on or for the market would be a preventative measure forestalling competition scrutiny. Competition law guidance would be beneficial in providing some legal certainty on the scope of such a remedy in competition law, for example creating a safe harbour where platforms undertake to provide access of FRAND terms and based on the European Commission's practice. This can be supplemented by *ad hoc* competition law enforcement to ensure access where competitive harm might otherwise occur. Moreover, while competition enforcement may not be able to resolve all of the issues raised by dominant digital platforms, competition policy can play an important supporting function in enforcement, policy and advocacy.

79 Alternatively, such access can be mandated by future legislation. Subjecting the platform to FRAND access provisions prevents the need to engage in regulated access *ex post*, as FRAND terms are market based. From an industrial policy perspective, however, the public interest tests elaborated in existing FRAND-based legislation are instructive in moving undertakings to adopt FRAND-based access. Therefore, while regulators deliberate *dominant* digital platforms, FRAND regimes can be considered as an effective access framework beyond the classic notions of market power.

80 This brief review of European regulation and policy should provide comfort and inspiration that a FRAND-based approach can ensure fair access to relevant platforms and services, in order to enable effective competition and fulfil European public interests. Regulation and competition policy will need to work hand in hand in identifying coherent regulatory approaches. Competition policy can assist European policy makers to engage in a more coherent manner by providing guidance for dominant digital platforms to adopt voluntary FRAND commitments and be consistent in the use of FRAND-based remedies, where appropriate.

117 See e.g. European Commission, *Setting out the EU approach to Standard Essential Patent* (Communication), COM(2017) 712 final, 29 November 2017.

118 See Neyrinck (2010), footnote 112.

119 See Jacopo Ciani, *Governing Data Trade in Intelligent Environments: A Taxonomy of Possible Regulatory Regimes Between Property and Access Rights, Intelligent Environments 2018* 285 in *I. Chatzigiannakis et al. (Eds.).*

Upload-Filters

Bypassing Classical Concepts of Censorship?

by **Amélie Pia Heldt***

Abstract: Protecting human rights in the context of automated decision-making might not be limited to the relationship between intermediaries and their users. In fact, in order to adequately address human rights issues vis-à-vis social media platforms, we need to include the state as an actor too. In the German and European human rights frameworks, fundamental rights are in principle only applicable vertically, that is, between the state and the citizen. Where does that leave the right of freedom of expression when user-generated content is deleted by intermediaries on the basis of an agreement with a public authority? We must address this question in light of the use of artificial intelligence to moderate online speech and its (until now lacking) regulatory framework. When states create incentives for private actors to delete user-content pro-actively, is it still accurate to solely examine the relationship between platforms and users? Are we facing an expansion of collateral censorship? Is the usage of soft law instruments, such as codes of conduct, enhancing the protection of third parties or is it rather an opaque instrument that tends to be conflated with policy laundering? This paper aims to analyse the different layers of the usage of artificial intelligence by platforms, when it is triggered by a non-regulatory mode of governance. In light of the ongoing struggle in content moderation to balance between freedom of speech and other legal interests, it is necessary to analyse whether or not intelligent technologies could meet the requirements of freedom of speech and information to a sufficient degree.

Keywords: Freedom of expression; censorship; democratic legitimation; upload-filters; prior restraint

Recommended citation: Amélie Pia Heldt, Upload-Filters: Bypassing Classical Concepts of Censorship?, 10 (2019) JIPITEC 56 para 1.

A. Introduction

1 Considering that user-generated content constitutes both speech in constitutional terminology as well as the basis for many social media platforms'[1] business models, its regulation poses many challenges. Social media platforms, or to put it more generally, *intermediaries*, rely on user-generated-content to attract other users. To sustain their attention and, by extension, revenue from advertisers, social networks are dependent on the activity of users on the one hand and on a clean, confidence-inspiring environment on the other. Examples such as the decline of MySpace[2] or the almost non-existent moderation policy at

* Amélie P. Heldt is a junior researcher and doctoral candidate with the Leibniz Institute for Media Research/Hans-Bredow-Institute, Hamburg, and currently a visiting fellow with the Information Society Project at Yale Law School.

1 In this article, "intermediaries" is used as a generic term for "social media services, platforms and networks". They will be used as synonyms for Internet-based applications that rely on user-generated-content to create online communities to share information, ideas, personal messages, etc. Definition retrieved from <https://www.merriam-webster.com/dictionary/social%20media> accessed 23 January 2019.

2 Stuart Dredge, 'MySpace – what went wrong: "The site was a massive spaghetti-ball mess"' (2015) <https://www.theguardian.com/technology/2015/mar/06/myspace-what-went-wrong-sean-percival-spotify> accessed 10 December 2018.

4chan have led to the assumption that a minimum level of content moderation is inevitable. Because of the immense amount of uploaded content that they have to negotiate, social networks fall back on technology to detect and, at times, remove illegal or undesirable content.

2 Deleting a post is, first of all, subject to the intermediaries' community guidelines, but content deletion can also be interpreted as (collateral) censorship if its legal basis is a law or even an agreement (such as a code of conduct) between intermediaries and legislators. Examining automated content deletion via upload-filters raises questions about the technology used, as well as the normative framework of intermediaries when they act on grounds of so-called "soft law". First, this paper will provide an overview of the protection of speech under German Basic Law and the European Convention on Human Rights (ECHR). Second, the increasing use of upload-filters in content moderation – especially to counter terrorist propaganda via user-generated content – will serve as a use case. This type of automated speech regulation could potentially be classified as censorship under certain conditions, an examination of which will constitute the third section of this paper.

B. Protection of freedom of speech and the notion of censorship

3 Social media platforms aim at connecting people globally, inevitably linking various jurisdictions through their contractual relationship with users. Freedom of expression and the notion of censorship are relevant in this context because users might feel violated in their freedom of expression when the content they have uploaded is deleted or blocked. In order to assess whether the use of filters for content moderation purposes is in accordance with our human rights framework, we need to first examine the scope of protection.

I. Under art. 5 German Basic Law

1. Broad protection of free speech

4 In Germany, freedom of speech is protected by art. 5 (1) Basic Law; this clause provides a relatively broad scope of protection. It protects freedom of expression and information as well as important ancillary rights to access means of expression and information, including the whole communicative process and all types of speech, regardless of its topic and its commercial worth.[3] Freedom of speech protects factual claims and value judgments and is considered fundamental to German democratic understanding.[4] This protection under art. 5 (1) Basic Law is, however, not boundless; there are limits to speech through general laws, youth protection, and the honour of third parties (art. 5 (2) Basic Law). Limiting fundamental rights by law is not an essential characteristic of freedom of speech: in German constitutionalism, only very few fundamental rights are guaranteed unconditionally, most can be restricted by law if the restriction is proportionate.

5 The restrictions allowed by constitutional proviso in art. 5 (2) Basic Law are themselves bound to certain requirements: in order to prevent state influence on speech targeting laws, the German Federal Constitutional Court (FCC/BVerfG) elaborated the principle of interdependency (so-called "Wechselwirkungslehre"); this means that not only should the laws restricting speech be in accordance with the scope of protection, but their case-related use needs to be reasonable and adequate when it comes to freedom of speech.[5] This doctrine is, on the one hand, a guarantee for a moderate application of speech-restricting laws and, on the other, it adds a certain complexity when balancing freedom of speech with other rights.

2. Limits to free speech

6 According to the FCC, any law restricting speech needs to serve a higher constitutional purpose than the freedom of expression. It also has to be proportionate and neutral as to the content of the opinion expressed.[6] For obvious reasons, laws according to art. 5 (2) Basic Law shall be as general as possible as to avoid any connection between the purpose of the law and opinions expressed. This means that statements may be punishable by law, but only in order to protect other rights and not to forbid certain opinions.[7] The law may never forbid an opinion due to a concrete political, religious, or ideological position. With this strict criterion, art. 5 Basic Law can guarantee that freedom of expression is only restricted by an opinion-neutral regulation.

7 For example, publicly calling for an unlawful action is penalised just as it would be if it was an incitement under section 111 German criminal code (StGB); i.e. it

3 Jurisprudence of German Federal Constitutional Court: BVerfGE 90, 241, 247.

4 BVerfGE 85, 1, 15; BVerfGE 5, 85, 205.

5 BVerfGE 7, 198, 208 f.

6 BVerfGE 124, 300.

7 BVerfGE 124, 300, 322.

bears the same legal consequence as committing the unlawful action itself. Calling for unlawful action can be considered as expressing an opinion, which makes sec. 111 StGB a speech-restricting law when the speaker is addressing an audience and calling upon them to commit violence. To fulfil the "publicity" criterion the speaker needs to be targeting an indeterminate number of potential recipients, not an individual or specific audience member (in contrast to an individual address such as a private message).[8]

8 At first glance, the use case of this paper – automated filtering and removal of online terrorist propaganda – does not violate the protection of fundamental rights. Uploading a video with a specific message which incites violence is highly likely to meet the requirements of criminal offences. Posting a video on a social network that calls for violence, a "holy war", or for the support of specific terrorist actions is covered by sec. 111 StGB because the internet and social networks in particular may be considered as "public space[s]".[9] To summarise, one cannot be punished for defending a religious belief by expressing his or her opinion but, rather, for calling on others to harm "all non-believers". Restricting this type of speech is therefore in line with the scope of protection outlined in art. 5 (1) Basic Law, unless its enforcement violates the ban on censorship.

3. Uncompromising ban on censorship

9 In German constitutional methodology, restrictions of art. 5 (1) Basic Law have to comply with the so-called restrictions of restrictions ("Schrankenschranke"), amongst others the ban on censorship which is enshrined in art. 5 (1) 3 Basic Law and cannot be subject to adaptations. According to the prevailing opinion in German constitutional jurisprudence and scholarship, censorship can only be the consequence of the obligation to submit a medium to a state agency for *prior* approval of the publication *before* it is produced or distributed.[10] The addressees of this rule are restricted to government agencies, that is, only state-driven actions are forbidden by art. 5 (1) 3 Basic Law and, in principle, the actions of private individuals or entities are not affected under its purview.[11] It shall be referred to as pre-censorship, in contrast to reviewing and possibly deleting content *after* publication or distribution. The majority of scholars are reluctant to extend the ban on this type of pre-censorship to non-state-driven actions.[12]

10 However, this formal and quite conservative interpretation might be subject to changes in the context of online intermediaries.[13] In view of increasing cooperation between tech companies and public authorities,[14] some have argued against this narrow interpretation of censorship that leaves no space for the examination of pre-censorship by private entities.[15] According to Justice Hoffmann-Riem (former judge at the FCC), controlling content on the internet (e.g. by filtering) is only covered by contractual freedom to the extent that it affects persons who have contractual relationships with the respective provider and have thereby consented to control and filtering. Furthermore, the state's duty to protect could require precautions which make it possible to use the infrastructures that are important for the general provision of communications without a framework that is similar to censorship.[16] Löffler, too, believes that the free development of intellectual life can only be guaranteed if the prohibition of censorship also addresses non-state institutions and private instances that have a significant influence on intellectual life.[17] When looking at the power private entities have over our digital communications' infrastructure, holding on to the classical definition of strictly state-driven censorship appears questionable.

II. Freedom of speech in the ECtHR jurisprudence

1. Protection under art. 10 ECHR

11 The jurisprudence of the European Court of Human Rights (ECtHR) on matters of freedom of speech and its protection under art. 10 ECHR has a rich tradition. Between 1959 and 2012 the court

8 Federal Court of Justice: BGH, NStZ 1998, 403, 404.

9 Karl-Heinz Ladeur, ´Ausschluss von Teilnehmern an Diskussionsforen im Internet – Absicherung von Kommunikationsfreiheit durch "netzwerkgerechtes" Privatrecht´ [2001], MMR, 787, 791.

10 BVerfGE 33, 52, 71; BVerfGE 47, 198, 236.

11 Herbert Bethge, Art. 5 Basic Law, *Grundgesetz-Kommentar*, (2014), para 135.

12 Bethge (n 11), para 133; Ansgar Koreng, *Zensur im Internet*, (2010), 235.

13 Christoph Grabenwarter, Art. 5 Grundgesetz, in Maunz/Dürig (eds.) *Grundgesetz-Kommentar* (2018), para. 119.

14 Michael Birnhack, Niva Elkin-Koren, 'The Invisible Handshake: The Re-emergence of the State in the Digital Environment' (2003), 1, Virginia Journal of Law & Technology, 49-52.

15 There is also an ongoing discussion about whether platforms should be bound to the human rights framework through a horizontal binding effect. This is however not the core issue of this paper because it rather focusses on the state acting *through* the platforms in a non-transparent manner, instead of platforms *acting as* public actors.

16 Wolfgang Hoffmann-Riem, Art. 5 Grundgesetz, *Alternativkommentar-Grundgesetz* (2001), para 95.

17 Martin Löffler, ´Das Zensurverbot der Verfassung´ (1969), 50, NJW, 2225, 2227.

asserted 512 infringements of art. 10 (1) ECHR[18] and has shaped a solid case law in balancing freedom of speech and personality rights, which deserves special mention. That being said, the jurisprudence of the ECtHR exists in harmony with the German constitutional understanding of freedom of speech mentioned above: expressions of opinion are protected as long as they do not incite violence. The scope of protection of art. 10 (1) ECHR is similarly broad: it protects the freedom of opinion and of expression and takes into account all opinion and expression of opinion regardless of subject matter, intellectual veracity, or social utility, including trivial, entertaining, commercial, absurd, as well as aggressive and offensive statements.[19] In other words, speech cannot be restricted in accordance with art. 10 (1) ECHR as long as it does not endorse the use of violent procedures or bloody revenge, nor justify the instruction of terrorist acts or potentially incite to violence due to profound and irrational hate towards certain people.[20]

2. No absolute ban on censorship

12 One difference between art. 5 Basic Law and art. 10 ECHR lies in the more restrictive interpretation of the ban on censorship. According to art. 10 ECHR, interventions that constitute censorship are not inadmissible per se. Rather, they must satisfy the principle of proportionality whereby the particular severity must in any case be taken into account.[21] The prohibition of censorship is to be derived – although not explicitly mentioned – from the prohibition of intervention by the authorities in accordance with art. 10 (1) 2 ECHR.[22] Accordingly, it is not surprising that interventions are only permissible within narrow limits and that the ECtHR carries out a detailed review of corresponding measures.[23] So-called "prior restraints"[24] are only permissible if they do not result in a complete prohibition of publication, if the information is less than current, if rapid court proceedings on prohibition orders are possible, and if complex issues of fact and law are clarified in the process.[25] The court has established in numerous cases that prior restraint is not prohibited *per se*,[26] which is the crucial difference when comparing it to art. 5 (1) 3 Basic Law. Nonetheless, the general protection and interpretation of freedom of speech by the FCC and the ECtHR is largely similar, especially when it comes to state-driven restrictions of fundamental rights, be it freedom of expression or media freedom.

C. The rise of upload-filters in content moderation

13 As mentioned above, the vast amount of data constantly uploaded onto social media platforms makes it almost impossible to manage without the help of technological solutions. Algorithms sort, filter, and prioritise content in order to present what is most relevant for each specific user. In this context, different types of filtering and sorting solutions have been developed. Results may be displayed according to a user's behaviour, his or her location, or his or her self-selected preferences, or simply not displayed because of possible infringements on rights or guidelines. When it comes to technological progress, questions regarding the compliance with freedom of speech proviso arise as artificial intelligence takes over the tasks of content reviewers. Practitioners must be aware of the risks and the opportunities that this development towards a machine-only moderation entails. Taking a closer look at upload-filters will reveal that they are not yet capable of moderating content according to our human rights framework,[27] but could nonetheless be deployed accordingly with further technological improvements.[28]

18 Matthias Cornils, Europäische Menschenrechtskonvention, Art. 10, *BeckOK Informations- und Medienrecht* (2016), para 3.

19 ECtHR, Cholakov v. Bulgaria, 20147/06, para 28.

20 ECtHR, Sik v. Turkey, 53413/11, para 105.

21 Matthias Cornils, Europäische Menschenrechtskonvention, Art. 10, *BeckOK Informations- und Medienrecht* (2016), para 67.

22 Gilert-Hanno Gornig, Äußerungsfreiheit und Informationsfreiheit als Menschenrechte,(1988), 317.

23 ECtHR, Ekin v. FRA, 39288/98, para 58.

24 The ECtHR uses "prior restraints" as a synonym for pre-censorship without fully endorsing the definition in the constitutional jurisprudence of the US Supreme Court, but rather as a "general principle to be applied in this field", see ECtHR, Observer and Guardian v. The United Kingdom, 13585/88, ftn. 6.

25 Christoph Grabenwarter, Katharina Pabel, *Politische und gemeinschaftsbezogene Grundrechte. Europäische Menschenrechtskonvention*, (2016), para 39.

26 ECtHR: Observer/Guardian v. The United Kingdom, 13585/88; Markt Intern Verlag/Beermann v. Germany, 10572/83; Yildirim v. Turkey, 3111/10.

27 Filippo Raso and others., *Artificial Intelligence & Human Rights: Opportunities & Risks* (2018), Berkman-Klein Center for Internet & Society; Viktor Volkmann, 'Hate Speech durch Social Bots' [2018], MMR, 53; Ansgar Koreng, 'Filtersysteme werden nicht lange auf Urheberrechte beschränkt bleiben' [2016], iRights <irights.info /artikel/eu-urheberrecht-content-id-filter/28046> accessed 20 January 2019.

28 Martin Husovec, 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown? Which is Superior? And Why?' (2018), 42 Colum. Journal of Law & the Arts, 53, 84.

I. Upload-filters: sorting content before publication

14 In the context of intermediaries, one of the main functions of algorithms is to sort content in a user-oriented way and present it differently depending on a user's profile. When it comes to combating criminal content online in conjunction with algorithmic decisions, the focus is on intelligent filters, such as upload-filters. Upload-filters constitute a subcategory of content-control software.[29] Their function is to recognise certain content, hash[30] it and then - if required - automatically delete it. This means that the entirety of the content uploaded to a platform by its users (user-generated content) is routed through the service provider's cache.[31] Until now, this approach followed a two-step procedure referred to as *notice and take down* (NTD) or *notice and stay down* (NSD), whereas upload-filters act before publication, i.e. while the uploaded content is not yet visible to other users. If a violation is discovered by the filter, the content will not be published at all. Hence, the decision-making process bypasses any human intervention; here, only the filter is doing the work of moderation. The remaining "human in the loop" is the initial programmer of the filter, so, in theory, no additional content moderators will review the content (in contrast to NTD processes that make use of human moderators).

15 One area of application for upload-filters is to search for unlawful content; however, the criterion of illegality is not inherent to the definition of upload-filters because the question of how and what is filtered depends on the initial programming. Beyond that, the system can be self-learning to the extent that, despite small changes to the original content, it still recognizes certain content as a rights or legal violation.[32] Bypassing the mechanism becomes increasingly difficult if the core content is the same. By marking the content as illegal, the filter, through machine learning processes, is trained to recognise it as such and continue to do so further along the process. Upload-filters have been a recurring topic in the discussion on upcoming EU regulation. The two main areas of use are against copyright infringements and terrorist propaganda, which will be examined in the following subsection. Regarding copyright infringements, private companies have already been using filters for a long time. Thanks to its Content-ID-technology,[33] YouTube has been able to identify copyright infringements at a very early stage. The filter was operational as soon as copyright holders had registered their intellectual property (with hashes). YouTube claims that, as of 2016, 99.5% of music claims on YouTube were matched automatically by Content-ID.[34]

II. Use against terrorist propaganda

16 Upload-filters' other area of use is to restrict terrorist propaganda online. Given the increasing risk that social networks and video platforms pose with regards to potential radicalising effects,[35] the EU Commission has proposed a more effective take-down policy for content glorifying violence, especially terrorist propaganda. In 2015, the EU Commission founded the EU Internet Forum which brought together interior ministers of the EU member states, high-ranking representatives of leading companies in the internet industry, Europol, the European Parliament, and the EU Counter-Terrorism Coordinator. The aim was to develop a common approach based on a public-private partnership to detect and combat harmful online content.[36] Against this background, the EU Commission presented its "Code of Conduct on illegal online hate speech"[37] in May 2016 (EU Commission, press release IP/16/1937).[38] The IT companies involved - Facebook, Twitter, YouTube, and Microsoft - committed to take action against illegal hate speech on the internet. Legally speaking, a code of conduct is a so-called "soft law instrument", that is, an agreement on the basis of which companies are bound to the terms, but it has no legislative activity as its basis.[39] The Code of Conduct on illegal online hate speech contains concrete obligations for IT companies, such as verifying the majority of valid reports relating to the

29 <https://en.wikipedia.org/wiki/Content-control_software> accessed 10 December 2018.

30 <https://techterms.com/definition/hash> accessed 10 December 2018.

31 <https://techterms.com/definition/cache> accessed 10 December 2018.

32 Henrike Maier, *Remixe auf Hosting-Plattformen: Eine urheberrechtliche Untersuchung filmischer Remixe zwischen grundrechtsrelevanten Schranken und Inhaltefiltern* (2018), 150.

33 <https://support.google.com/youtube/answer/2797370?hl=en> accessed 10 December 2018.

34 Lyor Cohen, 'Five observations from my time at YouTube' (2017) Official Blog <https://youtube.googleblog.com/2017/08/five-observations-from-my-time-at.html> accessed 10 December 2018.

35 Zeynep Tufekci,'YouTube, the Great Radicalizer', The New York Times, (2018), <https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html?smid=tw-share&referer=https://t.co/aXAthxinwn%3famp=1> accessed 10 December 2018.

36 EU Commission, press release IP/15/6243.

37 'Code of Conduct on Countering Illegal Hate Speech Online' <https://ec.europa.eu/info/files/code-conduct-countering-illegal-hate-speech-online_en> accessed 10 December 2018.

38 <http://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 10 December 2018.

39 Michelle Cini, 'The soft law approach: Commission rule-making in the EU's state aid regime', [2001], Journal of European Public Policy, 192, 194.

removal of illegal hate speech in less than 24 hours and removing or blocking access to such content. The first results[40] of the Code's implementation were evaluated in late 2016.

17 In March 2017, the EU Commission introduced the "Database of Hashes", a common database and network developed in collaboration with the four major IT companies who had already agreed to the Code of Conduct. The legal instruments and the technology used for this Database are an exemplary use case for this paper's main argument (which shall be fully elaborated in section D. below). The Database, which is accessible to all participating companies and the intergovernmental authorities mentioned above, collects so-called "hashes" (digital fingerprints) of content that has been marked as "terrorist" or "extremist" by the means of filters. Its purpose is to combat online terrorist propaganda more effectively, that is without the necessity of a human reviewer. But, in so doing this filtering system raises important questions for the exercise of freedom of expression and information.[41] This is mainly due to the "successful" implementation of filtering technology as described above. A few months after the introduction of the Database, representatives of the four IT companies reported that most unwanted content is now deleted before it even goes online. This content includes many videos that are uploaded for the first time and until then not filed with the relevant companies or police authorities and accompanied by a request for deletion.[42] This shows that the Database was fully operational as of late 2017 and contained more than 40,000 hashes for terrorist videos and images.[43] Currently, thirteen companies are associated with the Database which comprised approximately 100.000 hashes by late 2018.[44]

18 YouTube has already been mentioned as an example of a platform that uses filter technologies to prevent copyright infringements. It is also one of the major contributors to the Database of Hashes. This observation is consistent with the assumption that YouTube's recommendation system might lead further down the "rabbit hole of extremism" from video to video,[45] coming to the fore of those working on terrorist propaganda prevention. In an official statement, YouTube explained the use of intelligent filters to combat terrorist propaganda.[46] According to this report, YouTube has removed 7.8 million videos because of their "violative content" from July to September 2018. Through machine learning, it is capable of deleting five times more videos than before. 98% of the videos deleted in 2017 that were related to "violent extremism" were marked by machine-learning algorithms.[47] In this context, YouTube estimates that the human workforce "replaced" by the use of intelligent filters has been 180,000 full-time employees since June 2017. The company also announced its expansion of intelligent filter use to include youth protection and hate speech.

D. Frictions with the notion of censorship

19 The issue with 1) the obligation to use upload-filters to comply with the Code of Conduct, 2) the introduction of the Database, and 3) the collection of data through private companies in a Database accessible to public authorities, is that the distinction between state-driven action and contractual relationships becomes increasingly blurred. When bringing together the human rights framework on freedom of speech including the ban on censorship on the one hand, and the use of upload-filters by private entities such as social media platforms on the other, the question is: is it sufficient to limit our definition of censorship to state-driven action?[48] When public authorities push social media platforms to use upload-filters through "soft law", the effects for the end-user of the platform are identical to when they oblige them to do so by law,[49] because pre-censorship is brought into effect, regardless of the quality of the normative framework used. This phenomenon, referred to as an "invisible handshake", is a contentious one as

40 EU Commission, Code of Conduct on countering illegal hate speech online: First results on implementation, <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/news/docs/first_evaluation_of_the_code_of_conduct_en.pdf>, accessed 15 January 2019.

41 Maryant Fernández Pérez, 'Parliamentarians Encourage Online Platforms to Censor Legal Content', (2017), <https://edri.org/parliamentarians-encourage-online-platforms-to-censor-legal-content/> accessed 15 January 2019.

42 Matthias Monroy,'EU-Internetforum": Viele Inhalte zu „Extremismus"' werden mit Künstlicher Intelligenz aufgespürt', (2017), <https://netzpolitik.org/2017/eu-internetforum-viele-inhalte-zu-extremismus-werden-mit-kuenstlicher-intelligenz-aufgespuert/> accessed 10 December 2018.

43 EU-Commission, press release IP/17/5105, <http://europa.eu/rapid/press-release_IP-17-5105_en.htm> accessed 15 January 2019.

44 EU Commission, Statement/18/6681, <http://europa.eu/rapid/press-release_STATEMENT-18-6681_en.htm> accessed 15 January 2019.

45 Tufekci (n 35).

46 Youtube, Official Blog (2018), <https://youtube.googleblog.com/2018/12/faster-removals-and-tackling-comments.html> accessed 15 January 2019.

47 Youtube, Official Blog (2017), <https://youtube.googleblog.com/2017/12/expanding-our-work-against-abuse-of-our.html> accessed 15 January 2019.

48 Jack M. Balkin, 'Old-school/new-school speech regulation' (2013), 127, Harv. L. Rev., 2296.

49 Fernández Pérez (n 41).

it places citizens in an unusual position between private and public law.[50] The difference worth pointing out is that actions taken by virtue of a soft law instrument cannot be appealed in the same way as actions taken by virtue of an administrative act. If decisions related to speech on social media platforms are attributed to community guidelines and not to an act of public authority, the defence capabilities of citizens under that regime will be restricted.

I. Bad filters, good intentions?

20 The analysis above has shown that upload-filters intervene exactly at the point prohibited by the ban on pre-censorship, which is why they are so heavily criticised. But is artificial intelligence really the problem? Should we not summarise the protection afforded by upload-filters as follows: the protection of copyright holders via *Content-ID*, the protection of children via *PhotoDNA*, and the protection of public security from terrorist propaganda via the *Database of Hashes*? Filtering user-generated-content may serve a legitimate purpose (which is why this paper does not aim to question their purposes). Nevertheless, this should not come at the price of unconstitutionality. The intentions behind the use of certain technologies can rarely justify disproportionate rights infringements. This is even more relevant if machine learning is being utilised, as AI amplifies the possibility of losing control over the relevant mechanisms. Today already, the risk of both chilling effects on freedom of expression and collateral censorship is very real when using content-filtering algorithms. In particular, the proportionality of the use of upload-filters is highly doubtful since they operate in a manner that includes a mass and suspicion-independent examination of contents. This is why the use of upload-filters requires more scrutiny when it comes to possible violations of freedom of expression and information.

21 In the case of the German Network Enforcement Act (NetzDG), published reports demonstrated that technology is not yet capable of identifying criminal behaviour in the field of hate speech such as libel and defamation (reports from Facebook, Twitter, Google, YouTube and Change.org available at the German Federal Gazette).[51] Upload-filters still lack the ability to understand content in context or to identify satire in videos,[52] which means that content is often filtered and deleted before being published or made visible to other users even though it might not violate any laws or third-party rights (i.e. legal content). The intermediate conclusion to this section is that the EU impels private companies to use upload-filters which are, technologically speaking, not fit for purpose in meeting the requirements of our common human rights framework.

II. Censorship by whom?

22 Part of the complexity in designing regulation for this field is ingrained into its multi-stakeholder constellation. Instead of structuring a bipolar state-citizen or company-user relationship, communication in digital spaces involves state actors, intermediaries, and users/citizens.[53] We have already established that, in classical constitutional law, we understand "censorship" as the consequence of a state-driven action. However, in the context of online communication, numerous variations have emerged. Censorship *by proxy* is when public authorities control communication or censor it through any number of intermediaries.[54] *Collateral* censorship is when public authorities force intermediaries to control their users' communication.[55] This type of behaviour could be subsumed under the notion of censorship because under FCC jurisprudence, for instance, the internet is considered as a "publicly available source". Withholding information, therefore, interferes with the right to access appropriate information that is required by the general public to inform themselves.[56] Nonetheless, such an action would need to be taken by a *state* entity in order to be classified as censorship, not as content moderation.

23 In relation to the upload-filters used within the Database of Hashes to curtail terrorist propaganda, the question arises as to when might state action be considered an indirect encroachment on fundamental rights if it is implemented by private entities. This question has already been discussed for many years: is it an "unholy alliance" or a necessary cooperation between the state and private intermediaries?[57] Some scholars argue in favour of a more modern concept of state action which also includes private behaviour that can be attributed to the state on the basis of its intention - even if that behaviour is not based on a "hard law"

50 Birnhack, Elkin-Koren (n 14), 49ff.

51 <https://www.bundesanzeiger.de/ebanzwww/wexsservlet> accessed 10 December 2018.

52 YouTube, NetzDG Report 2018 <https://transparencyreport.google.com/netzdg/youtube> accessed 15 January 2019.

53 Jack M. Balkin, 'Free Speech is a Triangle' [2018] Columbia Law Review (forthcoming 2018).

54 Seth F. Kreimer, 'Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link' (2006), 155, University of Pennsylvania Law Review, 11-100.

55 Balkin (n 48).

56 BVerfGE 103, 44, 60.

57 Birnhack, Elkin-Koren (n 14).

regulatory framework.[58] If a legal implementation of an obligation to filter was to emerge out of the current regulatory propositions,[59] the preconditions for state action could be fulfilled.

III. Sound legal foundation required

24 Censorship functions must not be "outsourced" by the state in such a way that it demands censorship-like action by private actors or provides for corresponding legal obligations or the imposition of negative sanctions in the event of a violation.[60] Using intermediaries to fulfil certain functions on the internet is a collateral way of regulating (online) speech. Although the prohibition of pre-publication censorship is intended to protect freedom of speech and a free flow of information, it might be attractive to public authorities to bypass its protective purpose. Here, a rethink is called for: the vast majority of digital communication spaces are privately owned and therefore not the immediate addressees of the ban on censorship. Limiting the latter to state actors is no longer up-to-date as far as guarantees of freedom of opinion and information are concerned. When pre-censorship (according to the definition elaborated above) is directly based on the initiative of the state (in contrast to *strictly private* content moderation), legal reservations should nevertheless be observed as a barrier to a speech restricting behaviour. Basic legal guarantees such as accountability, transparency, or due process can hardly be ensured when the legal basis for 'voluntary' automated content removal is lacking.[61]

25 A soft law instrument such as a Code of Conduct may offer a certain degree of flexibility and room for manoeuvre, whereas laws take longer to come into force and cannot be adapted as quickly. In line with ECtHR case law, all forms of regulation must be defined by law, they must be in pursuit of a legitimate aim, and they must be necessary.[62] Clearly, soft law can at times serve as an adequate means of regulation but when it comes to restricting human rights, regulation by law is preferable as it fosters transparency and empowers citizens to respond.[63] In his report on the promotion and protection of the right to freedom of opinion and expression for the UN, David Kaye argues that obligations to monitor and rapidly remove user-generated content have increased globally and have established punitive frameworks that are likely to undermine freedom of expression even in democratic societies.[64] As a consequence, states and intergovernmental organisations "should refrain from establishing laws or arrangements that would require the 'proactive' monitoring or filtering of content, which is both inconsistent with the right to privacy and likely to amount to pre-publication censorship".[65] In their study for the Council of Europe, the committee of experts on internet intermediaries came to the same conclusion: "States should not impose a general obligation on internet intermediaries to use automated techniques to monitor information that they transmit, store or give access to, as such monitoring infringes on users' privacy and has a chilling effect on the freedom of expression".[66] This leaves no room for confusion and stipulates very clearly that such collateral censorship mechanisms must be avoided.

IV. Relief through a new EU regulation?

26 In September 2018, the EU Commission presented its proposal for a regulation on preventing the dissemination of terrorist content online,[67] which – in a nutshell – transfers the stipulations from

58 Andreas Voßkuhle, Anna-Bettina Kaiser, 'Der Grundrechtseingriff' [2009], Juristische Schulung, 313; Julian Staben, Markus Oermann, (2013)'Mittelbare Grundrechtsreingriffe durch Abschreckung? – Zur grundrechtlichen Bewertung polizeilicher „Online-Streifen" und „Online-Ermittlungen" in sozialen Netzwerken', Der Staat, 630, 637.

59 EU Commission, press release IP/18/5561, 'State of the Union 2018: Commission proposes new rules to get terrorist content off the web' <http://europa.eu/rapid/press-release_IP-18-5561_en.htm> accessed 15 January 2019.

60 Hoffmann-Riem (n 16), para 94; Bethge (n 11), para 135a.

61 Niva Elkin-Koren, Eldar Haber,'Governance by Proxy: Cyber Challenges to Civil Liberties' (2016), 105, Brooklyn Law Review, 161 f.

62 Council of Europe, 'Ethical Journalism and Human Rights' (2011), Issue Paper commissioned and published by Thomas Hammarberg, Council of Europe Commissioner for Human Rights, CommDH/IssuePaper (2011) 1; Andrew Sharland 'Focus on Article 10 of the ECHR' (2009), 14:1, Judicial Review, 59, 63; Linda Senden, 'Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?' (2005), 9.1, Electronic Journal of Comparative Law.

63 Tal Z. Zarsky,'Law and Online Social Networks: Mapping the Challenges and Promises of User-generated Information Flows' [2008], Fordham Intell. Prop. Media & Ent. Law Journal, 741, 780.

64 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations Human Rights Council, A/HRC/38/35, (2018), 7.

65 ibid 64.

66 Council of Europe, 'Algorithms and human rights', Study on the human rights dimensions of automated data processing techniques and possible regulatory implications, (2018), Committee of experts on internet intermediaries (MSI-NET), 46.

67 EU Commission, COM (2018) 640 final <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0640&from=EN> accessed 16 January 2019.

the Code of Conduct to a regulatory framework. The preamble of the proposal mentions that the regulation aims at increasing "the effectiveness of current measures to detect, identify and remove terrorist content online without encroaching on fundamental rights". These "new rules to get terrorist content off the web within one hour" are supposed to increase the speed and effectiveness of the ongoing "voluntary cooperation in the EU Internet Forum". Art. 6 of the proposal governs the implementation of pro-active measures by service providers, including but not limited to, "detecting, identifying and expeditiously removing or disabling access to terrorist content" in art. 6 (2) b. Here, "pro-active" is used as a synonym for automated removal and/or intelligent technologies. In accordance with art. 6 (1) the hosting service providers are required to implement this type of measure whilst taking into account the "fundamental importance of the freedom of expression and information in an open and democratic society".

27 The proposed regulation could produce relief for the issue outlined in this article. Due to the shift from an "invisible handshake" to a more visible governance by proxy[68] the problems regarding an opaque public-private-partnership could partly be solved. This proposal does, nonetheless, raise other questions regarding the respect of fundamental rights such as (amongst others) the right of "competent authorities" to "request the hosting service provider to take specific additional proactive measures" (art. 6 (3)). This adumbrates the quality of future measures and the usage of artificial intelligence for such purposes.

E. Conclusion

28 We are still unaware of the developments of artificial intelligence in the field of digital communication, and machine learning is – by definition – work in progress. In general, we should refrain from designing too many new, made-to-measure regulations in the field of AI research and implementation. Instead, we should be aware of the constitutional provisos that rule our legal system and think about expanding existing concepts such as the proportionality test. According to these requirements, no state action should be hidden – the alliance of state authority and intermediaries must be transparent and recognisable. We need to clarify the legal basis upon which upload-filters or other types of artificial intelligence are being utilised as part of digital communication processes and services. This need is even more prescient when their effects are forbidden by constitution or by constitutional jurisprudence and when the legal instruments used to regulate them do not meet the requirements of the rule of law. Creating a regulatory framework that renders the "invisible" handshake more visible is unavoidable in a democracy. The proposed regulation for the use case of terrorist propaganda could provide an adequate solution to the problem of the lack of the means of defence: where there is a clear regulatory act, citizens who feel violated in their fundamental rights can respond in a court of law. However, this claim is not only valid for freedom of speech and information issues, but for all fundamental rights that might be restricted by a law enforcement by proxy that exists by virtue of a hidden public agenda.

Acknowledgements

The author thanks Professor Wolfgang Schulz for his valuable feedback, Professor Niva Elkin-Koren for her inspiring and very helpful advice, and the participants of the Young Scholars Workshop on AI at the University of Haifa in December 2018 for their comments.

68 Elkin-Koren, Haber (n 61), 108.

Evaluating the EC Private Data Sharing Principles

Setting a Mantra for Artificial Intelligence Nirvana?

by **Begoña Gonzalez Otero***

Abstract: On April 25, 2018, the European Commission (EC) published a series of communications related to data trading and artificial intelligence. One of them called "Towards a Common European Data Space", came with a working document: "Guidance on Sharing Private Sector Data in the European Data Economy". Both the Communication and the guidance introduce two different sets of general principles addressing data sharing, contractual best practices for business-to-business (B2B), and business-to-government (B2G) environments. On the same day, the EC also published a legislative proposal to review the Public Sector (PSI) Directive. These two simultaneous actions are part of a major package of measures, which aim to facilitate the creation of a common data space in the EU and foster European artificial intelligence development. This article focuses on the first action, the "Guidance on Sharing Private Sector Data in the European Economy". First, because it is one of its kind. Second, although these principles do not qualify as soft law (lacking binding force but having legal effects) the Commission's communications set action plans for future legislation. Third, because the ultimate goal of these principles is to boost European artificial intelligence (AI) development. However, do these principles set a viable legal framework for data sharing, or is this public policy tool merely a naïve expectation? Moreover, would these principles set a successful path toward a thriving European AI advancement? In this contribution, I try to sketch some answers to these and related questions.

Keywords: Artificial intelligence; best practices; data access; data re-use; data sharing; standard contract terms; the internet of things; self-regulation

Recommended citation: Begoña Gonzalez Otero, Evaluating the EC Private Data Sharing Principles: Setting a Mantra for Artificial Intelligence Nirvana?, 10 (2019) JIPITEC 65 para 1.

A. Introduction

1 On April 25, 2018, the European Commission (EC) published a series of communications related to data trading and artificial intelligence. One of them called "Towards a Common European Data Space",[1] came with a working document: "Guidance on Sharing Private Sector Data in the European Data Economy".[2] Both the Communication and the guidance introduce two different sets of general principles addressing data sharing contractual best practices for business-to-business (B2B) and for business-to-government (B2G) environments. On the same day, the EC also published a legislative proposal to review the Public Sector (PSI) Directive.[3] These two simultaneous

* In-house Consultant at Latin America IPR SME Helpdesk; bgotero@gmail.com.

1 Commission, "Towards a Common European Data Space" (Communication) COM (2018) 232 final.

2 Commission, "Guidance on Sharing Private Sector Data in the European Data Economy" (Staff Working Document) SWD (2018) 125 final.

3 See the announcement at <https://ec.europa.eu/digital-single-market/en/proposal-revision-public-sector-information-psi-directive> (accessed on October 15, 2018).

actions are part of a major package of measures aiming to facilitate the creation of a common data space in the EU and foster European artificial intelligence technologies' development.

2 This article focuses on the first action, the "Guidance on Sharing Private Sector Data in the European Economy". First, because it is one of its kind. So far, the discussion on data sharing in Europe has been less intense than for data transfer; perhaps because the legal basis for a transfer can be a sale, lease, rental, while a data sharing legal basis is more intricate, as we are looking at network structures and co-operation. Second, although these principles do not qualify as soft law (lacking binding force but having legal effects) the Commission's communications set action plans for future legislation. Third, because the ultimate goal of these principles is to boost European artificial intelligence (AI) development. However, do these principles set a viable legal framework for data sharing, or is this public policy tool merely a naïve expectation? Moreover, would these principles set a successful path toward a thriving European AI advancement? In this contribution, I try to sketch some answers to these and related questions.

3 It is crucial to mention that EC private data sharing principles evaluation has clear connections to the data ownership debate.[4] This paper will neither re-examine this aspect nor the introduction of other possible doctrines,[5] nor review any other ramifications, such as the right to information privacy and personal data protection.[6] Finally, the assessment of these principles will also stay away from specific consumer law issues related to the use of personal data, including "counter performance" as proposed in the Digital Content Directive.[7]

4 This contribution is structured as follows: the first part will present the problems at stake: what is the current state of AI development in Europe, the availability of data for AI and the Internet of Things (IoT) research and development, and the current legal framework of data trading. The second part will evaluate the principles from an overall perspective focusing on their underlying goals. The evaluation will be addressed separately: first, the principles for business-to-business (B2B); and next, the principles for business-to-government (B2G) data trading will be considered. Last, the paper will conclude by answering the question of whether this public policy tool is merely an unrealistic expectation or whether it sets a favorable regulatory approach for a successful development of AI enabled technologies in the single market.

B. The Problems at Stake

I. The Status Quo of AI Development in Europe

5 Investment in artificial intelligence (AI) has rapidly increased in the last five years at the international level. According to a study presented in early 2018, which used basic research and market capitalization to track where AI is done, China leads the former statistic, with the U.S. behind and long followed by the UK, Germany, France and Italy.[8] When looking at market capitalization, the first four largest public companies with AI exposure are Apple, closely followed by Alphabet, Microsoft and Amazon,[9] all of which are headquartered outside Europe yet running business in the single market. Then, why is Europe behind the US and China with regards to capturing the opportunities of artificial intelligence?[10]

4 For an overview on the data "ownership" debate see: T. Hoeren, "A New Approach to Data Property?" (2018) 2018/2 AMI p. 58-60 <https://www.ami-online.nl/art/3618/a-new-approach-to-data-property> (accessed on October 15, 2018); B. Hugenholtz, "Data property: Unwelcome guest in the Houes of IP", 2018 <https://www.ivir.nl/publicaties/download/Data_property_Muenster.pdf> (accessed on October 15, 2018); J. Drexl, "Designing Competitive Markets for Industrial Data - Between Propertisation and Access" (2017) 8(4) JIPITEC p. 257; H. Zech, "A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data" (2016) 11 Journal of Intellectual Property Law & Practice, p. 460-470.

5 For an overview see: M. Dorner, "Big Data und *Dateneingentum*" (2014) Computer und Recht, p. 617-628; Osborne Clarke LLP, *Legal Study on Ownership and Access to Data* (2016) Study prepared for the European Commission DG Communications Networks, Content & Technology <https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1/language-en> (accessed on October 15, 2018).

6 See N. Purtova, "Do property rights in personal data make sense after the Big Data turn? Individual control and transparency", (2017) 10(2) Journal of Law and Economic Regulation November; Tilburg Law School Research Paper No. 2017/21 <https://ssrn.com/abstract=3070228> (accessed on October 15, 2018).

7 Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content, COM (2015) 634 final; see A. Metzger, "Data as Counter-Performance – What Rights and Duties do Parties Have?" (2017) 8(2) JIPITEC p. 2; A. Metzger, Z. Efroni, L. Mischau, J. Metzger, "Data-Related Aspects of the Digital Content Directive" (2018) 9(1) JIPITEC p. 1.

8 A. Goldfarb, D. Trefler, "AI and International Trade" (2018) National Bureau of Economic Research, Working Paper 24254, <http://www.nber.or/papers/w24254> (accessed on October 15, 2018), p. 2.

9 Ibid. p. 3.

10 See J. Manyika, "10 imperatives for Europe in the age of AI and automation" (2017) Report McKinsey Globarl Institute, October 2017 <https://www.mckinsey.com/featured-insights/europe/ten-imperatives-for-europe-in-the-age-of-ai-and-automation> (accessed on October 15, 2018).

6 First, for AI innovation to happen, R&D is a must. In the sector of AI this translates into "for AI technologies to evolve, machine learning (ML) needs to happen". Machine learning is a subset of AI that allows computer systems to learn by analyzing huge amounts of data and drawing insights from it rather than following pre-programmed rules.[11] It requires lots of data to create, test, and "train" the algorithms underlying the AI. Examples can be found in several fields; for instance, in drug discovery, Sanofi has signed a deal to use UK start-up Exscientia's AI platform to hunt for metabolic-disease therapies, and Roche subsidiary Genentech is using an AI system from GNS Healthcare in Cambridge, Massachusetts, to help drive the multinational company's search for cancer treatments.[12] Another example from a completely different sector is Alexa, Amazon's powered Echo cylinder. The household artificial intelligence device helper that can turn off the lights, tell jokes, or let us read the news hands-free. It also collects reams of data about its users, which is used to improve Alexa and add to its uses. How does this happen? 99% of the processing of Alexa takes place in Amazon's Cloud. As the technology is based on voice recognition, the device needs to always be "alert" listening, but not recording. The moment the machine recognizes the word "Alexa" or another similar wake word, it activates, starts recording and the snippet is sent to Amazon's cloud, and is used for further training of the AI device.[13] However, it is important to note that not all AI systems have the same type of data requirements, some are more "data-hungry" than others. Thus, as AI-enabled technologies are becoming more important to the economy, so too are large quality datasets. Large datasets, meaning structured (not raw) data, are critical input for companies that want to create and develop AI systems. Even the best AI algorithms would be useless without an underlying large-scale dataset, because datasets are needed for the initial training and fine-tuning of these algorithms. Therefore, we are talking about collections of separate sets of information that the computer, the algorithm, will treat as a single unit. It includes raw and processed data, information, and so on. To produce large datasets a considerable investment is necessary, and not all firms involved or who want to enter the AI technology market can afford these costs. However, a business that lacks access to good datasets faces a substantial barrier to entering a market involving AI technologies.

7 Second, most data used for research and development of AI technologies come from the Internet of Things (IoT). Although the definition on what IoT is fuzzy,[14] expressions such as "smart cars", "smart phones", "smart homes" are common nowadays. We normally relate such an expression to sensors embedded into devices of all kinds, which are connected to the Internet and transfer data over a network. But in fact, all IoT-related devices, no matter how different they may be, do much more than that. IoT related devices always follow five basic steps: they sense (the environment); they transmit (data); they store (data); they analyze (datasets); and then, act on (datasets). For any IoT application to be worth buying (or making), it must demonstrate value in the last step of that chain, the "act on."[15] AI and IoT are intrinsically connected and in need of each other to unleash their potential. The true value of any IoT product and byproduct is determined by AI, or more precisely, by the machine learning process. The reason is that machine learning allows the creation of smart actions that make IoT products and byproducts valuable to consumers. The key is to find insights in datasets.

8 Third, although the volume of data increases fast it is not really available between economic operators. Recent predictions are that by 2020, the number of IoT connections in Europe will reach 6 billion.[16] According to a 2017 research report by the Centre for the Promotion of Import from developing countries (CBI), Europe has an almost 40% share of the global IoT market, projected to reach a value of around €1.2 trillion in 2020.[17] However, the existence of

11 The Royal Society, *Machine Learning: The Power and Promise of Computers that Learn by Example*, (2017), p. 49 <https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf> (accessed on October 15, 2018).

12 See N. Fleming, "How artificial intelligence is changing drug discovery" (2018) 557 Nature S55-S57, <https://www.nature.com/articles/d41586-018-05267-x> (accessed on October 15, 2018).

13 For further details see: Amazon's website section on machine learning at: <https://aws.amazon.com/machine-learning/?nc1=h_ls> (accessed on October 15, 2018); S. Levy, "Inside Amazon's Artificial Intelligence Flywheel" (2018) Wired <https://www.wired.com/story/amazon-artificial-intelligence-flywheel/> (accessed on October 15, 2018).

14 See R. Minerva, A. Biru, D. Rotondi, "Towards a Definition of the Internet of Things (IoT)" (2015) IEEE <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf> (accessed on October 15, 2018).

15 "To act on" can mean an infinite number of things, ranging from a profound physical action (e.g. deploying an ambulance to the site of a car accident) to merely providing basic information to a relevant consumer (e.g. sending a text message to alert a driver that their car needs an oil change). But no matter what the ultimate step of "act on" actually is, it's value is entirely dependent on the penultimate analysis.

16 EC Final report - Study "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination", March 31, 2016, p.10; SMART number 2013/0037 <https://publications.europa.eu/en/publication-detail/-/publication/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1/language-en> (accessed on October 15, 2018).

17 See: "The Internet of Things in Europe" (2017) CBI-Ministry of Foreign Affairs <https://www.cbi.eu/market-information/outsourcing-itobpo/internet-things/> (accessed on October 15, 2018).

major issues regarding access and transmission of the data generated by IoT devices has been well recognized by the January 2017 European Commission's Communication "Building a European Data Economy". Much of those data are generated, retained and later on analyzed in "silos" by the "owners" of the technology.[18] This makes it very difficult for (European) businesses and organizations to access and use datasets. If companies face high barriers to accessing such datasets, then they may opt not to enter a market that requires large datasets as inputs, leading to less competition. Companies may forgo entry because of this difficulty, and so competition would decline in both new and established markets. Consequently, a lack of shared data access would harm consumers, sometimes via higher prices, sometimes via a reduction in the number of improved features or other innovations.

9 Altogether, Europe is running behind in the AI global race and in need of a strategy that promotes the democratization of data to overcome these challenges. If this current situation were due to a market failure, a regulatory intervention would be justified. Yet, would the EC's proposed contractual principles suit?

II. Availability of Data for AI and IoT Research and Development

10 A pre-condition of data sharing and data transfer is data access. As mentioned, access to privately held and controlled data is considered by the EC as key to the development of AI and IoT technologies in Europe, and only accessed data can be re-used.

11 Datasets' access and use are directed by both contractual and technical factors.

12 At the contractual level, there is a range of permissions, policies, legal considerations, personal and organizational preferences, and other factors that impact the data access rights. Rights, in this context, may cover permissions to view, use, reuse, repurpose, or distribute data. Metadata attributes, such as "rights management," can be assigned to data manually or automatically. When applied, rights management indicates data access status and use conditions. These conventions are primarily contractual and inform technical aspects of system design. To understand the complexities of data access, both contractual and technical, it is helpful to first review the status of data access; specifically, what is meant by open and closed data.

13 The term open data is very specific and covers two different aspects of openness. First, the data is legally open, which in practice generally means that the data is published under an open license and that the conditions for re-use are limited to attribution. Second, the data is technically open, which means that the file is machine readable and non-proprietary where possible. In practice, this means that the data is free to access for everybody, and the file format and its content are not restricted to a particular non-open source software tool.[19] The absence of restriction surrounding open data extends to any endeavor, including commercialization. There are a range of licenses that data producers or data hosts append to data, indicating open access.[20]

14 Following the Open Data Institute's definition, closed data refers to data that can only be accessed by its subject, owner or holder.[21] Closed data often contain private or sensitive information. Closed data extend across a wide range of entities, topics, and environment. Examples of closed data include personal, institutional, or industry data identifying financial resources (e.g., sums, transactions, account numbers), personal information relating to health and well-being, or status (e.g., married, single, divorced). Data may also be designated as closed, or regulated by controlled access, due to legal restrictions or organizational policies protecting current or predicted value.[22] More specifically, data access is often restricted because of a known or perceived competitive advantage, and the associated risks with making it public, including misuse, if the data fall into the wrong hands. Closed data are accessible to individuals or organizations who have the appropriate permissions.

15 Currently, most AI-centered innovation is based on a business model where most training datasets are considered closed data. Such datasets as noted before, are in private silos, not necessarily in machine readable and non-proprietary formats. Data storing is already well established as a defensive strategy among AI-centric companies. Google, Microsoft and others have open-sourced lots of software, and even hardware designs, but are less free with the kind data that make such tools useful.[23] Many startups

18 Commission, "Building a European data economy" (Communication) COM (2017) 09 final.

19 See European Data Portal, General Definition of Open Data <https://www.europeandataportal.eu/en/providing-data/goldbook/open-data-nutshell> (accessed on October 15, 2018).

20 See Creative Commons Licenses at: <https://creativecommons.org/> (accessed on October 15, 2018).

21 Definition by the Open Data Institute, available at: <https://www.theodi.org> (accessed on October 15, 2018).

22 See T. Aplin, "Trading Data in the Digital Economy: Trade Secrets Perspective" in S. Lohsse, R. Schulze, D. Staudenmayer (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden Baden, Nomos 2017), p. 59.

23 T. Simonite, "AI and Enormous Data Could Make Tech Giants

and small and medium sized enterprises (SMEs) have no bargain power when negotiating a license to get access and use of training datasets as neither can afford the costs.

16 A second challenge when looking at the licensing of datasets is that data can be protected by an overlapping patchwork of different intellectual property rights[24] and contractual restrictions on the purposes for which the data can be used. For example, one common misconception is that any freely available online data can be re-used for any purpose. This often isn't the case; website terms and conditions along with copyright and other IP rights, such as the database right, can prevent the data from being used to train a machine learning system. From the practical point of view, many SME's are faced with the problem (and associated costs) of drafting B2B licensing contracts with a necessary degree of legal certainty in respect of the conditions for and the scope of the uses allowed by third parties, and Europe lacks any sort of standard contracts or best practices in this regard.

17 As previously mentioned, access to closed data is considered by the European Commission as key to the data economy and the development of AI technologies since only accessed data can be re-used. As the Commission acknowledged in their Communication "Building a European data economy"[25] when evaluating the question of "ownership" of data in the industrial context, "voluntary data sharing might emerge, but negotiating such contracts could entail substantial transaction costs for the weaker parties, when there is an unequal negotiation position or because of the significant costs of hiring legal expertise".

18 Finally, if access to data is denied, the question of compulsory licensing becomes relevant,[26] as well as competition law intervention. But in the case of access to datasets - as it will be explained in a subsequent section - relying on competition law as the only regulatory tool might not be to the smartest move.

19 Availability of training datasets for AI and IoT R&D is still a hurdle, that, if not reduced, could stifle SMEs' innovation, reduce the overall size of the AI market and the benefits that AI could bring to the society.

Harder to Topple" (2017) Wired, July, 2017 <https://www.wired.com/story/ai-and-enormous-data-could-make-tech-giants-harder-to-topple/> (accessed on October 15, 2018).

24 For a detailed explanation of the current intellectual property rights framework of data in the EU, see B. Hugenholtz, supra n 4.

25 See supra n 18.

26 For a detailed study on compulsory license in data trading see: R. H. Weber, "Improvement of Data Economy Through Compulsory Licenses?" in S. Lohsse, supra n 22, p. 137.

C. Legal Framework of Data Sharing in Europe

20 If we look at the data trading (and sharing) relationships within the European single market, three are the existing dataset streams: public sector information to companies (i.e. government to business or G2B); companies to public bodies (i.e. business to government or B2G); and company to company (i.e. business to business or B2B). Until now, only one these flows has been partly regulated - the G2B.

21 The public sector is one of the most data-intense sectors within the European Union. Public Sector Information (PSI) is the wide range of information that public sector bodies collect, produce, reproduce, and disseminate in many areas of activity while accomplishing their institutional tasks. In other words, public sector information means information public bodies produce as part of their public task. That is, as part of their core roles and functions, as defined in legislation or established through custom and practice.

22 Access and re-use of these data have been regulated via the PSI Directive.[27] The PSI Directive, provides a common legal framework for a European market for government held data. The Directive was subject to a review in 2013 and is currently under review again. The aim of the current revision is to strengthen the position of SMEs by dismantling market barriers to reusing public sector information for commercial purposes. This is because re-use of open data by private companies could contribute to the development of AI and IoT markets.

23 According to the impact assessments,[28] there are three main barriers:

- data generated by utilities, transport and publicly funded research have tremendous re-use potential, but are not covered by the current rules, even though much of this research is fully or partly funded by public money;
- real-time access to public sector information is rare. This prevents the development of products and services using real-time information, such as meteorological and transport apps, and;

27 Council Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information [2013] OJ L 175/1.

28 Available at: <https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-4540429_en> (accessed on October 15, 2018).

- the re-use of PSI data can be very expensive, depending on the public institution offering them.

24 We need to wait and see the outcomes of the discussions between the European Parliament and the Council before any further evaluations.

25 Sharing of datasets both in B2B or B2G relationships falls under contract law and the principle of freedom of contract.

26 As contract law is part of the Member States' national law, the rules around private and public organizations entering into a contract for data sharing, access, use and re-use are essentially the subject matter of national law.

27 The same applies to regulations on contract terms, which are left for the Member States to decide upon under national law. Besides, B2B contract terms have long been supported by freedom of contract and distinguished from business-to-consumer (B2C) which are heavily regulated. For instance, B2B unfairness control of standard terms and conditions is an unfamiliar concept for the majority of Member States where such a regime does not exist and in others where it does exist, like in Germany, it has been criticized.[29]

28 However, in the last years and in certain sectors, studies and consultations commissioned and launched by the EC have shown important concerns regarding specific types of B2B trading practices. They also stem from the view that B2B relationships are not to be completely left for the parties to determine but that the weaker party, often an SME, should be given certain legal protection in a way that cannot be displaced or agreed otherwise between the parties. An example of this is the Directive (EU) 2015/2366 on payment services (PSD2 Directive),[30] which was implemented at national level in January 2018, and gives Member States discretion to treat SMEs as consumers in applying the conduct of business rules when a payment service is provided to them.[31] The Food Supply Chain Proposal Directive is another example into the same direction.[32] A third example is the Proposal for a Regulation on Online Platforms,[33] published in April 2018, which provides the same protections for both SMEs and non-SMEs using the online intermediation services.

29 In the current normative framework, only competition law provides a very wide basis to prevent abuses in both B2B or B2G. In the case of data sharing this would be between a data holder and a party (another firm or a public body) who wants to have access and/or use to the particular data.

30 Some scholars have proposed the need of regulatory intervention by crafting default contract rules.[34] This would provide a general legal standard on what a balanced distribution of rights and obligations is in a contractual relationship between the data holder and the other party requesting data access and/or use. Some stakeholders have showed their disconformity with this regulatory approach[35] and consider no legal intervention is necessary.

31 Additionally, as explained in the previous section, contractual relationships between parties trading in data imply the use of licenses. Model licenses or non-mandatory rules on the use and content of licenses might not be enough to democratize access and use of closed data and boost artificial intelligence in Europe. Particularly in the case of B2G supply of private data under conditions for re-use, one should wonder whether and to what extent mandatory licenses would be necessary, or whether public organizations and private companies should be left on their own under the principle of freedom of contract.[36]

29 See: M. Lehman, J. Ungerer, "Save the Mittelstand: How German Courts Protect Small and Medium-Sized Enterprises from Unfair Terms" (2017) 25(2) European Review of Private Law, pp.313, recommending not to emulate the German B2B control of standard terms model on the European level.

30 Council Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, [2015] OJ L 337/35. (PSD2 Directive).

31 Article 38 PSD2 Directive.

32 Proposal for a Directive of the European Parliament and of the Council on Unfair Trading Practices in Business-To-Business Relationships in the Food Supply Chain Com/2018/0173 Final - 2018/082 (Cod).

33 Proposal for a Regulation of the European Parliament and of the Council on Promoting Fairness and Transparency for Business Users of Online Intermediation Services COM 2018/0112 Final - 2018/328.

34 F. Graf von Westphalen, "Contracts with Big Data -The End of the Traditional Contract Concept?" in S. Lohsse, supra n 22, p. 249; Twigg-Flesner, "Disruptive Technology -Disrupted Law? How the Digital Revolution Affects (Contract) Law" in De Franceschi (ed.) *European Contract Law and the Digital Single Market*, (Intersentia 2016), p. 21.

35 See individual responses to EC Consultation Building an European Data Economy by Bayer AG; Industry Coalition on Data Protection (ICDP); Community of European Railway and Infrastructure Companies (CER); Ibec; available at: <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy> (accessed on October 15, 2018).

36 On the need of compulsory licenses in data sharing and transfer see: R. Weber, "Improvement of Data Economy through Compulsory Licenses?" in S. Lohsse, supra n 22, p. 137; M. Grützmacher, "Data Interfaces and Data Formats as Obstacles to the Exchange and Portability of Data: Is there a Need for (Statutory) Compulsory Licensing" in S. Lohsse, supra n 22, p. 189.

32 When looking at this complex scenario, the (non-mandatory) contractual principles published by the European Commission might seem a toddler step, but we should not forget that their Communications are a public policy tool which set action plans for future legislation.

33 Considering the above, another fact that is worth mentioning in this context: on April 23, 2018, two days before the EC's Communication and its guidance on contractual principles were published, a coalition of associations from the EU agri-food chain presented a joint "EU Code of Conduct on Agricultural Data Sharing".[37] This self-regulation instrument promotes the benefits of sharing data and enables agri-business models to swiftly move into digital data enhanced farming. The eleven pages of the Code shed greater light on contractual relations and provide guidance on access and use of data topics. It is important to recall that both the agriculture and automotive sectors have been at the heart of the debate around "data ownership" and "data access", thus the relevance of a sectorial code of conduct which focuses on data access and re-use, rather than in ownership regimes.

34 This can be also a symptom that self-regulation could be followed by other sectors, such as mobility, health, automotive, energy or aerospace, where industries are rather reluctant about the establishment of data access claims;[38] maybe because they are aware that there is no one-way system and that today's plaintiff could be on the other side tomorrow, being forced to provide access to competitors.

35 All in all, for both, boosting Europe's AI technology and harvesting the full benefits of IoT, companies also need to understand the practicability and impact of the principles proposed by the Commission. Thus, looking closer at the principles themselves might shed some light on what kind of legal intervention, if any, the future would bring.

D. Evaluating the Principles on Private Data Sharing

36 The EC Communication and its accompanying working document[39] present two separate sets of principles, which are meant to serve as a guide on contractual relations where data are shared between business organizations or where data are supplied by a business organization to public sector bodies. To evaluate them and answer the question of their practical use, the analysis will go as follows: first, a look into the policy reasons motivating them, as described in the introduction of the Communication and the Guidance; and second, as these principles and their underlying goals correspond to different contractual relationships, B2B and B2G, a separate analysis of each set of principles. Within the latter part, the B2B analysis will concentrate on their underlying objective, namely (to) "ensure fair markets for IoT objects and for products and services relying on data created by such objects". This connects with the debate on contract standard terms and the challenges of leaving the prevention of abuses in B2B alone to competition law. The B2G analysis will focus on the principles' primary reason, which is to "support the supply under preferential conditions for re-use." This would lead to the notion of public interest in the use and re-use of private sector (closed) data.

I. Policy Behind the Principles

37 When reading the introduction to these principles, one cannot miss the same and truthful common message in many of the Commission communications related to the EC's big-data strategy and the European data economy: "data-driven is a key enable of growth and jobs in Europe. The importance of data collected online and generated by the Internet of Things (IoT) objects, and the availability of big data analytics tools and artificial intelligence applications are key technical drivers."

37 Available at: <http://www.cema-agri.org/publication/new-brochure-eu-code-conduct-agricultural-data-sharing> (accessed on October 15, 2018).

38 See M. McCarthy, et al. "Access to In-Vehicle Data and Resources" (2017) EC Final Report May 2017, p. 55, 194 (Access to In-Vehicle Report) and M. Barbero et al, EC Final Report "Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability" (2016) SMART number 2016/0030, p. 31 and ff. (Emerging Issues Report).

39 See supra n 1 and n 2.

38 As some economic studies have shown,[40] we should take this statement with a grain of salt due to several reasons.

39 In the first place, it is indeed true that data can be used multiple times without inherently diminishing its value; thus, fostering the sharing and re-use of data among companies is logical. But for those who harvest data, sharing and making datasets available for re-use in certain formats come with high costs. Therefore, although data as such is a nonrival resource, it might not always be efficient for companies who have invested in data collection to share such datasets as a matter of principle with other companies only for the sake of maximum data exploitation. In this regard, the nonrival nature of data should not alone be *per se* turned into a maximum efficiency argument pro-data sharing.

40 Second, data have no value in themselves, only at their point of use. This is why we should be talking about "datasets" instead of "data". To deliver value, datasets need to be mixed and merged with other datasets.[41] The data holder is not always best placed to extract value from those datasets: this player could lack the skills, the culture or the incentives to deliver innovation. In other words, as Walsh and Pollock said: "the coolest thing with your data(sets) will be thought of by someone else."[42] But even if in some cases the most innovative applications come from unpredictable usage of existing datasets, this should not be considered as the general rule.

41 Last, the same degree of caution should apply when making statements about how businesses already benefit from access to public sector information available as Open Data. For instance, one study concludes that although the focus of the PSI Directive is to encourage commercial activity in the hope that this leads to new business models and economic growth, a harmonized Digital Single Market of PSI is still far from being a reality.[43] Thus, the EU institutions' ambition of creating a harmonized public information market across the EU, both in terms of the type of underlying works and in terms of compatibility of processes, licensing and formats, is still in the works (and under review).

II. The Business-to-Business (B2B) Principles

42 There are five key principles that, if respected, would ensure fair and competitive markets: transparency; shared value creation; respect for each other's commercial interests; (to) ensure undistorted competition; and, (to) minimized data lock-in.

43 The Communication defines each as follows:

a) **Transparency**: The relevant contractual agreements should identify in a transparent and understandable manner (i) the persons or entities that will have access to the data that the product or service generates, the type of such data, and which level of detail; and (ii) the purposes for using such data

b) **Shared value creation**: The relevant contractual agreements should recognize that, where data is generated as a by-product of using a product or service, several parties have contributed to creating the data.

c) **Respect for each other's commercial interests**: The relevant contractual agreements should address the need to protect both the commercial interests and secrets of data holders and data users.

d) **Ensure undistorted competition**: The relevant contractual agreements should address the need to ensure undistorted competition when exchanging commercially sensitive data.

40 N. Duch-Brown, B. Martens, F. Mueller-Langer, "The Economics of Ownership, Access and Trade in Digital Data" (2017), JRC Digital Economy Working Paper 2017-01, available at: <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf> (accessed on October 15, 2018); W. Kerber, J.S. Frank, "Data Governance Regimes in the Digital Economy: The Example of Connected Cars" (November 3, 2017); available at: <https://ssrn.com/abstract=3064794> (accessed on October 15, 2018); W. Kerber "Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective" (September 1, 2017). Forthcoming in S. Lohsse, R. Schulze, D. Staudenmayer (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools,* (Baden Baden, Nomos 2017); <https://ssrn.com/abstract=3033002> (accessed on October 15, 2018).

41 On the question of whether these datasets could be protected under the sui generis database right, the answer is probably not. As Hugenholtz's explains, it seems that for the European Court of Justice "investment in 'creating' data does not count towards investment (criterion for protection), even if such epistemological distinction between 'creating' and 'obtaining' data is not self-evident". For a detailed explanation, see B. Hugenholtz, "Data property: Unwelcome guest in the House of IP" (supra n 4) p. 7-8.

42 J. Walsh, R. Pollock, "The coolest thing to do with your data will be thought of by someone else", (2007) Open Data and Componentization, XTech2007 available at: <http://assets.okfn.org/files/talks/xtech_2007/> (accessed on October 15, 2018).

43 A. Wiebe, N. Dietrich (eds.) "Open Data Protection: Study on legal barriers to open data sharing – Data Protection and PSI" (2017) Universitätverl. Göttingen, p. 248.

e) **Minimized data lock-in**: Companies offering a product or service that generates data as a by-product should allow and enable data portability as much as possible[44]. They should also consider, where possible and in line with the characteristics of the market they operate on, offering the same product or service without or with only limited data transfers alongside products or services that include such data transfers.

1. Principles' Goal: Fostering Data Sharing Environments to Ensure Fair and Competitive IoT Markets

44 On the B2B data sharing, the underlying goal is to "ensure fair markets for IoT objects and for products and services relying on data created by such objects."

45 When looking at the results of the Synopsis Report Consultation on "Building a European Data Economy",[45] it is interesting to note that a considerable majority of the stakeholders were against any kind regulatory intervention because in their view, some of the data access issues set out in the Communication may result from the normal dynamic of an emerging market, rather than from a market failure.[46]

46 The question is why the Commission proposes this set of principles under the above-mentioned goal. Even though there is no clear evidence of a market failure, as recent economic studies have pointed out, it is not less true that we are in an ecosystem with a predominant presence of (traditional) data "silos".[47]

47 For IoT and AI markets to emerge and consolidate in the European Union, we need a data sharing ecosystem. It is to the setting of such ecosystems that the Commission is proposing these five guiding principles. It also needs to be clearly stated that when considering IoT (and AI applications as an extension of IoT), we are talking about several markets, thus "markets for IoT objects and market for products and services relying on data created by such objects."[48]

48 To help to understand this previous statement, it is crucial to understand what an IoT ecosystem consists of:

49 First, IoT objects do not "create" data but rather "collect" or "collect and act on" data. These objects are a different set of elements which constitute the first building block of an IoT platform. Those devices are part of the so-called physical layer, the hardware, the "thing". These sensors, actuators and devices collect data from the environment or perform actions in the environment. They need certain computing power, electric power, cooling, memory, sometimes a special footprint, multimedia support, and connectivity. However, they do not work alone, they are part of an ecosystem - the platform. Accordingly, the electronic utility that measures physical properties, the sensor, sends collected data to an aggregator in a cloud that transforms groups of "raw data" into "intermediate data." To get to the cloud, the sensor can be connected through a variety of methods including: cellular, satellite, WIFI, Bluetooth, low-power wide-area networks (LPWAN) or connecting directly to the internet via ethernet. Once the data gets to the cloud, software performs some kind of processing and then might decide to perform an action that goes back to the user.

50 Second, data management of IoT data is different from traditional data management systems. In traditional systems, data management handle the storage, retrieval, and update of elementary data items, records and files. In the context of IoT, data management systems must summarize data online while providing storage, logging, and auditing facilities for offline analysis.[49] Pattern recognition and data mining techniques can be used for the multitude of IoT applications and produce datasets, that, simply put could be useful for self-improvement of the IoT sensor itself, as well as for the development of new products, byproducts or services that might have no correlation with the initial aim for which data was collected in the first place, as illustrated in the figure below. For instance, data generated

44 "E.g. data produced by robots in the context of industrial processes, relevant for provision of after-sales services (e.g. repair and maintenance), or data on the rating of service providers."

45 See Annex to the Synopsis Report: Detailed analysis of the public online consultation results on "Building a European Data Economy" <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation--building-european-data-economy>, p. 12-13 (accessed on October 15, 2018).

46 See individual responses by Bayer AG; Industry Coalition on Data Protection (ICDP); Community of European Railway and Infrastructure Companies (CER); Ibec; available at: <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy> (accessed on October 15, 2018).

47 N. Duch-Brown, supra n 40; W. Kerber, J.S. Frank, "Data Governance Regimes in the Digital Economy: The Example of Connected Cars" (2017) <https://ssrn.com/abstract=3064794> (accessed on October 15, 2018); W. Kerber "Rights on Data: The EU Communication "Building a European Data Economy" from an Economic Perspective" (September 1, 2017) forthcoming in S. Lohsse, R. Schulze, D. Staudenmayer (eds.), *Trading Data in the Digital Economy: Legal Concepts and Tools,* (Baden Baden, Nomos 2017) <https://ssrn.com/abstract=3033002> (accessed on October 15, 2018).

48 See supra n 2, p. 3.

49 M Abu-Elkheir et al., "Data Management for the Internet of Things: Design Primitives and Solution, Sensors" (2013) Nov (11) p. 15582-15612; doi:10.3390/s131115582.

by location sensors could potentially be used by publishers to understand and reach a precise local audience or give local context to end-users.

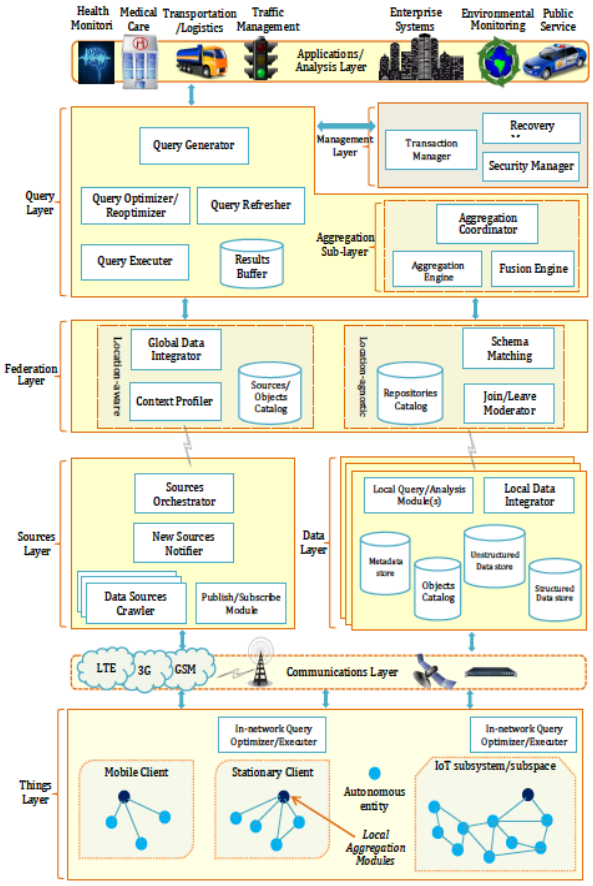

Fig. 1: IoT data management framework[50]

51 Next, we need to understand what IoT platforms consist of. An IoT platform is what makes IoT happen for the devices, that is, an IoT platform is an integrated service that offers the necessary tools to bring physical objects online. Trying to make it as simple as possible, and depending on the tools it provides, an IoT platform can be classified as:

- end-to-end or general IoT platform, providing the hardware, software, connectivity, security and device management tools to handle millions of concurrent device connections. A well-known example is Particle;
- connectivity management platforms, providing low power and low-cost connectivity through WIFI and cellular technologies, as in the case of Sigfox;
- cloud platforms, mainly enterprise software vendors that are offered by cloud service providers who extend typical enterprise services to include IoT capabilities, such as Google Cloud or Amazon Web Services; and,
- data platforms, providing data tools that allow routing device data and management and visualization of data analytics, such as Microsoft Azure.[51]

52 Nonetheless, each of the IoT platforms listed above can provide very different byproducts, solutions and uses, completely different from a vertical perspective; from smart systems, such as Salesforce, which is connected to Microsoft Outlook, an Oracle Database and various sales phone systems. In this case, instead of having multiple places to sort through data, a custom designed dashboard can bring in all of this data into a single pane view. This IoT platform allows correlations discovering and process elimination of inefficiencies. Another type of IoT vertical platform is an industrial IoT, normally used by manufacturers, energy or healthcare, because it integrates Big Data, Machine-to-Machine (M2M) communication, machine learning, smart equipment or robots, and an array of sensors into optimizing processes within a system. Last but not least, if we consider Echo Amazon (popularly known as Alexa), this technology includes particular capabilities that have even prompted Apple's founder to describe Alexa as the next big IoT platform.[52] We could endlessly continue as there are IoT platforms of every shape and size. There are platforms for specific industries like commercial real estate and family health. Some focus on one type of device; for example, there are platforms focused on augmented-reality headsets, whilst some are focused on a particular function, like manufacturing.[53] There are even IoT platforms for pets.[54]

53 Also, from a single dataset perspective, a data marketplace is a platform on which datasets can be offered and accessed.[55] Often cited examples are the Microsoft Azure Marketplace, Xignite, Gnip, AggData, or Cvedia. Data that are being offered may be static archives or online streams of new data. Different

50 Ibid.

51 For a similar breakdown explanation see J Lee, "How to Choose the Right IoT Platform: The Ultimate Checklist" (2018) Medium <https://hackernoon.com/how-to-choose-the-right-iot-platform-the-ultimate-checklist-47b5575d4e20> (accessed on October 15, 2018).

52 See <http://www.businessinsider.com/steve-wozniak-thinks-amazon-echo-is-the-next-big-platform-2016-3?international=true&r=US&IR=T> (accessed on October 15, 2018).

53 See Mckinsey Global Institute, "The Internet of Things: Mapping the Value beyond the Hype" (2015) June <www.mckinsey.com> (accessed on October 15, 2018).

54 See Mindsight, "Smart Pet Tech and The Intern et of Things" (2016) at: <https://www.gomindsight.com/blog/smart-pet-tech-and-the-internet-of-things/> (accessed on October 15, 2018).

55 F. Schomm, F. Stahl, G. Vossen "Marketplaces for data: an initial survey" (2013) 42(1) ACM SIGMOD Record p. 15-26.

modes of access may be offered; for instance, whole repositories, APIs or subscriptions. These are called "data products" as well, where the estimation of the value of such datasets is a continuous challenge.[56]

54 Finally, the latest reports on IoT platforms vendors alone in the global market, reveal that their number reached a new record in 2017, reaching 450 - a 25% increase compared to the 360 of the previous year.[57] Most of the increase occurred in the industrial and manufacturing sectors with more than half of the vendors headquartered in the US; the IoT analytics' report also shows that more than 30 vendors included in 2016 have ceased to exist in 2017, they have either gone out of business or been acquired by others. Furthermore, if we search *Crunchbase*[58] for venture-funded IoT platforms, we will find well over 100 hits. This list does not include bigger technology players entering the market with IoT platforms like Microsoft, IBM, and SAP or several industrial companies with similar aspirations like GE, Bosch, and Siemens.

55 In view of this wide-ranging array of horizontal and vertical potential markets for IoT, ranging from hardware, software, connectivity and storage to humans using the information created from data analysis in order to make better decisions. In an ecosystem where IoT platforms are the essential element, collaboration by means of data sharing is more important than ever before. When businesses share data, it is usually for mutual benefit, determined by commercial negotiation and agreed contract terms. But as the study "Cross-Cutting Business Models for IoT" shows, in the IoT scenario, one step further than traditional cooperation, such as the application of an open business model, where data sharing is fundamental, will be key.[59]

56 These principles might constitute a good first step towards enabling adequate market conditions for both IoT and AI markets and for the creation of B2B platforms.

2. Introducing Non-Mandatory Contract Terms in B2B

57 Overall these principles may be seen as too simplistic, but one cannot lose sight that they are framed in a Communication and that its accompanying document makes clear that "model contract terms for different types of data sharing agreements and for some sectors or types of data sharing are already being developed."[60] The measure comes originally from the Telecommunications Sector. In particular, on page 42 of the "Annex to the Commission Implementing Decision on the adoption of the work program for 2018 and on the financing of Connecting Europe Facility (CEF)".[61] We should not forget that the telecommunications sector has already faced very similar problems regarding giving access and re-using closed data and it may be worth looking at them for useful or inspiring solutions.

58 The Connecting Europe Facility (CEF) in Telecom[62] is a key EU instrument to facilitate cross-border interaction between public administrations, businesses and citizens, by deploying digital service infrastructures (DSIs) and broadband networks. If recalling what IoT platforms consist of, as explained above, the establishment of a Core Service Platform (central hubs which enable trans-European connectivity) with a Support Centre for data sharing, to support the knowledge exchange between all actors in the data economy would make sense. The aim of this Support Centre is also to provide practical advice, best practices, and methodologies for both data sharing and data analytics, and it will become operative in early 2019.

59 If looking at the principles in detail, the transparency one might somewhat resemble Article 5 of the Unfair Terms in Consumer Contracts Directive (UTD).[63] Yet, it is important to recall that B2B relationships have long been underpinned by freedom of contract and distinguished from B2C relationships which are heavily regulated. For instance, the European

56 A. Muschalle, et al. "Pricing approaches for data markets" (2012), IEEE 15th International Workshop on Business Intelligence for the Real-Time Enterprise.

57 See <https://iot-analytics.com/iot-platforms-company-list-2017-update/> (accessed on October 15, 2018).

58 See <www.crunchbase.com> (accessed on October 15, 2018).

59 PricewaterhouseCoopers, EC Final report – Study "Cross-Cutting Business Models for IoT" (2017) Study prepared for the European Commission DG Communications Networks, Content & Technology, SMART number 2016/0027.

60 See p. 6 of EC SWD (2018) 125 final, supra n 2. (Certain increase level of clarity or better placement of this non-regulatory measure would have been welcome, as one needs literally to fish in to find it).

61 Annex to the Commission "Implementing Decision on the adoption of the work program for 2018 on the financing of Connecting Europe Facility (CEF) – Telecommunications Sector", C (2018) 568 final – Annex, February 5, 2018.

62 See <https://ec.europa.eu/inea/en/connecting-europe-facility> (accessed on October 15, 2018).

63 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29. Article 5: "*In the case of contracts where all or certain terms offered to the consumer are in writing, these terms must always be drafted in plain, intelligible language. Where there is doubt about the meaning of a term, the interpretation most favorable to the consumer shall prevail. This rule on interpretation shall not apply in the context of the procedures laid down in Article 7 (2).*"

Commission's Green Paper which looked into B2B relationships in the sector of food supply chain,[64] described freedom of contract as a "cornerstone of any B2B relationship in the market economy";[65] consequently, parties should be able to design a contract that best suit their needs. Nonetheless, this well-established legal principle is increasingly questioned in recent times due to a lack of bargaining position of one of the parties to negotiate the terms on which they trade datasets.

60 Transparency is a precondition for fairness and good faith. In that sense, it might be worth looking at what the European Court of Justice (ECJ) has ruled on Article 3(1) of the UTD and its unfairness test. Because although the Directive applies exclusively to B2C relationships, the ECJ has applied this unfairness test to some B2B transactions. The UTD defines unfairness by resorting to broadly formulated standards of good faith and significant imbalance. The ECJ has stated in both *Invitel* and *VB Pénzügyi* that it is up to the national courts to adjudicate whether such "significant imbalance" exists in view of the respective contract term and all other terms, based on the applicable contract rules of the national law of the Member State.[66] Therefore, national rules must construe the benchmark for finding whether a contractual term causes a "significant imbalance" and is "contrary to good faith".[67]

61 At the European level[68] recent legislative proposals have agreed that B2B relationships are not to be completely left for the parties to determine, but that the weaker party, often an SME, should be given certain legal protection in a way that cannot be displaced or agreed otherwise between the parties. Declarations made by *Elżbieta Bieńkowska*, Commissioner for Internal Market, Industry, Entrepreneurship and SMEs, on April 24, 2018 follow this line of thinking: "We want to prevent the fragmentation of the Single Market through a patchwork of national rules. Today, the Commission is coming forward with an approach that will give EU businesses – particularly smaller ones – the transparency and redress mechanisms that will help them embrace the digital economy. It also gives platforms legal certainty." Moreover, as explained in previous sections in the PSD2 Directive, there is an example where an SME is treated as a consumer in a B2B relationship with regards to transparency of conditions and information requirements for payment services.[69] All the above builds on the studies and consultations related to data ownership and data sharing.[70]

62 In the Guide, the principle of **transparency** is linked to clearly expressing who has access to the datasets, what type of datasets are given access to and to what level of detail, and also for what purpose(s) is access and/or use license, all key to gain trust among parties. Whether this could also be a matter of **unfairness**, the truth is that to be able to identify who has been given access to datasets is essential to either determine any kind of liability for accuracy or completeness problems, damages arising from further connections, or use of the dataset by machines, devices, data user or third parties. But also, for determining liability in case of unlawful disclosure of trade secrets. Tentatively, a transparency principle could potentially help to assess a refusal to license situation as the more information provided in the contract on the datasets, the easier it could be to evaluate datasets substitutivity.

63 Similar reasons fall under **the shared value creation** principle and **respect for each other's interests**. The assurance of undistorted competition is limited to the exchange of commercially sensitive data. This could suggest a reassurance of the protection of trade secrets and protecting against tampering in particular. Both were flagged in the Synopsis Report as two core fears for B2B relationships not to share information as well as why business partners in joint projects are sometimes not allowed to receive data.[71] Also, if we look at the relationship between suppliers and an end producer, a contractual principle advocating undistorted competition could fit. Let us consider the Block Exemption Regulation in the Motor Vehicle Sector for the repair and maintenance of motor vehicles and for the supply of spare parts.[72] The treatment of data on the functioning

64 Green Paper on Unfair Trading Practices in the Business-to-Business Food and Non-Food Supply Chain in Europe, COM (2013) 37 final.

65 Ibid p 6.

66 Case C-472/10 Nemzeti Fogyasztóvédelmi Hatóság v Invitel Távközlési Zrt ("Invitel"), EU:C:2012:242, para 30; Case C-137/08 VB Pénzügyi Lízing Zrt. v Ferenc Schneider ("VB Pézügyi"), EU:C:2010:659 para 44.

67 For further details see R. Manko, "Unfair contract terms in EU law" (2013) Library of the European Parliament, ref. 130624REV1 <http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130624/LDM_BRI(2013)130624_REV1_EN.pdf> (accessed on October 15, 2018).

68 See PSD2 (supra n 30); Proposal for a Directive of the European Parliament and of the Council on unfair trading practices in business-to-business relationships in the food supply chain, COM (2018) 173; EC Press Release "Online Platforms: Commission sets new standards on transparency and fairness", April 26, 2018 (IP/18/3372).

69 See PSD2 recital 53 and article 38 (supra n 30)

70 See Access to In-Vehicle Report and Emerging Issues Report (supra n 38); Annex to the Synopsis Report (supra n 45); N. Duch-Brown et al., "The Economics of Ownership, Access and Trade in Digital Data" (2017), JRC Digital Economy Working Paper 2017-01 <https://ec.europa.eu/jrc/sites/jrcsh/files/jrc104756.pdf> (accessed on October 15, 2018).

71 See Annex to the Synopsis Report (supra n 45) p. 15-16.

72 Commission Regulation (EU) No. 461/2010 of 27 May 2010

of the vehicle between the supplier of part and the manufacturer of the vehicle is not regulated within the block exemption. Accordingly, there is the risk that the vehicle's manufacturer could implement contractual terms on data treatment concerning the parts that would place the supplier at a disadvantaged position.

64 More complicated at first glance is the last principle, namely, (to) minimize data lock-in by enabling data portability. Arguments supporting it are to be framed under two paradigms: on the one hand, the need to train artificial intelligence applications to boost innovation;[73] and on the other hand, the need to develop open, technical standards to foster interoperability (enabling data portability).[74] Both combined would ultimately improve Europe's competitiveness in the international dimension.

65 An example of a data-sharing platform that illustrates the above is the joint venture of the three German car manufacturers, Daimler, BMW and Audi. They acquired Nokia's digital map HERE[75] in 2015 as an important element of their systems for autonomous driving; in 2017, Intel bought 15% of HERE, and last April 2018, Bosch acquired 5%. There are other strategic partners such as Pioneer, Esri, DJI, NVIDIA, or Oracle and it is feasible to become a partner. The data produced by HERE are shared and simultaneously used by the partners, not only for systems of autonomous driving, but for other mobility sectors such as: transportation; logistics, publishers and advertising; improvement of cities infrastructures; and secure payment services, just to name a few.[76]

66 Other examples are Automotive Grade Linux (AGL) and Mobilityxlab, which are heading in a similar direction.[77] The former is a collaborative open source project aiming at bringing together car manufacturers, suppliers and technology companies to build a Linux-based, open software platform for automotive applications that can serve as the *de facto* industry standard. Its underlying idea is that adopting a shared platform across the industry will reduce fragmentation and allow car manufacturers and suppliers to reuse the same code base and same data-format, leading to innovation and faster time-to-market for new products. The latter, Mobilityxlab, is a coalition of leading Swedish firms that cooperate with startups to develop joint projects for solutions to the transport of the future, primarily to multiply the use of AI in the areas of electrification, connectivity and self-driving vehicles.[78]

67 Yet, discussing interoperability in the context of data portability or Art. 20 General Data Protection Regulation (GDPR)[79] still raises a number of controversial issues. On the one hand, the lack of obligations for interoperability in Art. 20 could have detrimental effects on users. For instance, the lack of interoperability and compatibility requirements could lead to a race to the "lowest common denominator" of standard datasets provided by data controllers. Adoption of universal requirements to interoperate with all other services would be expensive for companies with uncertain benefits for most users and such a burden would fall disproportionately on start-ups and SMEs, who would have to enter the market with systems in place to interoperate with all other systems already on the market.[80] Eventually, where competing services would need to have common features and functions, it would result in less variety and feature competition, also reducing consumer choice and finally reducing innovation.[81] Additionally, as a Joint Research Center's report indicates, many of the economic results supporting that a welfare-maximizing policy maker would prefer interoperable services in both traditional and platform markets, have been extracted from analyses that do not take data considerations explicitly. Therefore, more economic research is necessary to launch definitive conclusions.[82]

68 All in all, there are quite a lot of incentives for the private sector to follow, or at least to not disregard these set of guiding principles. Under these conditions, and as both scholars and industry operators have tabled over the last years in their dialogues and consultations with the Commission,

on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted Parties in the motor vehicle sector [2010] OJ L 129/52.

73 For arguments supporting that data portability would favor AI see "Data Economy Workshop Report" (2017) p. 4, available at: <https://ec.europa.eu/information_society/newsroom/image/document/2017-28/data_economy_ws_report_1A1E8516-DE2A-B8C4-54C4F7CA98621166_45938.pdf> (accessed on October 15, 2018).

74 See Section 6.2., JRC Report (supra n 40) p. 42-46.

75 See <www.here.com> (accessed on October 15, 2018).

76 Ibid.

77 See <https://www.automotivelinux.org/> and <https://www.mobilityxlab.com/en/news/artificial-intelligence-focus> (accessed on October 15, 2018).

78 Ibid.

79 Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

80 See Robin Wilton's opinion, from Internet Society during the OECD Expert Workshop on Enhanced Access to Data: Reconciling Risks and Benefits of Data Re-Use (2018) May, para 95.

81 Ibid.

82 See JRC Report (supra n 38), p. 46.

it seems the approach taken finally goes towards "(regulating) self-regulation", borrowing Prof. Dr. Hilty's pun.[83]

3. Challenges for Competition Law: The Example of a Refusal to Grant Access to Datasets

69 It is not the intention of this analysis to compare a public policy tool such as the principles contained in the Commission's communication "Towards a Common European Data Space" with a regulatory tool such as competition law. Yet, some reflections are necessary here for two reasons.

70 First, the results of the public consultation on "Building a European Data Economy" showed that a majority of stakeholders where satisfied with the effectiveness of competition law and its enforcement in addressing potentially anticompetitive behavior of companies holding or using data.[84] Yet, several respondents pointed to the difficulties that the concept of "data sharing" could pose on competition law, as well as that stakeholders believed that competition law should evolve in order to adapt to the digital economy and duly account for the reality of data-driven markets.

71 Also, some scholars have pointed out that access to data is a disputed topic under general competition law.[85] As this contribution looks at data sharing, the paper circumscribes to the example of refusal to license access to datasets. It is article 102 TFEU, which bans the misuse of a dominant position by one or more undertakings. The CJEU has ruled that this provision may be used for the granting of compulsory licenses (even) to information protected by intellectual property rights.[86]

72 Compulsory licensing for data access is a topic that has also been discussed in reference to sector specific regulations such as the PSI Directive,[87] the eCall Regulation[88] and in the field of financial services,[89] or in reference to e-platforms.[90] What all these *ex ante* sectorial regulations and proposals have in common, is that they imply an obligation either to share the data or to grant open access to the data collecting device.

73 For a unilateral refusal to license access to datasets that are found to be in violation of Art. 102, the following considerations are to be considered.

74 For starters, the definition of the relevant market plays a central role in all three areas competition law regulates. To determine abuse of a dominant position, it is important to determine whether a company has a dominant position in the first place. And to that end, the market on which it occupies that dominant position must be established. In 1997, the European Commission published a notice on the definition of relevant markets for the purposes of EU competition law.[91] Accordingly, the market definition is composed of the relevant product market and the relevant geographic market. Ever since, the Commission has continuously "commissioned" reports or launched consultations on market definition in different sectors such as the media (1997), pharmaceutical (2009), telecoms (2002), etc.[92] However, the application of competition law in general, and the definition of the relevant market in particular, are inherently case-specific. For example, while assessing merger control involves a prospective analysis, application of Art. 102 (and 101) TFEU look into past behavior.

75 Second, when looking at the current practice on refusals to deal and to license as a guide,[93] there is one difficult obstacle to overcome when considering

83 See R. Hilty, "Big Data: Ownership and Use in the Digital Age" (2018) 5, June 2018 CEIPI-ICTSD, p. 87-94. In the same line, see also M. Leistner, "Big Data and the EU Databases Directive 96/9/EC" in S. Lohsse, supra n 22, p 38.

84 See Annex to the Synopsis Report (supra n 45), p. 13.

85 B. Lundqvist "Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World – The Issue of Access" (2016) Stockholm Faculty of Law Research Papers, p. 3 <https://ssrn.com/abstract=2891484> (accessed on October 15, 2018); J. Drexl (supra n 4), para 1.

86 RTE and ITV v Commission ("Magill"), C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, [1995] ECR I-743; IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG., C-218/01, ECLI:EU:C:2004:257 [2004] ECR I-5039.

87 See PSI Directive (supra n 27).

88 Council Regulation (EU) 2015/758 of the European Parliament and of the Council of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service and amending Directive 2007/46/EC (E-call) [2015] OJ L 123/77.

89 See PSD2 Directive (supra n 30).

90 See W Maxwell and T Pénard "Regulating digital platforms in Europe – a White Paper" (2015) available at: <www.digitaleurope.org> against the French National Digital Council's (CNN) report recommending legislation targeting digital platforms, (accessed on October 15, 2018).

91 Commission Notice on the definition of relevant market for the purposes of Community competition law (97/C 372/03) [1997] OJ C 372/5.

92 The media sector is the more prolific, all the studies can be found at: <http://ec.europa.eu/competition/sectors/media/documents/index.html>; in the case of pharmaceutical industries: <http://ec.europa.eu/competition/sectors/pharmaceuticals/inquiry/index.html>; for telecommunications industries: <http://ec.europa.eu/competition/sectors/telecommunications/overview_en.html>. For studies on different sectors: <http://ec.europa.eu/competition/sectors/> (accessed on October 15, 2018).

93 For a detailed explanation see Drexl (supra n 4) p. 281-282.

datasets. Data is a non-rivalrous resource; if datasets could be substitutable, meaning the same individual data could be found in various datasets, this would count against the requirement of dominance. Thus, a refusal to deal or to license would not prosper.

76 Finally, if we consider dataset negotiations for analytics involving techniques of data mining by searching datasets for correlations necessary to improve algorithms of artificial intelligence applications, contractual agreements on access to datasets may simply fail because of asymmetries regarding the value of the datasets, not because of anti-competitive conduct.[94] This could also be the case with IoT platforms.

77 Therefore, Art. 102 may not be readily applicable to provide access to datasets per se, except when those datasets are indispensable to access an industry, or a relevant market and parties are not able to agree on price.[95]

78 All in all, in such an emerging market sector as the IoT platforms, with so many players and different niches, abuse of a dominant position and refusals to grant access to data might be very problematic to articulate.

79 Thus, relying on competition law as the only regulatory tool, might not be the smartest move. On the other hand, following the results of the consultation launched in 2017, the idea of setting the ground via recommending standard contract terms was generally preferred to the proposal of legislating laying down non-mandatory rules for B2B contracts.[96] Thus, the idea proposed by the Commission to test *ex-ante* measures in the field of contractual relations may be beneficial towards supporting fair markets for IoT products, byproducts and services.

94 This is known as the "information paradox" framed by Arrow in the context of patent law. See Kenneth J Arrow, "Economic welfare and the Allocation of Resources for Invention" in: National Bureau of Economic Research (ed.), The Rate and Direction of Inventive Activity (1962) p. 609.

95 Huawei Technologies Co. Ltd v ZTE Corp. and ZTE Deutschland GmbH, C-170/13, ECLI:EU:C:2015:477 [2015]. For a commentary on the case see C. Tapia, S. Makris, "Negotiating Licenses For FRAND-accessible Standard Essential Patents In Europe After Huawei v ZTE: Guidance from National Courts" Managing Intellectual Property, May 2018, available at: <http://www.managingip.com/Article/3804014/Negotiating-SEP-licences-in-Europe-after-Huawei-v-ZTE-guidance-from-national-courts.html> (accessed on October 15, 2018).

96 See Annex to the Synopsis Report (supra n 45) p. 20-21.

III. Business-to-Government (B2G) Principles

80 The primary reason to put forward a set of contractual principles regarding the supply of private data to public sector bodies for public interest purposes is to "support the supply (...) under preferential conditions for re-use." This goal could be rephrased as the wish to turn closed data into open data in the interest of the public (AI innovation).

81 The Commission proposes the six following principles as guidance: proportionality in the use of private sector data; purpose limitation; "do no harm"; conditions for data re-use; mitigate limitations of private sector data; and, transparency and societal participation.

82 They read as follows:[97]

a) **Proportionality in the use of private sector data:** Requests for supply of private sector data under preferential conditions for re-use should be justified by clear and demonstrable public interest. The request for private sector data should be adequate and relevant to the intended public interest purpose and be proportionate in terms of details, relevance and data protection. The cost and effort required for the supply and re-use of private sector data should be reasonable compared with the expected public benefits.

b) **Purpose limitation**: The use of private sector data should be clearly limited for one or several purposes to be specified as clearly as possible in the contractual provisions that establish the business-to-government collaboration. These may include a limitation of duration for the use of these data. The private sector company should receive specific assurances that the data obtained will not be used for unrelated administrative or judicial procedures; the strict legal and ethical provisions governing statistical confidentiality in the European Statistical System could serve as a model in this regard.

c) '**Do no harm':** Business-to-government data collaboration must ensure that legitimate interests, notably the protection of trade secrets and other commercially sensitive information, are respected. Business-to-government data collaboration should allow companies to continue being able to monetize the insights derived from the data in question with respect to other interested parties.

97 See EC COM (2018) 232 final, p. 13.

d) **Conditions for data re-use:** business-to-government data collaboration agreements should seek to be mutually beneficial while acknowledging the public interest goal by giving the public-sector body preferential treatment over other customers. This should be reflected in particular in the level of compensation agreed, the level of which could be linked to the public interest purpose pursued. Business-to-government data collaboration agreements that involve the same public authorities performing the same functions should be treated in a non-discriminatory way. Business-to-government data collaboration agreements should reduce the need for other types of data collection such as surveys. This should reduce the overall burden on citizens and companies.

e) **Mitigate limitations of private sector data:** To address the potential limitations of private sector data, including potential inherent bias, companies supplying the data should offer reasonable and proportionate support to help assess the quality of the data for the stated purposes, including through the possibility to audit or otherwise verify the data wherever appropriate. Companies should not be required to improve the quality of the data in question. Public bodies, in turn, should ensure that data coming from different sources is processed in such a way to avoid possible 'selection bias'.

f) **Transparency and societal participation:** business-to-government collaboration should be transparent about the parties to the agreement and their objectives. Public bodies' insights and best practices of business-to-government collaboration should be made publicly available as long as they do not compromise the confidentiality of the data.

1. Principles' Goal: Incentivizing B2G Data Sharing to Foster AI Innovation

83 From a business-to-government perspective, the question would be how to find a way that private companies would share and open their private datasets to public bodies to support AI development, not only for matters of public interest but for innovation.[98] In addition to that, such openness would need to be in a way that privacy of individuals is respected and guaranteed. And if this would be possible, how to set the conditions for collaborating without harming the legitimate interests of businesses, while also mitigating potential limitations of private sector data.

84 Three of the principles proposed by the Commission, namely "**do no harm**", **conditions for data re-use,** and **mitigation of limitation of private sector data**, show that there is a clear understanding that pursuing a public good is not a sufficient driver to incentivize data sharing for innovation. Businesses are profit driven. They share data typically by selling integrated analytics services, and they can provide different levels of access under different business models. From this perspective, these principles aim to create incentives for the private sector by either securing monetization, compensation, or by lowering costs:

- "Business-to-government **data collaboration should allow companies to continue** being able to **monetize** the insights derived from the data in question with respect to other interested parties."
- "Business-to-government data collaboration agreements should **seek to be mutually beneficial** while acknowledging the public interest goal (...) reflected in **particular** in the **level of compensatio**n agreed".
- "Business-to-government data collaboration agreements should **reduce the need for other types of data collection** such as surveys. This should **reduce the overall burden** on citizens and **companies**."
- "Companies supplying the data should offer reasonable and proportionate support to help assess the quality of the data for the stated purposes, (but), **should not be required to improve the quality of the data**"

85 If these principles would turn into a legislative proposal, it would be critical not to lose sight of how to develop incentive mechanisms. This would comprise an assessment on the legal, economic and technical obstacles preventing B2G data sharing, and advise on concrete actions to promote B2G data sharing for public interest purposes.

86 Beyond that, there are many questions left open, such as whether private data shared with public bodies could become open data, and if so, which and to what extent, or whether it could be re-used for official statistics. The good news is that the Directive on the Re-Use of Public Sector Information is currently under review, and some of its objectives are aligned with these proposed guiding principles. In particular, addressing the risk of excessive first-

98 The Commission also adds in their communication the goal of "the economization of public resources". Yet, the only example explaining it is: "this can also lower the burden on companies and citizens by avoiding survey questionnaires." It would be very helpful if this concept is explained in further communications.

mover advantage by requiring a more transparent process for the establishment of public-private arrangements by:

a) allowing any company to learn about the data being available, and;

b) increasing the chance of a wider range of re-users actually exploiting the data in question.[99]

87 The bad news is that we do not know how the PSI Directive would move forward, nor whether these principles would have any impact at all. In the meantime, besides giving these B2G principles an overall weak evaluation, we would need to see whether the Commission moves relatively quickly on developing this strategy.

2. Re-Use of Closed Data for Public Interest: A Win-Win Situation?

88 The famous quote by Walsh and Pollock: "the coolest thing with your data will be done by someone else" comes in handy here. Government agencies or researchers make use of private company data to address societal issues. As the Communication points out, statistical offices in some EU Member States use data from mobile telecom operators as an alternative source for official statistics, for instance on mobility or demography.[100] Nonetheless, a private telecom company such as Vodafone offers packaged services to public bodies based on the mobility data gathered by their antennas. In developing countries, they offer their data services as an alternative to poor-quality official statistics, and their main incentive lies in corporate image and the potential indirect business benefits.[101] These exact same datasets have proved an invaluable source for controlling outbreaks, surveilling and modeling of infectious diseases.[102]

89 Symmetrically, as explained previously, the re-use of (certain) public sector information by private companies is regulated by the PSI and in force since December 2003.[103] The evolving approach of this Directive is to overcome the resistance among public bodies in Member States to make public data more accessible to the private sector, obviously safeguarding the fundamental right of privacy and personal data protection of individual citizens.

90 There are other examples in the *acquis* where access to information is promoted by specific legislative means based on the nature of the information. For instance, scientific information is often controlled by academic publishers who tend to seek exclusive licenses for digital management of such information (publications), while public institutions tend to promote open-access systems. The Commission Recommendation of 17 July 2012 on access to and preservation of scientific information[104] provides a set of tools to ensure incentives so that businesses benefit as well as society and ultimately promote the use of open-access systems.

91 Yet, when considering public interest, some comments are deemed necessary.

92 First, the Commission's proportionality principle reiterates that the public interest reason for requesting data should be clearly and demonstrably justified. It shows a clear intention of an enhanced public interest reason; for example, to give an extra assurance to private companies when handing over their private data. There are examples in the European *acquis*, such as the processing of data for archiving, scientific or historical research or statistical purposes, and safeguarded by the GDPR.[105] In the field of patent law for instance, the EU Regulation on compulsory licensing of patents for the manufacture of pharmaceutical products for export to countries with public health problems outside the EU, where access to the patent information shall be given to others against a fee,[106] or in the case of law enforcement and national security.[107]

99 COM (2018) 125 final, p. 5 and footnote (19). For details on the current review of PSI2, see Proposal for a Directive of the European Parliament and of the Council of the re-use of public sector information (recast), COM (2018)/234 final – 2018/0111 (COD).

100 EC Com (2018) 125 final, p. 12.

101 D2.2 First Report on Policy Conclusions – Update of the European Data Market Study (SMART 2016/0063), p. 31.

102 See S. Bansal et al., "Big Data for Infectious Disease Surveillance and Modeling" (2016) Dec 1; 214 (Suppl. 4) J Infect Dis, p. 375–379 <https://doi.org/10.1093/infdis/jiw400> (accessed on October 15, 2018).

103 See PSI (supra n 27).

104 Commission Recommendation of 17 July 2012 on access to and preservation of scientific information, C(2012) 4890 final.

105 See Art. 89 of the General Data Protection Regulation (supra n 79).

106 See Council Regulation (EC) no 816/2006 of the European Parliament and of the Council of 17 May 2006 on compulsory licensing of patents relating to the manufacture of pharmaceutical products for export to countries with public health problems, [2006] OJ L 157/1.

107 A good example is the Mutual Legal Assistance Treaties (MLATs) which are in effect between and among countries around the world and can provide governments with the ability to access data in one jurisdiction but needed for lawful investigative purposes in another. For example, Germany signed a Mutual Legal Assistance Treaty in Criminal Matters with the United States in 2003 and a Supplementary Treaty to the Mutual Legal Assistance Treaty in Criminal Matters in 2006. Both treaties entered into force on October 18, 2009 and allow authorities in each country to request and receive information located in the other's jurisdiction (including information stored in third-party facilities

93 The question in the case of these principles comes with their legal status. If they are a non-binding instrument, how can a request to supply private data based on (enhanced or not) public interest be enforced? It looks good on paper, but there are no instruments that allow this principle to actually operate.

94 Second, can the fundamental right of privacy be overridden by public interest? And if so, how would this affect a provision of private data by a company to a public body in the context of these principles?

95 These questions arise after a ruling by the Court of Justice of the EU in 2017, related to the Universal Services Directive and telephone guides data, *Tele2 (Netherlands) and Others*.[108] European Directory Assistance (EDA) is a Belgian company offering directory enquiry services and directories accessible from the Belgian territory. EDA requested the companies which assign telephone numbers to subscribers in the Netherlands (namely, Tele2, Ziggo and Vodafone Libertel) to make available to EDA data relating to their subscribers, relying on an obligation provided for under Dutch law, which is itself the transposition of Article 25(2) of the European Universal Service Directive.[109]

96 The Court was asked whether an undertaking is required to make data relating to its subscribers available to a provider of directory enquiry services and directories established in another Member State; and whether it is necessary to leave the subscribers with the choice of whether to give their consent or not depending on the country in which the undertaking requesting that data provides its services. To the first question, the CJEU declared that the Universal Service Directive covers all requests made by an undertaking established in a Member State other than that in which the undertakings which assign telephone numbers to subscribers are established. To the second question, the Court confirmed that the passing of the same data to another undertaking intending to publish a public directory did not require the subscriber's "renewed consent".

97 It is undeniable that data held by private companies can be invaluable for addressing social issues. They are not a low hanging fruit: they require substantial investment and a degree of direct involvement for the supplier of the datasets. Thus, a mandatory data sharing measure without contemplating returns on investment could put in jeopardy the emerging data driven economy as well as the development of artificial intelligence. Each ecosystem is building its own set of business models and organizational arrangements to fit their particular system of incentives, thus for a B2G data sharing relationship to maximize, this should be the way too. And last but not least, as regards to the information contained in private data, or better said, private datasets, a distinction between which are in the public interest and which are only of commercial interest is very difficult to make. To overcome this highly challenging task, the principles proposed by the Commission try to set a framework where the supply of private datasets should be mutually beneficial and proportionately compensated to the supplier. The use of words and expressions such as "proportionality", "purpose limitation", "clear and demonstrable public interest", "do no harm", "mitigate limitations of private data", clearly suggest the Commission's goal is to build on trust while creating business incentives to foster this kind of data flow. To take into account the investment in data collection or adaptation that would be necessary before any private dataset could be supplied and used by public bodies (conversion into relevant formats, anonymization of personal data or confidential business information) while allowing companies to keep on monetizing the insights derived from the datasets provided to public bodies with respect to third parties.

98 In this scenario there is no "silver bullet" to ensure a boost of Europe's technology and the democratization of AI technology. It is a matter of setting the right

clouds). For further information see: W. Maxwell, "A Global Reality: Governmental Access to Data in the Cloud", (2012) Hogan Lovells White Paper. At the international level, the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. These were designed by the U.S. Department of Commerce, the EC and the Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. More information at: <https://www.privacyshield.gov/welcome> (accessed on October 15, 2018). For further information see also: J. V. J. van Hoboken, A. Arnbak, N.A.N.M. van Eijk, N.A.N.M., "Obscured by Clouds or How to Address Governmental Access to Cloud Data from Abroad" (2013) Privacy Law Scholars Conference <https://ssrn.com/abstract=2276103> (accessed on October 15, 2018); T. Christakis, "Lost in the Cloud? Law Enforcement Cross-Border Access to Data After the "Clarifying Lawful Overseas Use of Data" (Cloud) Act And E-Evidence" (2018) FIC Observatory <https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/> (accessed on October 15, 2018).

108 Case C-536/15 Tele2 (Netherlands) BV, Ziggo BV and Vodafone Libertel BV v Autoriteit Consument en Markt (ACM), ECLI:EU:C:2017:214 [2017].

109 Art. 25: "Operator assistance and directory enquiry services. (2). Member States shall ensure that all undertakings which assign telephone numbers to subscribers meet all reasonable requests to make available, for the purposes of the provision of publicly available directory enquiry services and directories, the relevant information in an agreed format on terms which are fair, objective, cost oriented and non-discriminatory.

policy mix of raising awareness among the market players and providing information and guidance about options, modalities and building trust to remove fears. In this sense, the set of principles as such, without any further enforcement measures and the articulation of real incentive mechanisms, would amount to a quite a naïve proposition.

E. Conclusions

99 In this digital era of sharing supply chain data, companies on the move need to develop business growth strategies with AI playing a central role to gain insights, knowledge, and ultimately innovate and be competitive. Data held by private companies can be invaluable for addressing societal issues, or for generating new products and services. Nevertheless, it is still unclear if all data or only certain datasets - since they are not real time data and have been analyzed and processed according to certain interests - are already biased. Therefore, before jumping into sharing data as a matter of principle, further research is necessary on what "raw data" means and what kind of datasets are B2B and B2G relationships in need of sharing to successfully address the above objectives.

100 The EU has been struggling for some time over the need for legal protection of data "ownership" in terms of property, even considering the creation of a new intellectual property right. These two sets of principles on private data sharing, despite of their simplicity, put on the table an important question for reflection: *should Europe move away from discussing a regulatory approach to data property and access to data, and rather focus on elaborating on the problem of how to foster data sharing and data collaboration to find better solutions?*

101 Creating economic incentive is necessary to evolve from a "one-company philanthropy" model for data sharing to an open data sharing community including competing firms. It is also critical to clarify the responsibilities and roles by governments and by private sector actors on issues such as data access, data sharing, and data quality. New legislation will just take too long to address these questions, while the amount of power data give to companies cannot be left without regulatory intervention, and just in the hands of stakeholders to be sorted out by the market. However, instead of looking towards a vertical approach, the Commission should look horizontally, as Europe has at hand considerable established rules in different fields such as competition law or intellectual property that could be applied or adapted to the new "data driven" reality. At a sectorial level, it would not hurt to look closer at the telecommunications sector, as it is already experienced in establishing formal and "quasi-formal" standards for the industry, in particular the standardization processes, standard setting and developing organizations, the use of FRAND commitments, etc. The same goes for the Open Source movement, a prototype for open innovation, as it allows independent companies to innovate in a collaborative process, where sharing is the key.

102 Moving toward a data sharing mantra is urgent in order to encourage not only further quality datasets training contributions, but to boost the development of AI-enabled technologies, and these basic principles are an approach worth considering. However, more needs to be done. Moreover, the development of instruments within the context of freedom of contract aiming at protecting the weaker party (or a third party) from unfair exploitation, needs to be taken into account. Therefore, the approach needs to include more than recommendations and models for how the parties can design their own contractual arrangements. We need a normative approach with strong regulators, in order to protect both parties' freedom of contract. But at least for now, similar to Buddhism, these principles set the right mantra for a potential AI nirvana.

Acknowledgements

This paper was initially drafted during a research stage at the Institute for Information Law (IViR), in Amsterdam. I am grateful to Bernt Hugenholtz, Niko van Ejik, Kristina Irion, Joost Poort, Steff van Gompel, Raquel Xalabarder and Claudia Tapia for all their comments and feedback.

Responsibility for Data Protection in a Networked World

On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe

by **René Mahieu, Joris van Hoboken and Hadi Asghari***

Abstract: In the current networked world, almost no system in which personal data is processed stands on its own. For example, websites and mobile applications integrate third party services for behavioral targeting, user analytics, navigation, and many other functionalities. Governments build central infrastructures to share data efficiently between different branches of government and with other organisations. This paper analyses the current system in Europe for determining who is (or better, are) responsible for observing data protection obligations in such networked service settings. In doing so we address the following problems: (1) of ambiguity in applying the concept of data controller in networked settings; and (2) of insufficiencies in the framework for establishing the extent of the responsibilities in situations of joint control. We look at how the law and regulators address these problems and how the European Court of Justice tackles these problems by applying the principle of "effective and complete protection". The issue of joint responsibility has gained particular relevance in the wake of Wirtschaftsakademie, a case recently decided by the European Court of Justice. In this case, a Facebook fan page administrator was found to be a joint-controller and therefore jointly responsible, together with Facebook, for observing data protection rules. Following this decision, there are many more situations of joint control than previously thought. As a consequence, part of the responsibility for compliance with data protection legislation and risk of enforcement measures are moved to those who integrate external services. This will change the incentive structure in such a way that joint-controllers will place a much higher value on data protection. To explore the practical implications of the legal framework, we analyse a number of examples taken from our earlier empirical work on the right of access to reflect on the newly emerging data responsibility infrastructure. We show that the coordination of responsibilities is complex in practice because many organisations do not have a clear overview of data flows, there are power imbalances between different actors, and personal data governance is often happening in separated specialised units.

Keywords: GDPR; data controller; joint-control; right of access; C-210/16 Wirtschaftsakademie; principle of "effective and complete protection"; access rights

Recommended citation: René Mahieu, Joris van Hoboken and Hadi Asghari, Responsibility for Data Protection in a Networked World: On the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe, 10 (2019) JIPITEC 84 para 1.

A. Introduction

1 European data protection law grants individuals rights in relation to their personal data, such as the right to transparency and the right to request access, correction or erasure. Legally speaking, these rights are granted in relation to the organisations that are in charge of the processing of their data, vis-à-vis the so-called data controllers. Therefore, for the system of rights to function, it should be possible to determine who counts as the data controller for the processing of personal data in specific contexts. In the end, it is the data controller who has obligations towards the data subject. And it is towards the data controller that the data subjects exercise their rights.

2 As others have noted, the legal framework for determining responsibility under European data protection law - which has its roots in the 1960s - may not function well in the current socio-technical environment.[1] Nonetheless, the core of this framework was retained as the basis of the current General Data Protection Regulation (GDPR).[2] In two recent high profile cases, *Google Spain*[3] and *Wirtschaftsakademie,*[4] national courts asked the European Court of Justice (ECJ) questions regarding how the framework of responsibility allocation should be applied. In both cases the ECJ expands the concept of data controller, arguing that these broad interpretations are in line with the principle of "effective and complete protection", a principle first introduced by the Court in *Google Spain.*[5]

3 This paper analyses the current system for determining who is (or better, are) responsible for observing data protection obligations in networked service settings.[6] In doing so we address the following problems: (1) of ambiguity in applying the concept of data controller in networked settings; and (2) of insufficiencies in the framework for establishing the extent of the responsibilities in situations of joint control. Both the Article 29 Working Party (Working Party) and the GDPR address these problems but leave many questions unanswered. The ECJ has now tackled the issues by applying the principle of "effective and complete protection".

4 In section B. of this paper, in order to answer these questions, we analyse the relevant legal provisions of the Data Protection Directive (DPD) (95/46/EC) and the GDPR, the guidance of the Working Party,[7] and the recent ECJ judgment in the case *Wirtschaftsakademie*. We find that, following the interpretation of the Court regarding the concept of data controller in this case, many more actors in networked settings could be considered data controllers than was previously considered. We conclude that under the ECJ's interpretation, any actor who has a purpose for a data processing operation, and can directly influence that processing, can be considered a data controller. Moreover, we find that, notwithstanding

* By René Mahieu, doctoral candidate at Interdisciplinary Research Group on Law Science Technology & Society (LSTS) at Vrije Universiteit Brussel (VUB), connected to the Chair 'Fundamental Rights and the Digital Transformation'; Joris van Hoboken, chair 'Fundamental Rights and Digital Transformation' at Vrije Universiteit Brussel (VUB) and Senior Researcher at the Institute for Information Law (IViR) at the University of Amsterdam. The Chair at VUB is established at the Interdisciplinary Research Group on Law Science Technology & Society (LSTS), with the support of Microsoft; Hadi Asghari, assistant professor department Technology, Policy and Management (TPM) at Delft University of Technology.

1 See for example Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1217; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

2 Regulation (EU) 2016/ 679 of the European Parliament and of the Council - of 27 April 2016 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/ 46/ EC (General Data Protection Regulation) [2016] OJ L119/1.

3 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González* [2014] EU:C:2014:317.

4 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] EU:C:2018:388.

5 A search of the CURIA database shows that the "effective and complete protection" formulation was first used in *Google Spain* and since in the judgments on *Weltimmo*, *Schrems*, *Wirtschaftsakademie* and *Jehovan todistajat.*

6 There has been academic work on the responsibility in European data protection regulation in general (e.g. Brendan Van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25.) and in specific cases such as intermediary publishers (David Erdos, 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' [2018] International Journal of Law and Information Technology 1.) such as hosting providers, search engines, blogging services and social media (Patrick Van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review 535.) on which this paper builds. However, the *Wirtschaftsakademie* judgement as well as the introduction of the GDPR merit a new look at the situation.

7 The Article 29 Working Party is an independent advisory body comprising of members from the national Data Protection Authorities, which writes opinions interpreting specific elements of data protection law. while these documents are not legally binding they do tend to have impact (Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007) , 9-10). To give an example of the influence of this opinion, see how it figures prominently in the decision of the Administrative Court of Schleswig and the opinion of Advocate General Bot on ECJ C-210/16 (2017).

the specific inclusion of a provision in the GDPR on the attribution of responsibility among joint controllers, it is still unclear what the legal consequences are in case the joint controllers do not suitably arrange their responsibility or fail to uphold the terms of the arrangement. In light of the Court's broad interpretation of the possibility of joint controllership, we conclude that these are urgent questions, that should be answered in future guidance of the European Data Protection Board (EDPB)[8] and future court decisions, such as *Fashion ID*.[9]

5 In section C., we analyse some of the practical implications of the current data responsibility infrastructure, with a focus on the right of access and transparency.[10] We do this by building on examples taken from our earlier empirical work on this topic. We show that the coordination of responsibilities is complex in practice because many organisations do not have a clear overview of data flows, there are power imbalances between different actors, and personal data governance is often happening in separated specialised units.

8 The EDPB replaced the Article 29 Working Party. It is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between the EU's data protection authorities.

9 *Fashion ID* deals with similar questions as *Wirtschaftsakadmie*, but this case is not yet decided by the Court. An opinion in this case has recently been delivered by Advocate General Bobek. See: *Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 26 January 2017 — Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV (C-40/17)* (ECJ). See B.III.2. and C.I for a further discussion of this case.

10 Previous work on the responsibility for data access rights has focused on the difficulty, from the perspective of the data subject, of determining who the data controller is. See Xavier Duncan L'Hoiry and Clive Norris, 'The Honest Data Protection Officer's Guide to Enable Citizens to Exercise Their Subject Access Rights: Lessons from a Ten-Country European Study' (2015) 5 International Data Privacy Law 190. This study on the exercise of data access rights shows how difficult it is for a data subject to find out who the data controller is and how much effort it takes to find the contact details of the data controller. Similarly, Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 4. This paper reports on the amount of time and clicks it takes to find the privacy policy of data controllers. However, in these instances it is presupposed that, with regards to the data processing taking place, it is clear from the legal point of view, who the data controller is. And the problem presented is how the data subject can find and/or reach this data controller. However, there are numerous cases in which it is ambiguous who the data controller is, or who the right data controller is for a data subject to turn to in the case of a number of different networked data processing operations.

B. Data protection responsibility in networked settings: The Law

6 In the EU,[11] the development of the legal framework for determining responsibility for data protection in networked settings comes directly from the Data Protection Directive (DPD).[12] While the GDPR recently came into force, key elements for the determination of responsibility for data protection within the GDPR are therefore a continuity. Because of this, the analysis of the commentaries on this directive, as well as opinions by the Article 29 Working Party and legal literature, are still relevant and will be included in this section.

7 This section is organised as follows. We start with an analysis of the key concepts of the responsibility framework (data controller, data processor). In section B.II, we discuss three Article 29 Working Party opinions in which it develops a more detailed interpretation of the responsibility framework. These influential opinions gave more body to the basic concepts, and also focused on the application of the framework in networked settings. In section B.III, we will discuss a case recently decided by the ECJ, *Wirtschaftsakademie*, in which the Court came to a landmark decision with regards to the reach of the concept of data controller, and the criteria for joint control. In the last section (B.IV), we will discuss the changes brought by the GDPR. Specifically, we look if the open questions that were laid bare by the Court are resolved by its additional provisions on joint control.

I. Controller and processor

8 The two central actors whose relation is governed by data protection legislation are the data subject and the data controller. In addition to these two main actors, the European data protection framework includes data processors; actors which pursue operations on behalf of others (data controllers).

11 In this paper we restrict ourselves to an analysis of the EU law. Other data protection frameworks, such as for example Canada's PIPEDA, are quite different, for example because they do not have the explicit controller-processor distinction. It would be very interesting to conduct further research in order to investigate how such different frameworks fare with regards to the complicated issues we raise in this paper.

12 The genealogy of the key legal actors (data controller, data processor, data subject) can be traced back to the 1970s (See Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 184). However, its current formulation is very close to that in the DPD to such an extent that most of the legal interpretation can be applied to the GDPR.

9 Data controllers are responsible for compliance with the obligations following from data protection law including ensuring that data subjects can exercise their data subject rights. Article 24(1) GDPR gives them the responsibility to make sure that data processing is in accordance with the regulation and the articles 12 until 23 which cover the rights of the data subject are also directed at the controller. Moreover, data controllers are liable to pay compensation in case of unlawful processing leading to damage (art. 82 GDPR).[13] "Data controller" is defined in article 4(7) GDPR as follows: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".[14]

10 Data processors are secondary actors in data protection regulation. According to article 28 GDPR, they process data on behalf of the controller, and they are not allowed to process personal data except on the instructions of the controller.[15] Article 4(8) GDPR defines "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".

11 These basic elements of the legal framework of the GDPR have been carried forward without substantial changes from the DPD, while they are difficult to apply to contemporary practices of personal data processing. The legal categories of data controller, data processor and data subject form what Tene (2013) has called a "linear model". It is a model that fits to an environment of centralised data processing with independent relationships between data subjects and data controllers, which was prevalent around the time that the DPD was written. Within this logic underlying the law, the controller is the main architect of an information system and decides the why and how of the system's operations. In building the system, the controller might use or integrate the systems and services of other organisations; but this happens under the controller's control and responsibility.[16] Several authors have noted that there are problems in applying this restricting dichotomy between data controller and data processor to the complex relationships between actors which characterise the contemporary technological and economic reality.[17] As a consequence, there are many situations in which it is unclear to what extent organisations have data protection obligations.

12 Gürses and van Hoboken (2017) have argued that recent developments in software production have major implications for data protection and privacy governance more generally. The shift from shrink-wrap software to software as a service, and the rise of the mobile internet, cloud computing and agile software development processes, have meant that the way in and the extent to which personal data is being processed across multiple actors has changed dramatically. Software is becoming more modular, meaning that most applications, websites and other software is built out of service modules of third-party software. Many of these modules are offered across organisational and sectoral boundaries and their quality and efficiency are contingent on the effective capture of personal data to function. These developments, in addition to data-driven monetisation strategies, will make it increasingly complex to apply the existing linear controller-processor model.

II. Article 29 Working Party guidance

13 The Article 29 Working Party provided guidance on how to apply the basic concepts of data protection law in its opinion *1/2010 on the concepts of "controller" and "processor"*. This was in reaction to "a lack of clarity of certain aspects of these concepts [of data controller and data processor]", and noting that "the concrete application of the concepts of data controller and data processor is becoming increasingly complex", in particular because of "the

13 Processors can also be liable but only if they did not comply with the instructions given to it by the controller (Article 82(2) GDPR). Article 23(1) DPD assigned liability for damages to data subject to the data controller.

14 This definition of data controller in the GDPR is almost identical to the formulation in the DPD where it is defined as follows in article 2(d): "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data".

15 The role of the processor is also discussed in Recital 81 GDPR. See similarly art.16 and art.17 DPD.

16 This framework can be compared to the situation where a contractor that uses subcontractors in the building of a house, keeps the final responsibility for the quality of the house, and the car manufacturer being responsible for the whole car even when much of the parts may be built by suppliers.

17 See Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007) 72; Brendan van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) 28 Computer Law & Security Review 25, 35; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179, 184.

increasing complexity of the environment".[18] The analytical framework developed in this opinion was subsequently applied in opinion 2/2010 to online behavioural advertising.[19] Both opinions touch on three key issues:

(1) Definition of controller: interprets the phrase "determines the purposes and means of processing" and introduces controller as a "functional concept"; and

(2) Joint controllership: develops a framework for determining whether two actors qualify as joint controllers; and

(3) Division of responsibility: discusses how the different responsibilities should be divided between joint controllers and to what extent they are liable.

14 We will see in the discussion of recent case law (in section B.III) that some elements of the opinions help to achieve a consistent application of data protection law as intended. However, there are also more problematic elements that have led and will likely continue to lead to considerable confusion, in particular with regards to determining who is responsible for upholding data protection obligations, as well as with regards to the extent of this responsibility.

1. Controller: determining the purposes and means

15 To clarify the concept of controller, the Working Party rephrases what it means to determine the purposes and means of processing into the one who determines the *"why"* and the *"how"* of the processing of personal data.[20]

16 About determining the *purposes,* the Working Party states: "one should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions 'why is this processing taking place? Who initiated it?'"[21] For example, a building owner that asks a security company to install cameras in order to secure their building initiates the processing of personal data; they decide why processing takes place. Therefore, they are considered the controller.[22] The security company, even if it handles some of the personal data, is considered a data processor.

17 According to the Working Party "determination of the *means* [...] includes both technical and organizational questions where the decision can be well delegated to processors (e.g. 'which hardware and software shall be used?'), and essential elements which are traditionally and inherently reserved to the determination of the controller such as 'which data shall be processed?', 'for how long shall they be processed?', 'who shall have access to them?', and so on."[23]

18 The Working Party further deliberates the extent to which an entity must determine the purposes and means to be considered a controller. The question of why the processing is happening in the first place is essential: determining this purpose(s) unequivocally leads to the qualification as controller.[24] With regards to the question of how the processing is carried out, there is more flexibility, and "it is well possible that the technical and organizational means are determined exclusively by the data processor."[25] However, an entity or person who determines the "essential means" is considered a controller.[26] So while the wording of the law seems to imply that determining both the purposes and means of processing are required to be considered a controller, the Working Party asserts that there can be situations in which a processor decides on the non-essential means and the controller decides only on purposes. Moreover, an entity that decides on essential means is also a controller. Effectively, the question of determining the purposes *and* means is transformed into determining the purposes *or* the *essential* means.[27]

19 The factual circumstances, rather than what is written in a contract, are leading to establish who is the controller. "The concept is [...] functional in the sense that it is intended to allocate responsibilities

18 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 2.

19 See Frederik J Zuiderveen Borgesius, *Improving Privacy Protection in the Area of Behavioural Targeting* (Kluwer Law International 2015) for a detailed work on data protection in the area of behavioral targeting. Borgesius does not discuss the question of responsibility distribution in networked settings.

20 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 13.

21 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 8.

22 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14.

23 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14.

24 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010),14.

25 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14.

26 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 14, 23 and 25.

27 See also Patrick van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law & Security Review 535, 539.

where the factual influence is, and thus based on a factual rather than a formal analysis."[28] In some cases, control over the purposes and means follows directly from a law—for instance when a national law determines that a government body shall process data for a public service such as social security. In other cases, it follows from an implicit competence—when the necessity of data processing follows from another legal relationship, such as an employer having to process employee data. In other cases, the non-legal facts dictate who is a controller—for instance when there is no legal provision or contract in place to determine the data controller, or there is a provision or contract, but the factual situation does not correspond with its stipulations of the contract. This understanding of controller as a "functional"[29] concept as established by the Working Party, remains relevant today, as it is being applied in court cases as well as enforcement action by Data Protection Authorities (DPAs).[30]

2. Joint controller and pluralistic control

20 The Working Party opinions further elaborate the notion of joint control, which in the DPD was captured in the words "*or jointly with others*" in the definition of controller. This limited articulation of joint control suggests that networked data processing was not a focal point of the legislator.[31] But the increasing interconnectedness of digital service offerings, as a result of cloud computing and service integration, increases the importance of a clear conceptual framework for such situations. Without a clear framework to attribute responsibility, it is unclear who is responsible for data protection obligations and to what extent, hampering the effectiveness of data protection law.[32]

21 The main guideline of the Working Party for determining if there is joint (or pluralistic) control is again to apply the functional approach.[33] Thus, joint control is not primarily determined by what the contract between the parties states, but by the factual control they yield over the purposes and means of processing.

22 Furthermore, the Working Party stresses that there can be many different constellations of joint control and it is not necessary that the different parties determine the purposes and means equally.[34] The Working Party does not give clear cut criteria to determine to what extent purposes and means have to be determined together. Instead, it develops a "typology", i.e. a collection of examples, which offer useful guidance but also raise many questions. To illustrate, in the example of behavioural advertising, the Working Party says that if publishers transfer personal information regarding their visitors to the ad network provider, they will be joint controllers.[35] The Working Party later says that when publishers trigger the transmission of personal data like the IP address or cookies—by setting up their website in such a way that the user's browser is redirected to an ad-network provider website— they have "data controller *related* responsibilities".[36] It is unclear how this concept should be interpreted and how it differs from "data controller responsibilities". And do they have responsibility because they are an independent controller, a joint-controller, or even in spite of not being a controller at all?

23 Nonetheless, the following principle can be deduced from the Working Party's opinions. Parties qualify as a joint controller when they determine together the purposes *and* means *to some extent* and *for some part of the data processing*. However, it remains unclear to what extent and to which part of the processing a party needs to be involved in order to be classified as a joint controller.

28 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 1.

29 Which means the concept defines a socio-economic reality, not a formal legal arrangement. In other words, you cannot simply make some organisation a controller or processor by stipulating it in a contract, if the actual control is not in line with the contract.

30 The continued relevance of the concept of "functional analysis" can be seen for example by its use by advocate general Bot in *Wirtschaftsakademie* paras 46, 76 and extended to determining where the location of an establishment of a data controller is located para 92 (See B.III. below). It has been used by DPAs, moreover, in deciding that an organization is a controller even when a contract says that they are a processor (Autoriteit Persoonsgegevens (2018) pp.11-12).

31 Although it was a step in the right direction as the DPD was the first data protection law that had a concept of joint control at all. See Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 17.

32 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 18; See also Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007), 71-77, indicating that the existence of these unclear situations is not a mere theoretical concern.

33 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 18.

34 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 19.

35 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 18.

36 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 23.

3. Allocating responsibility and liability for joint controllers

24 Allocating responsibility and liability in situations of joint control is one of the central goals the opinion of the Working Party on the concept of controller—"[...] the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules and how data subjects can exercise the rights in practice. In other words: to allocate responsibility."[37]

25 The guiding principle here is that relevant actors are free to distribute responsibilities as long as everything is covered. In cases of joint control, controllers should determine whom among them is responsible (competent, liable) for which of the data subjects' rights.[38] So, for example, in the case of a shared information infrastructure (pool) among banks, the Working Party states that it should be decided who answers data access requests.[39] This may be either the bank of the data subject or the organisation that operates the infrastructure.

26 For the Working Party, a data controller does not necessarily carry complete responsibility for all data protection obligations.[40] They develop two ways of assigning partial responsibility: responsibility for distinct *stages* of data processing; and different *degrees* of responsibility. In situations in which data processing takes place in different stages (or phases), actors may only be responsible for the stages they are part of. For example: " [the] responsibility of a publisher in the context of behavioral targeting, covers the first stage of the processing, i.e. the transfer of the IP address to ad network providers that takes place when individuals visit their web sites [...]."[41] In other words, the Working Party proposes differentiating between processing operations and looking at the question of responsibility more *granularly*. At the same time, it notes that publishers share responsibility for transparency towards data subjects with ad network providers (and they should help to provide information to data subjects) because they are the main interlocutor from the point of view of the data subject.[42]

27 Regarding the degrees of responsibility, the Working Party notes that different actors can be involved in the processing to different degrees, and therefore carry responsibility to different degrees.[43] We interpret this to mean that if multiple actors are involved in the same stage(s) of processing, they nonetheless may not have equal responsibility to uphold specific obligations like the fulfilment of the lawfulness requirement, transparency, or the respect for data subject rights in practice. For example, in opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), the Working Party states that SWIFT and financial institutions have a joint responsibility, although to differing degrees.[44] However, it does not offer principles to determine the degrees of responsibility. Later in the same opinion they state that SWIFT must comply with its obligations under the DPD, and member financial institutions in the EU have the legal obligation to make sure that SWIFT fully complies with the law.[45] It seems to us that if financial institutions have to make sure that SWIFT complies with the law, then in the end they have the same degree of responsibility: full responsibility.

28 The Working Party introduces the principle that parties can have partial responsibility, but it does not develop a consistent framework to determine the exact scope and limit of this partial responsibility. While the DPD and GDPR only allow for full responsibility by the controller for all aspects of data protection. This creates a situation where there is no explicit legal basis for partial responsibility, there is no legal framework to distribute such partial responsibility, and there is no coherent guidance of the Working Party. This is an additional source of legal uncertainty.

29 Another issue with the Working Party's analysis is that it presupposes that the different actors are able to work together to make sure that all relevant

37 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 4. Emphasis in the original.

38 For example: Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 22 and 24. "Parties acting jointly have a certain degree of flexibility in distributing and allocating obligations and responsibilities among them, as long as they ensure full compliance".

39 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 23.

40 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 11. "In sum, for these reasons, publishers will have some responsibility as data controllers for these actions".

41 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 18.

42 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 17-19.

43 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 1, 22 and 33; Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 2.

44 Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 2.

45 Article 29 Data Protection Working Party, 'Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (2006), 26.

obligations are met—an assumption that may not hold in practice. It does not identify what minimum responsibilities need to be upheld when cooperation is impossible, or what the consequences of not meeting the minimum responsibilities would be.

30 The last question that the Working Party discusses is how liability for compensating damages (Article 23 PDP and Article 82 GDPR) should be attributed in situations of joint-control.[46] To answer this question the Working Party introduces the concept of "joint and several liability".[47] This means that when a data subject exercises a right, such as the right of access, all joint controllers are liable in relation to the data subject in case of non-compliance—irrespective of how they had determined their obligations among themselves.[48] The controllers can still arrange a certain distribution of the cost of non-compliance, but this arrangement is between themselves and does not affect the data subject. According to the Working Party, "joint and several liability" should only be applied when the distribution of responsibilities as determined by the controllers or by the factual circumstances do not yield an unambiguous conclusion.[49] This opinion does not offer clarity on how to deal with the situation in which this is not the case.

31 As demonstrated by the changes made by the GDPR and the case law discussed further below, the opinions by the Working Party, while not having binding legal character,[50] have impacted the interpretation of the concept of controller and the corresponding allocation of responsibility and liability. But, as we will show, some of the issues identified above also lead to considerable confusion.

III. ECJ decision in Wirtschaftsakademie

32 Given the ambiguities in the law and the Working Party's guidance on the controller concept, it's not a surprise that the ECJ was asked prejudicial questions on several occasions about the determination of data protection responsibility in networked settings. Two of these cases stand out. One is *Google Spain*, decided in 2014, which deals with the responsibility as an independent controller of a search engine.[51] The second case, C-210/16 *Wirtschaftsakademie Schleswig-Holstein*, decided in 2018, deals primarily with determining the requirements for being a joint controller, and the responsibility that follows from being a joint controller.

33 The key facts of *Wirtschaftsakademie* are as follows. A private school, *Wirtschaftsakademie Schleswig-Holstein (WSW),* used Facebook for creating a so-called fan page. When users visited the fan page, a cookie was placed on their computer, but users did not receive a notification about this from Facebook or the school.[52] The Data Protection Authority of Schleswig-Holstein ordered the school to deactivate the fan page because not informing the user of the related processing of personal data breached data protection law.[53] The school contested this decision, arguing that they were not a data controller with regards to this processing.[54] The German courts agreed with the school and ruled in all instances that the school should not be considered a joint data controller.[55] The German Federal Administrative

46 We note that the concepts of responsibility and liability are sometimes used as if they are synonyms, but they are not. Responsibility is much broader concept which includes the questions: "Which actor is legally obliged to make sure all obligations of the law are met?" "Who can be legally held accountable for breaching these obligations?". Being held accountable can be either through enforcement actions by the DPA, or by the courts after an enforcement action initiated by the DPA or a data subject. Liability only refers to the obligation to pay compensation to data subjects in case they have suffered damage as a result of infringements of the law by the data controller. (i.e. Article 82 GDPR and Article 23 DPD). See for a detailed of liability under EU data protection law: Brendan Van Alsenoy, 'Liability under EU Data Protection Law' (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 271.

47 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 22.

48 The Working Party is not precise enough in its use of the term joint and several liability to unambiguously determine how they interpret it.

49 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 24.

50 Christoper Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007), 10.

51 For a detailed discussion of this case see Eleni Frantziou, 'Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761; David Erdos, 'Intermediary Publishers and European Data Protection: Delimiting the Ambit of Responsibility for Third-Party Rights through a Synthetic Interpretation of the EU Acquis' [2018] International Journal of Law and Information Technology 1.

52 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 15.

53 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388,para 16.

54 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 16.

55 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, paras 19, 21 and 23. The German national implementation of the DPD, the Bundesdatenschutzgesetz, did not have any mention of the possibility of joint control. However, from the very early stages of the procedure the DPA refers to the formulation of joint control in the DPD as well as in the Working Party's opinion on the concepts of 'controller' and 'processor'. None of the parties involved questions the existence of joint control as a legal concept;

court asked in preliminary questions to the ECJ if a party who is not a data controller, such as the school in their view, can nonetheless be held responsible for data protection infringements committed by the company they choose to do business with, in this case Facebook, in "multi-tiered information provider relationships".[56]

34 Advocate General Bot (the AG) delivered the opinion for the Court and argues, in line with the position taken by the Working Party, that the decision of who is to be considered a data controller should follow a "functional approach".[57] The AG argues in two ways that the fan page administrator should be considered a data controller. He first argues that the administrator made the choice to use Facebook for creating a fan page and solely by making this choice determined the possibility for Facebook to start data collection. This alone is enough to see them as data controller, according to the AG.[58] The AG's second argument is that a fan page administrator influences the actual processing of data by Facebook, for example by setting filters that determine to whom the fan page will be shown. This *de facto* exercise of influence over the processing constitutes participation in the purposes and means of processing, and therefore leads to the conclusion that the administrator has to be considered a (joint) controller.[59] As a supporting argument for qualifying the administrator as a controller, Bot notes that if the administrator is not a controller, for example because they cannot decide on the further contract between itself and Facebook, then it would be too easy to evade responsibility. Moreover, he argues that by assigning responsibility to less powerful economic actors in their relationship with suppliers, they will start to demand adequate data protection by such suppliers, thus creating positive ripple effects with regards to data protection compliance.[60]

35 With respect to the question of which responsibilities follow from being a joint controller, Bot refers back to the Working Party. He states that shared responsibility does not imply equal responsibility,[61] but does not discuss how this non-equal responsibility should be assigned.

36 In its judgment, the ECJ follows the AG in concluding that the premise underlying the question asked by the German court, i.e. that the administrator is not a data controller, is wrong. The administrator of a fan page, by choosing that particular service, is a data controller, according to the Court. The Court argues that the goal of the DPD is to "ensure a high level of protection of the fundamental rights and freedoms of natural persons".[62] To ensure this aim, the DPD defines the concept of data controller broadly, which in turn helps to ensure "effective and complete protection".[63] In line with these principles, the data controller does not have to be singular.[64] The ECJ adds that the fan page administrator has a role in determining both the purposes and the means of the data processing.[65] One of the purposes of the placement of cookies is to enable the fan page administrator to obtain statistics. By defining the type of statistics, the fan page administrators contribute to the processing. "[T]he administrator of a fan page [...] must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page."[66]

the question is if the concept applies to this case.

56 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 24.

57 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, paras 46 and 76. Interestingly a search of the digital archive of ECJ judgements shows the court itself does not explicitly refer to the term "functional approach" in its analysis of the concept of data controller neither in this case nor in any other.

58 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 56 "Inasmuch as he agrees to the means and purposes of the processing of personal data, as predefined by Facebook, a fan page administrator must be regarded as having participated in the determination of those means and purposes."

59 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 57.

60 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 74.

61 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 75.

62 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 26.

63 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388. The principle of "effective and complete protection" is not only used to argue for a broad definition of controller, but also for arguing for the broad scope of other concepts. In *Google Spain* for example, the same principle is invoked to decide if "processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State". In particular the Court argues that "in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words ["in the context of the activities of an establishment"] cannot be interpreted restrictively. Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 53.

64 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 29.

65 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, paras 36-39.

66 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 39.

37 With respect to answering the question regarding which responsibilities follow from being a joint controller, the Court also follows Bot and the Working Party.[67] It adds that "the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case".[68]

38 In the following subsections, we discuss two key elements of the ruling with regards to responsibility in networked settings in more depth: (1) how the concept of controller is interpreted expansively broadening the applicability of data protection law to more actors; (2) how the Court refers to a framework for allocating responsibilities which is insufficiently developed.

1. Extending the concept of controller to guarantee effective and complete protection

39 A ground-breaking aspect of the ruling is that the ECJ settles on a broad interpretation of what it means to determine the purposes and means of processing. The Court goes out of its way to argue that the fan page administrator takes part in determining the purposes and means of the processing of personal data. In doing so, the Court weighs more heavily the need to ensure effective and complete protection, than a more literal interpretation of the law's text would seem to point to.

40 The Court deviates from the conventional doctrine that only actors who determine the reasons and the ends for which data is processed are controllers. For example, in the SWIFT case, SWIFT became a joint controller because it decided, on its own, to share data with US law enforcement. Moreover, according to the *Google Spain* judgment, Google was an independent controller because it processed previously published data for its own independently determined purposes.[69] On the contrary in *Wirtschaftsakademie,* all the lower courts held that the purposes for processing personal data are set by Facebook and by Facebook alone. It is Facebook who designs the whole of Facebook's technical possibilities, and system of ends that it can be used for, such as the ability to compile statistics on users, as well as the means of doing so. The ECJ nonetheless comes to the conclusion that the fan page operator is a joint controller.

41 The crucial step the Court takes to arrive at this conclusion is that, instead of only looking at the general purposes and means of Facebook as a whole, it looks at the individual data processing operations within the system. In particular, it notes that the fan page administrator can request specific statistics to be displayed. If administrators do this, they contribute directly to a specific processing operation conducted by Facebook. Facebook's servers will start processing personal data of data subjects in a way that would not happen without the specific request of the administrator. The Court rules that because the fan page administrator has an effect on the processing, and can even initiate a particular processing operation, that it contributes to determining the purposes and means.

42 This move from what we would call a "macroscopic view" to a "microscopic view" of data processing operations, is a significant expansion of the interpretation of "determines the purposes and means", beyond how it has so far been interpreted. All German courts who had ruled on this case before had come to the opposite conclusion—ruling that the fan page administrator was not a data controller on the grounds that it decided neither the purposes nor the means.[70] And the interpretation by the German courts was argued directly based on the interpretation of determining the purposes and means as it was given by the Working Party.[71]

43 With this far reaching interpretation, the ECJ wants to do justice to the principle that EU law requires the "effective and complete protection" of the right to protection of personal data, while at the same time recognising that responsibility in the data protection legislation is primarily assigned to data controllers. This principle entered the arguments of the ECJ for the first time in the *Google Spain* case. There, it was also used to argue for the need for a wide interpretation of the concept of "data controller"

67 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 43.

68 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, para 43.

69 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González* [2014] EU:C:2014:317, paras 35-41.

70 *Wirtschaftsakademie Schleswig-Holstein* [2013] Verwaltungsgericht Schleswig VG 8 a 14/12: "Denn vorliegend fehlt es sowohl hinsichtlich der Zwecke als auch der Mittel der Verarbeitung von personenbezogenen Daten der Nutzer der Fanpage der Klägerin an einer von dieser allein oder gemeinsam mit der Beigeladenen bestehenden Entscheidungsgewalt." and Oberverwaltungsgericht Schleswig-Holstein, 04.09.2014 - 4 LB 20/13: "Insbesondere entscheidet sie [the school] nicht gemeinsam über die Zwecke und Mittel der Verarbeitung" and Bundesverwaltungsgericht, case BVerwG 1 C 28.14 [2016] para 27: "Ihre Entscheidung, für ihr Informations- und Kommunikationsangebot auch die Facebook-Infrastruktur zu nutzen, macht die Klägerin nicht zu einer Stelle, die - allein oder gemeinsam mit der Beigeladenen - über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 2 Buchst. d) RL 95/46/EG) bzw. zur verantwortlichen Stelle im Sinne des § 3 Abs. 7 BDSG".

71 Oberverwaltungsgericht Schleswig-Holstein, 04.09.2014 - 4 LB 20/13, paras 78 and 79.

in light of the purpose of the DPD.[72]

44 An important consequence of the application of this principle is that in many situations one personal data processing system will have a large variety of joint controllers. The potential consequence of applying such a wide interpretation of the wording of the law, to fit the overall principle of data protection law's effectiveness is that while it indeed helps to defend the relevant rights, it also leads to legal uncertainty.[73] That uncertainty would have been less if the Court would have stayed closer to the AG's first argument for seeing the fan page administrator as a controller. Bot argues that when a first actor (i.e. the fan page administrator) makes possible the data processing by another second actor (i.e. Facebook) *and* that first actor accepts the purposes and means of the second actor (even if the actor has no choice but to accept those as is), that actor is participating in determining the purposes and means and should therefore also be considered a data controller.

45 The AG's argument (that an entity is a data controller whenever it makes possible data processing by another actor and accepts the way that the processing is taking place) was not reproduced by the Court. This may be a missed chance for three reasons. First, the AG's interpretation of the concept of data controller is much closer to the text of the law and existing interpretation of the law, since it upholds what we have called a macroscopic view. Second, this interpretation is simpler and easier to handle in practice, more general in formulation and therefore would lead to more certainty about the interpretation of the law. Third, it would be a lower bar to meet, because it does not include the condition that the Court added—that an actor has to contribute to a specific processing operation, for example by setting filters or requesting statistics. It seems to us that this condition is of little relevance, as it seems unreasonable that if Facebook would not offer the so-called Insights function, the fan page administrator would no longer have responsibility for the data processing. An additional consequence of abandoning this condition is that it would lead to the conclusion that more actors are data controllers.[74]

46 In contrast to the extensive deliberation about purposes and means in the opinion of the Working Party, neither the AG nor the Court make any distinction between determining the purposes or determining the means. "Purposes and means" is consistently used as one noun-phrase and there is no discussion if and to what extent both elements are needed to be a controller. Influencing the processing (or agreeing to the processing and making it possible) appears to be enough to qualify as determining both the purposes and the means of that processing operation.[75]

2. Still no reliable framework to assign responsibilities

47 In its judgment, the Court does not offer any clear criteria for determining how responsibilities should be allocated between joint controllers. Within the data protection framework, data controllers are the actors who have the responsibility to ensure compliance with the data protection principles enshrined in the law. The Court rules that an actor is a data controller exactly because it opens up the possibility of assigning data protection responsibility to that actor, thereby contributing to effective and complete protection. But as we have discussed (in section B.II.4) there is no clear mechanism for allocating responsibility in cases of joint control.

48 It is a pity, therefore, that the referring court only asked whether the fan page administrator is accountable for infringements of data protection law predominantly caused by Facebook but did not ask which responsibilities would follow if this is the case. The ECJ does comment that joint control does not always imply equal responsibility: "[given that] operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case."[76] However,

72 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González* [2014] EU:C:2014:317, paras 32-34.

73 For a similar argument with respect to the invocation of the need to for effective and complete protection in the *Google Spain* case, see: Eleni Frantziou, 'Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) 14 Human Rights Law Review 761.

74 This would also fit with the Court's auxiliary argument that the responsibility of the fan page administrator is greater because through the fan page, Facebook also processes data of users who do not have a Facebook account. If this argument is central, then it should not matter if the fan page administrator contributes to any specific processing operation. See: Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388 para 41. The Working Party argues in a similar way to Bot, for the responsibility of the publishers, who by allowing for cookies on their websites trigger the processing of data by ad-networks, while visitors only intended to visit the website of the publisher in: Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 11.

75 Both the AG and the Court do mention that the administrator also has its own purpose (i.e. reasons) for using the service, but this is not presented as a necessary condition for being a controller. Moreover, it seems unlikely that there are cases where an actor uses/integrates a service without having a purpose for it.

76 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388 para 43.

the Court does not provide criteria for how these responsibilities should be allocated. Instead, they refer to the arguments made by the AG on this matter, whom in turn bases his argument on the opinion of the Working Party.[77]

49 But as we have shown in section B.II.3, the Working Party is far from clear on this point. The only clear principle for allocation of responsibility in situations of joint control formulated by the Working Party is that the actors – who are joint controllers – should have determined their respective responsibilities amongst each other. We see this principle clearly applied in a declaration by the German DPAs on the responsibilities applied to Facebook fan page operators after *Wirtschaftsakademie*.[78] Even after the decision, the DPAs do not assign any particular responsibility to operators, except for the general obligation to make an arrangement between Facebook and the operators to determine their respective responsibilities for compliance with the obligations.

50 The key legal question, however, is what happens when actors do not actively distribute the responsibilities among themselves—which remains unanswered. The only thing the Working Party has said is that, in such situation, the allocation of responsibilities should follow from the factual circumstances. If we try to apply that principle in this case, it seems reasonable to conclude that Facebook has the necessary control to be able to handle all responsibilities under data protection law, and therefore, using this criterion, Facebook should be responsible.

51 Alternatively, we can consider what the Working Party concluded in its opinion on behavioural advertising: a publisher has a role in providing information to the data subject. This was contingent, however, on the fact that in a situation of behavioural advertising, the data subject interacts with a website which is under the control of the publisher. Since in this case the way that personal data is being processed through the fan page is primarily controlled by Facebook, it would still lead to the conclusion that it is Facebook who should be responsible, as they can implement the appropriate tools and notifications.

52 However, because the Court ruled that the school is a joint controller after which the level of responsibility that each party carries for the various data protection obligations should be assessed, it seems unlikely that the Court intends an interpretation where that level of responsibility is no responsibility at all. This is the main reason the AG argues that by assigning responsibility to less powerful economic actors (in their relationship with suppliers), they will start to demand adequate data protection from their suppliers—thus creating positive ripple effects. While the Court does not repeat this argument, it effectively moves in a similar direction with its principle of effective and complete protection. The intended effect of the increased scope of (joint) data controller in *Wirtschaftsakademie* may be that by making the organisations who use services provided by other parties responsible for making sure that the services they implement live up to data protection standards, the use of non-compliant services becomes a risk. This can create a much needed incentive for actors in networked settings to demand services that do comply with data protection regulation.[79]

53 The Court does not address the fact that there is no existing framework for assigning specific responsibilities to specific "stages" and particular consequences (enforcement actions) to different "degrees of responsibility". Therefore, the reach and limits of the shared responsibility are unknown. Is the responsibility of the fan page operator only restricted to the first "stage" and only to information provision? Or does the operator share responsibility for non-compliance with regards to all data protection obligations? Can the operator be held responsible for non-compliance with regards to a data protection obligation that can clearly only be provided by Facebook, such as providing an option to opt-out of processing, as the DPA that initiated the case asserted?[80]

77 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, paras 75 and 76.

78 Datenschutzkonferenz (DSK), 'Beschluss der DSK zu Facebook Fanpages' (2018).

79 Jonathan R Mayer and John C Mitchell, 'Third-Party Web Tracking: Policy and Technology', *2012 IEEE Symposium on Security and Privacy* (2012), 416-418, note the current lack of market pressure to exercise good privacy practices and the general lack of enforcement of privacy rules, especially in the EU. And similarly, Seda Gürses & Joris van Hoboken note in particular the lack of enforcement on "curators" in Seda Gürses and Joris van Hoboken, 'Privacy after the Agile Turn' in Jules Polonetsky, Omer Tene and Evan Selinger (eds), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2017), 16.

80 See VG Schleswig, 09.10.2013 - 8 A 14/12: The DPA argues that according to the law there should be a possibility to opt out of processing. Facebook does not offer this possibility and the fan page administrator has no way to meet this obligation. Therefore, the only way to halt the non-compliant processing of personal data is by ordering the fan page operator to close the website. "Zur Begründung verwies der Beklagte darauf, dass Nutzungsdaten nach § 15 TMG (u.a. IP-Adresse, die Cookie-ID aus dem Cookie „datr", Familien- und Vorname, Geburtsname) von Nutzern, welche die Fanpage der Klägerin aufrufen, nach § 15 Abs. 3 Satz 1 TMG für Zwecke der Werbung von Facebook erhoben würden, ohne dass die Klägerin als die nach § 12 Abs. 3 TMG i.V.m. § 3 Abs. 7 BDSG für die Datenverarbeitung datenschutzrechtlich verantwortliche Stelle den Nutzer über eine Widerspruchsmöglichkeit unterrichte. Eine technische Möglichkeit zur Beachtung eines Widerspruchs

54 Advocate General Bobek proposes in his opinion in *Facebook-ID* that responsibility should be limited to the stages for which the joint-controllers share purposes and means.[81] The website-operator which integrates a Facebook like button would only have to provide information about, and collect consent for, the stages of collecting and transferring the personal data.[82] While this may respect the principle of limiting responsibility to operations which parties can meaningfully influence, we believe that this interpretation may not respect the Court's principle of effective and complete protection. Imagine a cookie notice that says: "We *collect* your IP address and Browser-ID and *transfer* this personal data to Facebook. We do not know what Facebook does with the data. Click here to accept and proceed." That would not amount to meaningful transparency in practice.

55 One potential alternative source for answering these questions is *Google Spain*, because in that case the Court also had to allocate specific responsibilities to different actors who are involved in processing the same data. In *Google Spain* the Court similarly invoked the principle of effective and complete protection to argue for an expansive interpretation of the data controller concept in the context of search engines and their processing of personal data in search results. But the analogy between the two cases is only partial because the relationship between Facebook and the fan page operator differs in essential ways from the relationship between Google and the publishers whose publications it indexes. The *Google Spain* case revolves around the analysis that Google's processing of personal data "can be distinguished from and is additional to that of the original publisher"[83] and that its "data processing [...] affects the data subject's rights additionally".[84] Because the data processing by Google was additional to that of the original processor, *and* the processing affects the data subject's rights as well, Google must be considered an independent data controller to effectuate that "the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved".[85] Google controlled in every conventional sense the purposes and means of their independent processing. On the contrary, in the *Wirtschaftsakademie* case all data protection obligations could in principle be enforced through Facebook.[86]

56 *Google Spain* nonetheless offers some insight into how partial responsibilities should be assigned. The Court held that the search engine operator has to ensure that processing meets the requirements of the law "within the framework if its responsibilities, powers and capabilities".[87] When we apply this limiting principle "within the framework of their responsibilities, powers and capabilities", developed in a situation of independent control to a situation of joint control, two interpretations are possible: each controller is responsible for what it is able to do—even without proper coordination with other joint controllers. For example, a publisher could inform data subjects about the fact that personal data processing is happening through the use of cookies.[88] Alternatively, it could mean that whenever one of the controllers is able to prevent infringement of data protection laws, they should do so, either by persuading their joint controller to commit to all data protection obligations, or by not integrating the infringing service.

57 In sum, we conclude that the existing frameworks for assigning responsibilities are inconclusive with respect to the question of how far the responsibility of the fan page administrator reaches. The framework developed by the Working Party relies on the active collaboration of joint-controllers to distribute responsibilities but does not specify what to do when this coordination does not take place. The framework derived from *Google Spain* is also unfit to be used in situations of joint control.

bestehe nicht, da Facebook hierfür keine technische Möglichkeit bereitstelle, sodass allein deshalb bereits ein Verstoß gegen § 15 Abs. 3 Satz 1 und 2 TMG vorliege." and "Da die Klägerin keine technische Möglichkeit zur Einrichtung eines Widerspruchsmechanismus habe, gleichwohl aber eine datenschutzrechtliche Verantwortlichkeit bestehe, sei die Anordnung zur Deaktivierung der Fanpage erfolgt".

81 Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, EU:C:2018:1039, Opinion of AG Bobek, para 101.

82 Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.*, EU:C:2018:1039, Opinion of AG Bobek, para 141.

83 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 35.

84 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 38.

85 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* para 38.

86 Which raises the question why the German DPA did not go after Facebook in the first place. Indeed, the German DPAs may not have the competency to initiate enforcement actions against Facebook, because that competency is given to the DPA in the county where the company has its main establishment (Ireland). An additional reason for the German regulator to go after the fan page instead of Facebook is therefore the issue of jurisdiction.

87 Case C-131/12 *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) and Maria Costeja González [2014] EU:C:2014:317,* paras 38 and 83. This criterion is also referenced by AG Bot in Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 63.

88 Although even providing information cannot be done well without proper information being provided by the other controller. We discuss this in section C.IV.

IV. GDPR

58 The case law discussed above was decided on the basis of the DPD. In this section we discuss the elements that the GDPR adds to the existing system of determining who is responsible for data protection obligations in networked settings and show these additions do not solve the uncertainties we identified above.

59 As mentioned earlier, the definition of data controller remains essentially unchanged. A new provision (Article 26) deals with the allocation of responsibilities between joint controllers. And Article 82 on liability now includes explicit clauses in Article 82(4) and Article 82(5) on liability in situations of joint control.

60 Article 26 on the allocation of responsibilities between joint controllers states the following:

> 1. Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them, unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects.
>
> 2. The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.
>
> 3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

61 Thus, with regards to the distribution of responsibilities, the main rule still is that actors are free to divide the responsibilities among themselves, as long as they make sure that all responsibilities and obligations are met. Article 26(1) adds explicitly that joint controllers should determine their respective responsibilities among each other. Yet, according to Article 26(3), data subjects can still exercise their rights in relation to each of the data controllers, irrespective of the terms of the arrangement between the joint controllers. This can be understood as follows: the agreement that joint controllers make is there to arrange the *practical* division of tasks, while both controllers remain *legally* responsible to enable the data subject to exercise their rights; and they are both liable and risk enforcement action if not.

62 With regards to liability, Article 82(4) lays out that joint controllers "each shall be held liable for the entire damage in order to ensure effective compensation of the data subject," and according to Article 82(5): "Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation *corresponding to their part of responsibility for the damage*, in accordance with the conditions set out in paragraph 2." In effect, this is the same as the joint and several liability which was already proposed by the Working Party.

63 With regards to the provision on fines, in Article 83 GDPR, which is a major addition when compared to the DPD, there are no specific rules to allocate a fine between multiple data controllers in situations of joint control.[89]

64 To conclude, the GDPR does not fill all the gaps in the existing framework for allocating responsibility among joint controllers. As a consequence, national courts will have a hard time to fill this interpretative void and it seems likely that further questions will still have to be settled by the ECJ.

V. Comments and conclusion

65 Despite introducing some provisions that explicitly deal with joint control, the GDPR does not solve the key problems identified before. While there has been a sustained critique within the academic literature on the system of allocating responsibility in the DPD,[90] the key aspects of the framework remain in place. The basic dichotomy between controller and processor remains, and while there is now a more explicit mention of joint control, there is still no system for allocating responsibilities between joint controllers. In particular, when it comes to the concept of "data controller" and the crucial question of what it means to "determine the purposes

89 Article 83(1) GDPR only postulates as a general principle that fines shall be effective, proportionate and dissuasive.

90 See for example Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 Ohio State Law Journal 1217; Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 179.

and means" of data processing, the formulation remained the same and no extra guidance in the form of recitals or additional articles is given. In light of the developments in the way that personal data is being processed, as well as the clear issues with applying the basic framework to contemporary data processing practices, further adaptation or clarification of the law is called for.

66 The direction taken by the ECJ, in favour of an expansive interpretation of the concept of "data controller" and the possibility of joint control, in order to secure the overall purpose of "effective and complete protection" of the protection of personal data, has become the legal reality. Deciding for what purposes personal data is being processed and on the means of the processing are no longer the only criteria to determine if an actor is a controller. Integrating a service which involves processing data, and having the ability to influence the processing, also leads to the qualification of controller.

67 With regards to division of responsibilities between joint controllers, the GDPR provides some clarification. In networked situations, joint controllers can decide as they like how they distribute the responsibilities among each other internally, as long as all the obligations are covered. With regards to data subject rights, the data subject should still be able to exercise their rights against each controller involved in the processing of their personal data. However, it is still not clear what happens when joint-controllers do not manage this, which is a highly relevant question in practice. The ECJ has pointed to the Working Party's opinion on the concepts of "controller" and "processor" as a source for deciding how responsibility should be distributed between joint controllers. However, we have shown that the framework for assigning responsibilities to different stages of processing and different degrees of responsibilities is underdeveloped; there are no guidelines for assigning specific responsibilities to specific "stages", no clear principles to determine different "degrees of responsibility", nor criteria to connect particular consequences (enforcement actions) to particular levels of responsibility.

68 While one of the key objectives for replacing the DPD with the GDPR was to reduce legal uncertainty,[91] our analysis shows that with regards to responsibility in networked settings, this objective is not met. The key issue it identified regarding legal uncertainty was the "divergences between the national laws implementing the Directive",[92] but the impact assessment that was part of the legislative process underlying the GDPR,[93] also identifies insufficiencies in the responsibility framework: "Although the definitions and concepts of 'controller' and 'processor' remain themselves relevant, they need to be clarified and detailed in specific provisions as regards the obligations, responsibilities and liability of both controllers and processors."[94] Considering this assessment in which the European Commission relied heavily on the Working Party's guidance, it can be considered a missed opportunity that the GDPR does not provide more clarity on the distribution of responsibilities for joint controllers.

69 The extension of the notion of "data controller" by the ECJ may have the most tangible effects in combination with the introduction of fines. The fines have the potential to change the incentive structure under which organizations operate. Article 82 GDPR states in quite general terms that "the imposition of administrative fines [...] shall in each individual case be effective, proportionate and dissuasive". Although there is no explicit system to determine how to deal with situations in which joint data controllers cannot themselves control the conditions which make a certain data processing operation non-compliant, it seems likely that such circumstances have to be taken into account when assessing the imposition of a fine. Nonetheless, the AG (and in less clear terms also the Court) have said that the fact of using an integrated third-party service instead of your internally developed service should not be a way to evade responsibility.[95] Moreover, according to the AG, it neither matters if there is economic power to influence the processing contract.[96] Given the direction that the Court has taken, it is likely that joint controllers can be fined for continuing to make use of services that do not comply with data protection laws. Whether this will cause sufficient pressure on the market for the necessary coordination to take place depends on how Data Protection Authorities and national courts will develop the direction given by the ECJ.

91 COM(2010) 609, "Communication on a comprehensive approach on personal data protection in the European Union adopted on 4 November 2010", 10.

92 COM(2010) 609, "Communication on a comprehensive approach on personal data protection in the European Union adopted on 4 November 2010", 10.

93 SEC(2012)72 final, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)"

94 SEC(2012)72 final, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", Annex II, 19.

95 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 64.

96 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 61. Following this line of reasoning we would add it should not matter if any compliant alternative is practically available.

C. Practice of data protection in networked settings

70 In this section we will reflect on some of the practical implications of the responsibility framework for organisations and data subjects who operate in a networked environment. We focus on the responsibility to provide information about the data processing to data subjects (Article 13 and 14 GDPR) and on data access requests (Article 15 GDPR). We look at what technical and organisational arrangements organisations need to have in place, to comply with data protection obligations in networked settings. We also look at structures that impede the ability to be compliant. Rather than trying to aim at a full analysis of all the implications of the emerging responsibility framework, we draw from some practical examples in order to gain insight into the challenge of ensuring data protection safeguards are observed by relevant parties.

71 We first discuss how many organisations do not supply an overview of the recipients to whom personal data is disclosed, which seems to indicate that many organisations do not have a good overview of the data flows they are involved in. Having this overview is a precondition for responsible and transparent data processing in networked settings. We then reflect on the system that needs to be in place to avoid this situation by looking at an example of an organisation that records in great detail how data is being shared. Subsequently, we will look at the use of radio-frequency identification cards (RFID cards) in a public transportation system to reflect on the implications on the systems design for data subject rights. Finally, we look at the debate about responsibility for data protection in networked settings between Google and publishers that use their AdSense network.

I. Who is data shared with?

72 When it comes to organising the technical and organisational arrangements needed for data protection in networked settings, having a clear overview of all the inter-organisational streams of personal data is an important first step. Organisations will need this basic information in order to assess for themselves if these exchanges of data with other entities are lawful. Moreover, organizations need to have this information in order to be able to inform data subjects.

73 In a study we conducted in 2017, we found that only 20% of organisations that received an access request informed data subjects about the *specific* recipients of the data.[97] This low rate of specific answers with regards to the recipients of personal data is indicative of a lack of transparency regarding networked situations. The explicit goal of the right of access, according to recital 63 of the GDPR, is that it should allow data subjects to be aware of and verify the lawfulness of the processing. But without information about who accessed the data, an important aspect of the lawfulness of processing in networked settings cannot be assessed.

74 An interesting example drawn from the above-mentioned study is Bol.com, a Dutch online retailer who did disclose with which other service providers they shared data in specific terms. In our case, data was shared with Accountor Nederland BV in order to process payments and with Docdata BV and Fiege BV for shipment. But even Bol.com did not share all the information about the transfer of data to other organisations. One missing category of recipients for instance was social media plugins and other services placing third-party cookies.

75 Most internet users are familiar with notices about cookies when visiting websites. These notifications often indicate that both first as well as third party cookies are used and provide a link to a cookie policy which explains in greater detail the types of cookies used, as well as a list of the third party advertising cookies with links to the privacy policies of those companies. More recently, options are offered to turn third party cookies off. However, in the answer to the access request, none of the organisations provided information about the personal data that had been collected by third-parties through the use of cookies.

76 The Working Party has written that ad network providers should provide access to data subjects,[98] but following *Wirtschaftsakademie,* it is clear that website owners who integrate their cookies and social plug-ins will share that responsibility in many cases. Bot discusses this situation in his opinion in *Wirtschaftsakademie* when he makes a sidestep to another case currently pending for the Court, *Fashion ID*. Like *Wirtschaftsakademie*, *Fashion ID* also deals with a company which makes use of Facebook technology, the so-called Facebook "Like" button.[99] Bot asserts

97 René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review, 10 <https://doi.org/10.14763/2018.3.927> accessed 26 February 2019.

98 Article 29 Data Protection Working Party, 'Opinion 2/2010 on Online Behavioural Advertising' (2010), 24.

99 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 67. For a discussion of how Facebook's plug-ins function through the use of cookies see Güneş Acar and others, 'Facebook Tracking Through Social Plug-Ins' (Commission for the protection of

that "Like fan page administrators, operators of websites with embedded social plugins can benefit from the 'Facebook Insights' service and obtain precise statistical information about the users of their website." [100] According to the AG, this leads to the conclusion that a website manager who includes a Facebook like button is also a controller in relation to the data being collected through the Facebook like button.[101] Since the arguments by the AG were followed by the Court, organisations would qualify as a joint controller for the processing of data through the Facebook like button.

77 The question that follows is which responsibilities the website administrator would have as a joint controller? The Court has held that each controller does not have the same responsibility. In the Working Party opinion that the Court refers to in this context, providing information could be best done by the website administrator, while Facebook should answer to access requests. A division of tasks along these lines would be in line with the main principle of Article 26 GDPR that joint controllers should distribute their respective tasks.

78 But what happens if Facebook does not provide access to the data? What happens when either of the actors does not uphold their responsibility?[102] A key aspect of Article 26(3) GDPR is that while joint controllers should distribute the responsibilities, data subjects may exercise their rights of access against each of the controllers. From this, we suggest that a data subject can also direct a request to access to the website administrator, irrespective of the fact that the personal data is collected through the use of cookies by Facebook and the administrator has no access to data. The administrator could solve this practically by redirecting the request to Facebook. However, if Facebook would not adequately comply, the organisation integrating their plugin may also be held accountable. Bobek, the AG in *Fashion ID,* on the contrary argues that that responsibility for data access rights should be restricted to Facebook alone, and also argues that Facebook and the website operator do not have to make an agreement about this.

II. Establishing a traceable data trail

79 Whilst it is hard for data subjects to trace which organisations have received data about them in many cases, it is certainly technically possible to establish a traceable data trail. However, we observe that even when a system is built in this way, there can be other aspects that impede tracing with whom personal data is shared.

80 To ensure transparency about data processing in networked settings, systems would need to be designed to enable this. In our empirical study, Dutch municipalities stood out in the level of detail they provided on the recipients of personal data.[103] The municipalities were able to provide data subjects with a detailed list of all organisations that access their data, including a complete overview of which particular data was accessed by which organisation. The municipalities were able to provide this level of transparency because they all use a central system for processing personal data, and the architecture of this system is designed in such a way that any access to and/or transfer of the data is recorded.[104] The information on specific recipients of personal data in response to an access request is supplemented by a website which contains general information about the organisations that are allowed to access the system.[105] This website also links to the underlying legal documents ("besluiten"). These legal documents under Dutch law create the legal basis for granting access for the organisations to the system and specify the conditions under which organisations can access the personal data. Moreover, the source code for the system is openly available, creating another layer of accountability.[106]

privacy 2017) Version 1.1.

100 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 70.

101 Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein,* EU:C:2018:388, Opinion of AG Bot, para 72.

102 Clive Norris and Xavier L'Hoiry, 'Exercising Citizen Rights Under Surveillance Regimes in Europe – Meta-Analysis of a Ten Country Study' in Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer International Publishing 2017), 444-446, argue that Facebook does not comply adequately with its obligation to provide access.

103 See René LP Mahieu, Hadi Asghari and Michel van Eeten, 'Collectively Exercising the Right of Access: Individual Effort, Societal Effect' (2018) 7 Internet Policy Review, 11 and 20 <https://doi.org/10.14763/2018.3.927> accessed 26 February 2019.

104 The system is called Personal Records Database (In Dutch: Basis Registratie Persoonsgegevens, BRP), the centralised governmental database of personal data in the Netherlands. On an organisational level it can be added that citizens can exercise their right of access through their current municipality of residence. Another interesting feature of the system is that the code is available open source on GitHub. English language information about the system can currently be found at: <https://www.government.nl/topics/personal-data/personal-records-database-brp>.

105 <https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/vraag-en-antwoord/wie-krijgen-mijn-persoonsgegevens-uit-brp>.

106 See press release by Dutch government (in Dutch): <https://www.rijksoverheid.nl/actueel/nieuws/2017/11/29/broncode-programmatuur-operatie-basisregistratie-personen-openbaar>. For commentary in English: <https://fsfe.org/news/2017/news-20171206-01.en.html>.

81 Even with such a system in place, a clear view of the data trail can be lost. One of the organisations listed in a reply to an access request to a municipality, sent as part of our study, was SNG, the *Foundation establishing a Network of Court Bailiffs*, which had accessed personal data in the database five years prior.[107] SNG is not itself a court bailiff, but rather an intermediary organisation set up to facilitate flows of information from central databases controlled by the municipalities, the Social Insurance Bank and employers, to the individual court bailiffs that seek access to personal data. The problem is that a person would be interested to know who the final recipient of the personal data is, and to find out why a court bailiff accessed the data. Without knowledge of the final recipient, the data subject is unable to verify the lawfulness of the processing. However, SNG was not able to answer which particular court bailiff had accessed the data through their system because they only retained these records for one year.[108] Thus, the link to the final recipient of the data was broken.

82 This form of data sharing through intermediaries, or clearing houses, is very common in networked settings,[109] because coordination of data streams can be more efficiently managed through these specialised actors. But as our example shows, this form of data sharing can also lead to a lack transparency for data subjects. When the first data controller only logs data sharing with the intermediary, and the intermediary does not retain the log of personal data being accessed through its system, data subjects are unable to know who accessed their data and their data rights are diminished. If the right of access should enable data subjects to follow who processes their personal data and verify the lawfulness of the sharing and processing of the personal data, the link should at least be traceable for as long as the last party in the chain processes the data.

83 Does the responsibility framework under European data protection law help to solve the problem? No, because under the GDPR it is still unclear if any actor would be directly accountable for solving this problem. According to SNG's privacy policy they are a data processor and the individual court bailiffs are the data controllers. According to the responsibility framework, this is indeed the case as long as the court bailiffs determine the purposes and means of all the processing by SNG. The answer depends on a functional analysis, stipulating that this depends on which party has the actual control, and that the contract is not determinative. Regardless of the answer to the question of who the controller is, the question is if the GDPR has any provision that directly assigns responsibility in such a way that this situation would not occur.[110]

III. Building privacy preserving intermediaries for shared infrastructures

84 Across many sectors, personal data is governed through centralised specialised organisations. In this subsection we ask how this organisational setup affects the effective use of the right of access. Examples of this can be found in the healthcare sector, where different healthcare providers need to have access to the medical data of patients; public transportation, where multiple public transport companies share a single payment system; and energy sectors, where multiple energy suppliers share the same grid.

85 Organisations that use this model of centralised data processing will have to coordinate how to deal with the obligations regarding data protection, including the right of access. We found that in most cases data subjects are requested to send their access requests to the organisational users of the system. The organisations that run the technical infrastructure are not data subject facing. This form of coordinating responsibility for data access requests is along the lines proposed by the Working Party,[111] as well as the demands of the GDPR.[112]

86 An example can be found in the Dutch public transportation system, which has transitioned to a centralised dedicated Smart-card travel system for its travellers, called OV-chipkaart. This is an RFID based system, similar to systems in use worldwide, that can be used on the national railways as well as on local public transport. In order to build and manage the infrastructure for a centralised digital payment system, the transportation providers set up a new organisation, Trans Link Systems BV. This organisation is owned by the participating public transport providers.

107 More information on SNG (in Dutch) can be found at: <https://www.sng.nl/>.

108 Following a change in the law, SNG now retains records of final recipients for 20 years, thus solving the issue that we found.

109 Examples include specialised data exchanges for personal data processed by the government, in the insurance industry, in the energy sector, but also add exchanges.

110 According to recital 64 of the GDPR, controllers "should not retain personal data for the sole purpose of being able to react to potential requests." The GDPR does not regulate specifically how long information on recipients of the data should be retained. But if we would apply the guiding principle of effective and complete protection, actors should be responsible for making sure there will be no gaps in the data trail.

111 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 23.

112 Article 26 GDPR.

87 One aspect of the technical specification of this system is that very precise movement patterns are being collected at a centralised level.[113] These movement patterns are always connected to an individual card. Because most travellers have a personalised card, which has their name and photo, most movement patterns are directly connected to an individual person.[114]

88 Another aspect of the system, which we found out about by sending access requests to multiple actors in this system, is that the system is built in such a way that not all transport providers have access to personal data. When a traveller has a personalised card from transport provider A, this provider A has access to the movement pattern that the traveller has with that provider, but not to the data related to transactions that traveller has with other transport providers. When that same traveller then uses the same personalised card, which is registered with provider A, to travel with another transport provider B, this provider B cannot access any travel pattern. In relation to provider B, the card functions as an anonymous card. Only the central organisation has access to all travel patterns across all transport providers. But even within the central organisation, access to some information is restricted, so that most employees of the company cannot access the location data.

89 Jacobs has argued that the way OV-Chipkaart is designed is a "privacy disaster" because of its centralised architecture.[115] In particular because a centralised system can easily be used for surveillance, while the non-digital / non-centralised system that it replaced did not have this feature.[116] Regardless of the qualification of such systems, we observe that in order to provide transparency to data subjects, clear information needs to be provided about elements of data protection by design used in such systems, in order for data subjects to understand how their personal data is being processed in these centralised systems.

90 Intermediaries play a decisive role in the data protection features of a system. Article 25 GDPR demands that organisations apply "data protection by design and by default". The main takeaway of this example is that the design of the shared infrastructure has an impact on effectuating data protection in a networked world, and the participating organisations have to critically assess their designs with regards to data subject rights and the joint-controller doctrine.

IV. Coordination between controllers with asymmetric information

91 While the responsibility framework for joint controllers depends crucially on coordination and collaboration between the parties, the reality of the market is that providers of digital services may present "take it or leave it" offers that do not leave any room for genuine coordination. An ongoing dispute between a group of trade associations that represent major news publishers[117] and Google[118] is exemplary of this situation and serves as an example to show the potentially far reaching consequences of the *Wirtschaftsakademie* ruling, as well as the legal unclarity that exists. The dispute started when Google informed publishers, by means of a blogpost, that because of the introduction of the GDPR, the terms and conditions for the use of various services, including advertisement services with respect to data protection, were going to change.[119] The publishers reacted to this with a letter, finding fault with Google's behaviour on three counts.[120] First, the fact that Google identified itself as an independent controller, second that it relied on the publishers for asking for consent for their data processing, and third for allocating liability to them.

113 Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010), 289, 293.

114 65% of cards are personalized cards according to Translink jaarverslag 2017 <https://www.translink.nl/TLS_Corporate/media/Beeldbank/Headerfoto's/Cijfers%202017/Jaarverslag-2017-Translink.pdf>.

115 Bart Jacobs, 'Architecture Is Politics: Security and Privacy Issues in Transport and Beyond' in Serge Gutwirth, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer Netherlands 2010), 289, 292.

116 This concern was not merely theoretical. In 2017 Translink was nominated for the Big Brother Award—a prize for the organisation that does most to threaten privacy—for sharing travel data with the Dutch organisation responsible for student loans (DUO) for fraud prevention without a court order.

117 The trade group consists of four major non-profit trade organisations, Digital Content Next <https://digitalcontentnext.org/membership/members/>, European Publishers Council <http://epceurope.eu/about/our-values/>, News Media Alliance and News Media Association. They represent many major digital content companies such as Associated Press, New York Times and Slate, Volkskrant and Reuters.

118 Google is the biggest player in behavioural advertising and accounts for over a third of US digital ad spending <https://www.emarketer.com/content/google-and-facebook-s-digital-dominance-fading-as-rivals-share-grows>.

119 <https://www.blog.google/products/ads/changes-to-our-ad-policies-to-comply-with-the-GDPR/>.

120 Jason Kint, 'Publisher Letter to Google Re GDPR Terms' (30 April 2018), <https://digitalcontentnext.org/wp-content/uploads/2018/04/Publisher-Letter-to-Google-re-GDPR-Terms-042918.pdf> accessed 19 July 2018.

92 The first problem that the publishers indicate is that in the terms offered by Google,[121] both Google and the users of advertisement services are identified as an "independent controller". The publishers claim that in taking this position, Google is claiming rights over data too broadly. Moreover, they believe that Google should offer an option in which Google would operate as a data processor with regards to the data. However, neither Google nor the publishers consider the possibility that they may be considered joint controllers under the GDPR. Given the interpretation of data controller as a functional concept, the terms and conditions agreed upon between Google and publishers would serve as an input, but would not exclusively determine the role an organisation would have for the GDPR.[122] Given the criteria developed by the ECJ in *Wirtschaftsakademie* to determine whether there is a situation of joint control, this may well be the case. AdSense has a reporting function that is in some ways similar to Facebook Insights. With the reporting function, AdSense users can request reports based on categories, such as country.[123] Because the cases are not exactly similar and the criteria developed by the ECJ are not very clear, the determination cannot be made with certainty, but given the prominence of the effective and complete control doctrine, it seems entirely possible that a court would rule that AdSense creates a situation of joint control with respect to some of the data processing going on.

93 The fact alone that Google offers a controller-controller agreement, in which some data protection obligations are delegated to the publisher, signals that Google and the publishers may have to be considered joint controllers. When two controllers are joint controllers they are obliged to determine in an arrangement their respective responsibilities for compliance.[124] Also when the relationship would be one between a controller and a processor, the details of the conditions under which the processor would process data for the controller have to be laid down in a contract.[125] But if two controllers are truly independent controllers, there is no reason to make a contract stipulating who is responsible for which data protection obligations (like obtaining consent). By asking the publishers to ask for consent on their behalf, Google gives - contrary to what the agreement states - another indication that there is a situation of joint control.

94 Which brings us to the second problem raised by the publishers. They argue that they cannot take on the responsibility of asking for consent for Google's processing of data as long as they do not fully know how Google processes data. They argue that: "Placing the full burden of obtaining new consent on the publisher is untenable without providing the publisher with the specific information needed to provide sufficient transparency, or to obtain the requisite specific, granular, and informed consent under the GDPR."[126] This highlights a bigger problem. Many of the data flows that are part of information systems built out of a combination of services are not transparent. The lack of transparency of many of these systems for end-users is well established,[127] but these systems are quite likely similarly opaque to business partners like the publishers. As long as business partners have no transparency regarding the way elements they integrate in their services process personal data, the processing of personal data by these elements cannot be made transparent for the individuals whose data is being processed. For that reason in itself, the use of these elements is in clear tension with the requirement of transparency under the GDPR.

95 The combination of being a joint controller, with the inability to conduct genuine coordination, the intrinsic opacity of the services offered, and the associated potential of non-compliance creates a potential for enforcement actions against companies who integrate third party digital services. The publishers raise the issue that Google's terms indemnify Google for fines that may have to be paid by Google. But as joint controllers, the publishers also run the risk of being fined directly.

121 The 'AdSense Online Terms of Service' can be found at: <https://www.google.com/adsense/new/localized-terms?gsessionid=D0KST4BDIK97GPoA8n_aSIuRkmeQG3gx> and the associated 'Google Ads Controller-Controller Data Protection Terms' can be found at: <https://privacy.google.com/businesses/controllerterms/>. It states:

> "4. Roles and Restrictions on Processing
>
> 4.1 Independent Controllers. Each party:
>
> (a) is an independent controller of Controller Personal Data under the Data Protection Legislation;
>
> (b) will individually determine the purposes and means of its processing of Controller Personal Data; and
>
> (c) will comply with the obligations applicable to it under the Data Protection Legislation with respect to the processing of Controller Personal Data".

122 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the Concepts of "Controller" and "Processor"' (2010), 18.

123 See AdSense Help: <https://support.google.com/adsense/answer/160562?hl=en> "For example, to see which devices your ad units were viewed on broken down by country, you would select the Platforms report and then add the Countries dimension".

124 Article 26 GDPR.

125 Article 28(3) GDPR.

126 Jason Kint, 'Publisher Letter to Google Re GDPR Terms' (30 April 2018), 3 <https://digitalcontentnext.org/wp-content/uploads/2018/04/Publisher-Letter-to-Google-re-GDPR-Terms-042918.pdf> accessed 19 July 2018.

127 See for example Jonathan R Mayer and John C Mitchell, 'Third-Party Web Tracking: Policy and Technology', *2012 IEEE Symposium on Security and Privacy* (2012), 413.

96 The opacity of the data processing by Google, as well as the power imbalance that characterises the "take it or leave it" agreement making, is not unique to this case. Many of the building blocks of digital services, such as payment services, user analytics, maps integration and many others, have the same characteristics. For all these situations, *Wirtschaftsakademie* opens the door to enforcement actions against those organisations that integrate the services into their offerings in case of potential violations by the integrated service offerings. But because of the absence of a clear framework of assigning responsibilities, the development of future case law will be necessary to know the scope and limits of the enforcement in such cases.

D. Conclusion

97 In the wake of *Wirtschaftsakademie,* the concept of data controller is wider than it was thought to be before. Users of platforms and organisations who use/integrate services that rely on the processing of personal data are much more likely to be considered a (joint) data controller. However, notwithstanding the specific addition of an article in the GDPR on the attribution of responsibility among joint controllers, it is unclear what the legal consequences are in case the joint controllers do not suitably arrange their responsibility or fail to uphold the terms of the arrangement. These questions will still have to be answered in future court cases. Our discussion of responsibility for access rights shows that coordination of responsibilities is complex in practice, because many organisations do not have a clear overview of data flows, because of power imbalances between different actors, and because data governance is often taking place in separated specialised units. If the principle of "effective and complete protection" that guided the Court in its interpretation of the concept of data controller will also be applied to the application of remedies in case of non-compliance, this will incentivise organisations that integrate or connect to other services to care for data protection aspects of the services they choose.

The Impact of Smart Contracts on Traditional Concepts of Contract Law

by **Maren K. Woebbeking***

Abstract: The concept of smart contracts entered the legal discourse only a few years ago, yet the subject has already given rise to remarkably different approaches. While some assume that smart contracts can be fully integrated into existing contract law, others predict that they will mark the beginning of the end of contract law. The aim of this article is to contribute to the assessment of smart contracts by examining how they can be situated within the traditional Western concept of contract law and how they differ from traditional contracts in the individual phases of a contract's life cycle. In particular, these findings show that the automated execution of the promises contained in a smart contract, specifically their technical characteristics, lead to an increased significance of the contract drafting phase compared to the execution phase. Among other aspects, smart contracts are considerably more difficult to modify than traditional contracts and they are limited by the fact that the encoding of contracts requires an increased formalization of the contractual terms. On the other hand, the technical architecture of smart contracts offers possibilities ranging from automatic self-help to the enforcement of legally unenforceable agreements. It is precisely this autonomy of smart contracts from existing contract law that finally raises the question of whether an adaptation of contract law will become necessary and what difficulties such an adaptation would face.

Keywords: Smart Contracts; self-execution of contracts; formalization of contracts; modifying smart contracts; regulation of cyberspace; code is law; contractual ambiguity

Recommended citation: Maren K. Woebbeking, The Impact of Smart Contracts on Traditional Concepts of Contract Law, 10 (2019) JIPITEC 105 para 1.

A. Introduction

1 Contracts play a central role for the ordering of liberal market relations and therefore have an irreplaceable importance for Western and other societies.[1] Accordingly, contract law is probably the most important private law institution of individual self-determination and autonomy and it evolved continuously to respond to the emergence of new contract models.[2] Today, like many other legal institutions, it faces the challenges of digitization. Next to Big Data analytics and Artificial Intelligence (AI), especially smart contracts pave the way for a new era of contracting and pose a potential challenge to the prevailing concepts of contract law.

* Doctoral candidate and research assistant of Prof. Dr. Gerald Spindler, Department of Corporate Law, Civil Law - Internet Law, Copyright and Telecommunications Law, Georg-August-University Goettingen, Germany.

1 E Allan Farnsworth, 'Comparative Contract Law' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (OUP 2016) 901; Arthur von Mehren, 'A General View on Contract', *International Encyclopedia of Comparative Law: Contract in General*, vol VII/1 (Mohr Siebeck 2008) 19ff.; Caroline Bradley, 'Private International Law-Making for the Financial Markets' (2005) 29 Fordham Int'l L.J. 127, 158f.

2 Regarding the history of the contractual concept in Europe and Germany, see Andreas Thier in HKK, § 311 Abs. 1 Rn. 4ff; on the respective development of society and contract law in the US, see Walter F Pratt, Jr., 'American contract law at the turn of the century' (1988) 39 S. C. L. Rev. 415.

2 This article deals precisely with the impact of smart contracts on German and European contract law with comparative references to American contract law. On a larger scale, it is intended to contribute to answering the question, whether predominantly nationally influenced, analogous law is ready for the challenges posed by ubiquitous and borderless digitization.

3 The remainder of the paper is structured as follows. Part B briefly describes how contracts and contract law have developed so far and why smart contracts, at least partially, represent the next step in this development. In part C, the individual phases of the life cycle of a contract are examined in order to determine how smart contracts can be accommodated within German and European contract law in particular. Finally, part D focuses on evaluating what impact smart contracts could have on the future of contract law.

B. The Development of Contract Law and the Advent of Smart Contracts

4 It has been thousands of years since the first contracts were concluded.[3] However, many of the most significant changes in the development of contracting occurred in the course of the last century.[4] Traditionally, contracts were mostly a result of a fair negotiation process between parties with equal bargaining power, i.e. parties negotiating at arm's length.[5] This changed with the standardization of contract terms which allowed mass-market contracting, both nationally and internationally. This more simplified way of contracting minimized the human involvement in the negotiation process, thereby lowering transaction costs and brought with it a change to the bargaining process.[6] Especially the rise of the information society made it necessary to adapt the contract law to these new conditions.

5 Accordingly, in the last decades one could observe the evolution of a plethora of regulations addressing standardized contracts. Be it regulations on the use of general terms and conditions or consumer protection regulations.[7] The overall aim was to restore the equal bargaining power that had been disrupted by standardization.[8] Despite the resulting large number of regulations, there is not much left regarding the principle of contractual freedom, at least in the case of consumer contracts. Looking in particular at contracts in e-commerce, it becomes clear that consumers are commonly faced with a "take-it-or-leave-it" proposition.[9]

6 Yet, only recently a new kid on the block has emerged, that could bring about a change to this current approach: smart contracts. Even though not necessarily limited to blockchains, smart contracts are usually associated with the innovation of this technology.[10] Blockchains, which are the most popular form of distributed ledger technology, have attracted a great deal of attention in recent years and, although crypto currencies have experienced setbacks due to price volatility last year,[11] the hype does not seem to cease after all.[12]

7 In a technical sense, smart contracts can be defined as computer protocols that are self-executing.[13] Relying on the abilities of blockchains, they operate autonomously, transparently, and they are basically tamper-resistant and immutable.[14] This provides the contracting parties with several significant advantages over traditional contracts: they can rely on contractual promises that are memorialized in the smart contract, i.e. the transaction protocol, to be executed without recourse to the courts and they do not need to trust in their contracting party anymore.[15] This allows them to take calculated

3 Cf., e.g. James Gordley, 'Contract in Pre-Commercial Societies and in Western History', *International Encyclopedia of Comparative Law: Contracts in General*, vol VII/1 (Mohr Siebeck 2008) 12f.

4 Richard R Orsinger, 'The Rise of Modern American Contract Law' (2015) 1 <www.orsinger.com/PDFFiles/the-Rise-of-American-Contract-Law.pdf> accessed 22 January 2019.

5 Cf. Farnsworth (n 1) 911; Alexander Savelyev, 'Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law' (2017) 26 (2) Information & Communications Technology Law 116, 120.

6 Pratt (n 2) 416f; Karl-Heinz Neumayer, 'Contracting Subject to Standard Terms and Conditions', *International Encyclopedia of Comparative Law: Contracts in General*, vol VII/2 (Mohr Siebeck 2008) 8.

7 Neumayer (n 6) 8; Farnsworth (n 1) 913ff.

8 Cf. Farnsworth (n 1) 912f; cf. Von Mehren (n 1) 64ff.

9 Farnsworth (n 1) 911; cf. Neumayer (n 6) 8.

10 Accordingly, the following explanations concentrate substantially on blockchain-based smart contracts.

11 Cf. Jamie Redman, 'Year in Review: 2018's Top Cryptocurrency Stories' (25 December 2018) <https://news.bitcoin.com/year-in-review-2018s-top-cryptocurrency-stories/> accessed 22 January 2019.

12 See, eg, CryptoNynjas, 'IOHK launches two new smart contract tools for Cardano blockchain' (11 December 2018) <www.cryptoninjas.net/2018/12/11/iohk-launches-two-new-smart-contract-tools-for-cardano-blockchain/> accessed 22 January 2019.

13 Vitalik Buterin, 'Ethereum White Paper' (2014) 1 <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> accessed 22 January 2019; for a more detailed explanation of blockchain technology, see, e.g., Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (HUP 2018) 33ff.

14 Joachim Schrey and Thomas Thalhofer, 'Rechtliche Aspekte der Blockchain' (2017) NJW 1431, 1432; Martin Heckelmann, 'Zulässigkeit und Handhabung von Smart Contracts' (2018) NJW 504, 505; De Filippi and Wright (n 13) 72.

15 Cf. Timothy C May, 'The Crypto Anarchist Manifesto' (22

risks, even in those areas in which the parties are not directly opposed to each other but which are characterized by a certain anonymity and risk-laden enforcement, as is usually the case in e-commerce and international contracts. Consumers in particular could benefit from these advantages since they usually do not enforce their rights.[16] Moreover, smart contracts open up the possibility of reducing transaction costs.[17] In general, they mean a further minimization of human intervention and further formalization of contracts.[18]

8 However, formalization involves a certain limitation as to what smart contracts can contain.[19] After all, encoding contracts also entails certain security vulnerabilities, such as the risk that the code is incorrect. For these and other reasons, smart contracts and blockchains are still a very controversial topic.

9 The fields of application of smart contracts are numerous. They can be used, at least in theory, wherever economic assets show interfaces to the internet and certain events can be verified digitally.[20] Thanks to the increasing interconnectedness of things (or the so-called "Internet of Things"),[21] this affects more and more areas. In addition to the financial and insurance sectors, which have been particularly present up to now,[22] smart contracts are suitable for use in areas such as Sharing Economy, Energy, Supply Chain or Identity Control.[23] Naturally, contracts that deal with access to digital content, and are therefore easily translatable into software, are predestined for smart contracts. A noteworthy example is the distribution of music via blockchain-based smart contracts.[24]

10 In a nutshell, with smart contracts the drafting stage of the contract ex ante, leading to an automatic execution, will become more important than subsequent law enforcement ex post. Whether the development of this new contract concept requires a modification of the applicable contract law is a different question. The answer to that depends mainly on how this new way of contracting is accommodated by existing legal provisions.

C. The Life Cycle of a (Smart) Contract

11 The characteristics of a smart contract affect different phases of the contractual life cycle. In the following, the phases that require a special legal evaluation with regard to smart contracts are to be identified decisively. The focus will be on German and European law.

I. The Legal Nature of Smart Contracts

12 Although the term "smart contract" originates from the nineties[25] and a real hype about smart contracts can be observed for some years now, no unanimous definition of the term exists to this day.[26] Especially defining their legal character has indeed proven to be one of the most controversial issues in connection with smart contracts. While some make a distinction between smart contracts, smart contract code and smart legal contracts,[27] others even stress that smart contracts are independent of the law.[28] As computer scientists and economists have shown on several occasions, it is quite possible to actually talk about smart contracts without even considering their

November 1992) <www.activism.net/cypherpunk/crypto-anarchy.html> accessed 22 January 2019.

16 Martin Fries, 'Smart Contracts: Brauchen schlaue Verträge noch Anwälte?' (2018) Anwaltsblatt 86, 88.

17 See, e.g., Goldman Sachs, 'Blockchain: Putting Theory into Practice' (24 May 2016) passim <https://de.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1> accessed 22 January 2019.

18 Cf Savelyev (n 5) 120f.

19 Cardozo Blockchain Project, 'Research Report #2: „Smart Contracts" & Legal Enforceability' (2018) 8f <https://cardozo.yu.edu/sites/default/files/Smart%20Contracts%20Report%20%232_0.pdf> accessed 22 January 201.

20 Cf., e.g., Florian Glatz in Stephan Breidenbach and Florian Glatz, *Rechtshandbuch Legal Tech* (C.H. Beck 2018) 111ff.

21 See, e.g., Christiane Wendehorst, 'Consumer Contracts and the Internet of Things' in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Nomos 2016) 189ff.

22 Several examples in Wolfgang Prinz and Alex T. Schulte (eds), 'Blockchain und Smart Contracts: Technologien, Forschungsfragen und Anwendungen' (2017) Fraunhofer-Gesellschaft, 27ff <www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Fraunhofer-Positionspapier_Blockchain-und-Smart-Contracts.pdf?_=1516641660> accessed 22 January 2019.

23 Cf. Florian Glatz, 'Blockchain – Bitcoin – Smart Contracs – Anwendungsmöglichkeiten' in Walter Blocher, Dirk Heckmann and Herbert Zech (eds), *DGRI Jahrbuch 2016* (Otto Schmidt 2016) 83 with further references.

24 See, e.g., Ujo Music <https://ujomusic.com> accessed 17 November 2019.

25 Nick Szabo, 'Smart Contracts: Building Blocks for Digital Markets' (1996), <www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> accessed 22 January 2019.

26 Cf., e.g., the different definitions used in recent American legislation presented by Cardozo Blockchain Project (n 19) 23f.

27 Stéphane Blemus, 'Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide' (2017) Corporate Finance and Capital Markets Law Review, 13; cf ISDA and Linklaters, 'Whitepaper on Smart Contracts and Distributed Ledger - A Legal Perspective' (2017) 4ff.

28 Cf., e.g., Glatz (n 20) 115.

legal nature in the slightest. This may already be due to the fact that smart contracts, although they include the wording "contract", are not necessarily seen as a legal issue, at least with regard to the blockchain.[29] One may agree with that as far as smart contracts in a technical sense are concerned, they actually show no legal relevance. The description of smart contracts as "account holding objects" on the website of the important Ethereum Blockchain illustrates that smart contracts do indeed not always have to be contracts in a legal sense.[30] In this regard, Ethereum's founder's recent finding, that a more technical term would have been more appropriate,[31] is indeed plausible. In any event, however, smart contracts do not operate in a legal vacuum.[32] As soon as legally relevant acts are concerned, laws are generally applicable.

13 Ultimately, in these cases the term could be understood in the way Nick Szabo originally coined it: smart contracts are "a set of promises, specified in digital form, including protocols within which the parties perform on these promises".[33] He emphasized the increased functionality of smart contracts compared to non-coded contracts and consequently did not assume a detachment from the law. In light of this, a smart contract is nothing more than the encoding or digital memorialization of a contract or parts thereof.[34] Its legal evaluation depends on the law applying to the underlying contract.[35] Naturally, the conclusion of a contract and its digital representation in a smart contract can coincide.[36] Nevertheless, it can be assumed that most smart contracts will probably be contextualized in an additional written or electronic agreement in natural language.[37]

29 See, e.g., MONAX, 'Smart Contracts' <https://monax.io/learn/smart_contracts/> accessed 22 January 2019 ("To begin with, smart contracts are neither particularly smart nor are they, strictly speaking, contracts.").

30 <www.ethereum.org/greeter> accessed 22 January 2019.

31 Vitalik Buterin (13 October 2018) <https://twitter.com/vitalikbuterin/status/1051160932699770882?s=12> accessed 22 January 2019.

32 De Filippi and Wright (n 13) 78.

33 Szabo (n 25).

34 De Filippi and Wright (n 13) 79; see also Dimitrios Linardatos, 'Smart Contracts – einige klarstellende Bemerkungen' (2018) K&R 85, 87.

35 Markus Kaulartz and Jörn Heckmann, 'Smart Contracts – Anwendungen der Blockchain-Technologie' (2016) CR 618, 622; Gerald Spindler and Maren K Woebbeking, 'Smart Contracts und Verbraucherschutz' in Tom Hinrich Braegelmann and Markus Kaulartz (eds), *Rechtshandbuch Smart Contracts* (C.H. Beck 2019) (forthcoming).

36 Cf. Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1 Geo. L. Tech. Rev. 305, 322; see also Linardatos (n 34) 89.

37 Cf. Cardozo Blockchain Project (n 19) 4f; cf ISDA and Linklaters (n 27) 13.

II. Formation

1. Applicable Law

14 As they encode traditional contracts, the law applicable to smart contracts is determined according to general principles.[38] This means that the question of whether a legal contract was concluded depends on the applicable legal provisions, which may, for example, require certain formalities.[39] This could lead to a diverging assessment of smart contracts in different jurisdictions.

15 In the European Union, the applicable law includes not only respective national contract law but is also strongly influenced by European law. There are two important legal measures with respect to contract law at the European level.[40] Namely, the Directive 2000/31/EC on e-commerce and the Consumer Rights Directive 2011/83/EU. If it were to enter into force, the current proposal for a directive on certain aspects concerning contracts for the supply of digital content would complement them.[41] Some of the provisions of these measures focus on the formation of a contract on the internet. For example, they establish pre-contractual obligations for a trader in e-commerce consumer contracts to inform the consumer about relevant facts, which could be interpreted as also containing certain information about security vulnerabilities of smart contracts.[42] Although the General Data Protection Regulation (GDPR) is not contract law, it should not be ignored. Some of the provisions in it may prove problematic for smart contracts if they are based on a public, permissionless blockchain characterized by immutability and transparency.[43]

16 Yet, apart from the applicable law and seen from a factual point of view, smart contracts also offer the possibility of enforcing certain agreements

38 This can lead to difficulties, especially with international smart contracts, see e.g. Alexander Djazayeri, 'Rechtliche Herausforderungen durch Smart Contracts' (2016) jurisPR-BKR Anm. 1 4; Gerald Spindler, 'Kurzgutachten „Regulierung durch Technik' (2016) SVRV 4.

39 Philipp Reusch and Niklas M. Weidner, *Future Law: Blockchain, Industrie 4.0, Internet of Things, Robotik* (Fachmedien Recht und Wirtschaft 2018) 109ff; Martin Heckelmann (n 14) 506f; cf., e.g., the requirements established by the "statute of frauds", Cardozo Blockchain Project (n 19) 9 with further references.

40 Regarding the US, see Cardozo Blockchain Project (n 19) 9; cf. also De Filippi and Wright (n 13) 79f.

41 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, Brussels, 9.12.2015 COM(2015) 634 final.

42 Spindler and Woebbeking (n 35).

43 See, e.g., Schrey and Thalhofer (n 14) 1434ff.

which cannot be enforced in courts.[44] For instance, in order to be fully enforced in the US, a contract must generally contain consideration.[45] A smart contract can, however, enforce an agreement without consideration.

2. Contractual Terms

17 Smart contracts will formalize contracts more than is the case with traditional contracts.[46] This is simply for the reason that code cannot be as ambiguous as written text. One can certainly assume that smart contracts, more generally code, encounter difficulties with the implementation of ambiguous clauses and principles such as good faith in continental law or equity in common law.[47]

18 In the foreseeable future, if there is a need to use ambiguous clauses in a smart contract, it is likely that interpretational difficulties will be resolved by assigning them to a human-based oracle.[48] This assignment to a human-based oracle naturally also means to rely on a centralized intermediary. Yet, this can still be seen as an improvement in comparison to traditional contracts, as the infrastructure requirements are at least reduced,[49] but there is still considerable reason to believe that in the foreseeable future, smart contracts will mainly be used for unequivocal cases, encoding those parts of an underlying contract that can be clearly defined.[50]

19 Apart from the rather obvious fact, that encoded contracts will be more formalized than traditional contracts, the question whether they will also be more standardized requires considerably more complex consideration. Although it may seem obvious at first glance that commercial smart contracts used for mass contracts will lead to even greater standardization,[51] this approach may be too short-sighted. As already mentioned, smart contracts are only one of many digital innovations that will have a great impact on society and revolutionize the law. Especially during the contract drafting phase, companies as well as consumers will increasingly rely on technical support, such as data mining and scoring techniques, to assist in finding suitable contractual offers.[52]

20 Electronic agents, sometimes referred to as AI agents or digital agents, might actually be the crucial factor to individualize and personalize contracts again. Depending on their autonomy they may conclude a contract on behalf of their principal by accepting an offer or generating a counter-offer.[53] The possibilities offered by smart contracts in combination with electronic agents, i.e. AI, could therefore offer consumers great opportunities in terms of more individual contract design, but they are also accompanied by new risks for consumer protection.[54]

3. Interpretation

21 Interpreting contractual terms has in the past been the subject of a large number of court decisions and corresponding legislation.[55] This was mainly due to the fact that natural language is by definition ambiguous. In fact, ambiguity allows for a more concise version of contracts, as not all eventualities need to be differentiated (the same is incidentally true for legal provisions).[56] Ambiguity ensures a reduction of transaction costs in the context of contract drafting and therefore makes economic sense. Nevertheless, ambiguity always leaves room for interpretation and the associated risks. This resulted in the use of general terms and conditions for mass contracts, which provided an interpretation standard for court decisions and thus minimized conflicts over terms and made risks calculable.[57]

44 A great concern in that regard is given to the possibility of enforcing illegal agreements through smart contracts, see, e.g., De Filippi and Wright (n 13) 87ff with further references.

45 Raskin (n 36) 322; for a detailed illustration see Val D. Ricks, 'In Defense of Mutuality of Obligation: Why "Both Should Be Bound, or Neither"', (1999) 78 Neb Law Rev 491, 494; see also Restatement (Second) of Contracts §§ 71ff.

46 De Filippi and Wright (n 13) 84; cf Savelyev (n 5) 120f.

47 Cf. De Filippi and Wright (n 13) 77.

48 Cardozo Blockchain Project (n 19) 6; Oracles can in general be described as agents that find and verify certain real events and transmit this information to the blockchain.

49 Buterin (n 13) 21.

50 De Filippi and Wright (n 13) 195f.

51 Cf. De Filippi and Wright (n 13) 86.

52 See, e.g. Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things' in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Nomos 2016) 138ff; cf. Michal S. Gal and Niva Elkin-Koren, 'Algorithmic Consumers' (2017) 30 2 Harv. J.L. & Tech. 309, 313f.

53 Stefan Grundmann and Philipp Hacker, 'Digital Technology as a Challenge to European Contract Law' (2017) 13 (3) ERCL 255, 283; see also the „Paid-Option Regime" suggested by Ryan Calo, 'Digital Market Manipulation' (2014) 82 No 4 Georg Washington Law Review 995, 1047f.

54 Cf., e.g., Eliza Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8 (1) passim, Law, Innovation and Technology <https://ink.library.smu.edu.sg/sol_research/1736/> accessed 22 January 2019.

55 See, e.g., Armbrüster in Erman, BGB, 15. Aufl. 2017, § 157 BGB with extensive references to German court decisions; see also E Allan Farnsworth, '"Meaning" in the Law of Contracts' (1967) 76 5 Yale L.J. 939.

56 De Filippi and Wright (n 13) 77, 199.

57 Cf. Neumayer (6) 8; Farnsworth (n 1) 911.

22 Similar or maybe even further effects could be achieved by formalizing contracts, as it would be the case with the computer code used for smart contracts.[58] Yet, interpreting a programming language is likely to cause difficulties for courts. In such cases, recourse to competent extrajudicial dispute resolution is certainly an appropriate option. Particularly precarious, however, remains the interaction between the interpretation of the smart contract code and a respective underlying written contract. Extrajudicial dispute resolution can only provide a limited redress in this respect. Rather, it will be crucial that the parties stipulate explicitly to what extent the smart contract code should serve for interpretation. Such an agreement would, for instance, probably have evidential value before German courts.[59] It remains to be seen how courts will interpret smart contracts, which have no explicit agreement to that effect.

4. Modification

23 By design, a blockchain-based immutable smart contract cannot be adjusted in the same way as a traditional contract. Usually, once put in motion the encoded promises will be executed without any possibility of exerting influence.[60] Nevertheless, there are possibilities to modify smart contracts. A rather impractical solution might be for the parties to agree to reverse the smart contract afterwards. They'll be considerably better served if they conclude a dynamic contract from the outset. This would mean, that the parties plan for certain possibilities for modification or adaptation to external circumstances by including oracles. These oracles can then adjust and update certain contractual obligations.[61] The possibilities for oracles are manifold and can range from human-based oracles to certain digitally verifiable events, such as current stock prices, to an AI algorithm.[62]

III. Performance and Self-Help

24 With smart contracts, sections of or even all contractual obligations can be performed automatically the moment a certain digitally verifiable event occurs. The triggers of certain performances defined in the smart contract can be of a different nature and depend on the individual case.

25 In principle, the parties to a smart contract benefit from this autonomous automation and no longer have to monitor performance obligations to the same extent as is the case with traditional contracts.[63] The automated performance also gains importance whenever a smart contract memorializes obligations that cannot be enforced by resorting to a court. In Germany, for example, claims arising from games and bets are usually not enforceable.[64]

26 These benefits attributed to the autonomy of blockchains and the difficulties with changing or terminating smart contracts, can nevertheless become rather problematic if the performed contract provision violates the law.[65] A difficult topic to assess here is that some automation could turn out to be forbidden self-help. A prominent example is that of a starter interrupter which automatically prevents a leased car from starting if the debtor is in default. Some states in the U.S. already confirmed the legality of such devices.[66] Corresponding self-help measures in other smart contracts would certainly have to provide for various exceptions in order to be able to assess the corresponding individual case in such a way that the contract complies with the law.[67] An example could be rental agreements, where the door to an apartment could be locked automatically by the landlord if certain events occur. This is a sensitive topic, especially considering the fact that automated self-help will often be of importance in consumer contracts and thus consumer protection laws apply.

IV. Restitution

27 Apart from contractual amendments that both parties wish to make, there are cases in which the law prescribes a contractual adjustment. In particular, if the contract on which the smart contract is based is terminated, the effects of the smart contracts might need to be reverted.

58 Raskin (n 36) 324; De Filippi and Wright (n 13) 195 with further references; cf. Savelyev (n 5) 125.

59 Cf. Fries (n 16) 89.

60 Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67 Duke Law Journal 313, 340.

61 Cardozo Blockchain Project (n 19) 6.

62 Grundmann and Hacker (n 53) 284; Vitalik Buterin, 'Ethereum and Oracles' (*Ethereum Blog* 22 July 2014) <https://blog.ethereum.org/2014/07/22/ethereum-and-oracles/> accessed 22 January 2019.

63 Cardozo Blockchain Project (n 19) 5; De Filippi and Wright (n 13) 80f.

64 § 762 German Civil Code.

65 Grundmann and Hacker (n 53) 281; De Filippi and Wright (n 13).

66 Reviewed in detail by Raskin (n 36) 330f with further references.

67 Regarding starter interrupters, see Eric L. Johnson and Corinne Kirkendall, 'GPS & Payment Assurance Technology: Are You Compliant?' (*Passtime*, 14 January 2016) <https://passtimegps.com/starter-interrupt-and-gps-devices-best-practices/> accessed 22 January 2019.

28 A striking example of this can be found in the right of withdrawal in European law, which is granted to consumers when concluding a particular type of contract, for example in e-commerce.[68] The obligation to return a performance received in case of the contract being withdrawn does not entail any special legal aspects for a smart contract. However, given that public, permissionless blockchains as the basis for the smart contract bring with it the characteristic that the transaction is basically immutable, particular attention must be paid to the technical implementation.

29 Generally, one can revert to a former state of a blockchain by using so-called reverse transactions.[69] However, this does not lead to the deletion of the transaction history and the withdrawn transaction remains permanently documented in the blockchain. From a contract law point of view, this is unproblematic, but problems may arise in data protection law.[70] Additionally, the execution of a reverse transaction can cause difficulties as it can only be triggered by the owner of the private key.[71] Yet, it is hardly conceivable that a fork is used instead.[72] However, it is quite imaginable that, at least with regard to the right of withdrawal, the transaction will initially take place off-chain and will only be integrated into the blockchain after expiry of the withdrawal period.[73] The same would apply to other legal reasons making it necessary to revert a smart contract.

V. Dispute Resolution

30 Due to their characteristics, smart contracts can contribute to conflict avoidance. However, a conflict cannot be prevented in all cases. Parties having a dispute over a contract can resort to a court system for enforcement. This principally also applies if the contract was encoded in a smart contract. Nevertheless, resorting to a court is often expensive and time-consuming. Accordingly, the number of extrajudicial resolution options has grown enormously.[74] Both private and alternative dispute resolution proceedings, online dispute resolution, and arbitration proceedings could potentially be integrated into smart contracts.[75] In addition, legal tech applications, mostly used for simple cases, such as compensation for flight delays, have been increasing in importance for some time.[76] The development of AI in this area will open up unprecedented possibilities for smart dispute resolution in the future.

D. Quo Vadis Contract Law

31 Smart contracts are probably not "the mature end of the evolution of electronic agreements",[77] notwithstanding, they represent a new era of contracting. As seen above, the existing contract law can stand up to some of the challenges posed by smart contracts. Apart from the parts where smart contracts and contract law intersect, there are characteristics of smart contracts that are not covered by existing contract law, while at the same time there are legal provisions whose requirements may be difficult to meet by smart contracts.

32 In this regard, a further adaptation of smart contracts to existing provisions is certainly conceivable, but at any rate limited by technical features. An adjustment of the law to smart contracts, on the other hand, is likely to be more feasible and seems more appropriate.

33 One of the reasons for this is that smart contracts, as outlined, will place the legal protection ex ante before the legal protection ex post. Western contract laws, however, are based on the opposite premise.[78] This increasing importance of the drafting stage of a contract should be reflected accordingly by the law. Additionally, smart contracts pose risks such as

68 Art. 9 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights.

69 Schrey and Thalhofer (n 14) 1435f; David Saive, 'Rückabwicklung von Blockchain-Transaktionen' (2018) RdTW 85, 88.

70 See n 43.

71 Under German law, the enforcement of such an act is governed by § 888 code of civil procedure (ZPO) which is regulating actions that may not be taken by others, cf. Merih E Kütük and Christoph Sorge, 'Bitcoin im deutschen Vollstreckungsrecht' (2014) MMR 643, 644.

72 A fork can be described as a way of using hash power to change the rules of the software, cf., e.g., 'Amy Castor, A Short Guide to Bitcoin Forks' (*CoinDesk,* 27 May 2017) <www.coindesk.com/short-guide-bitcoin-forks-explained> accessed 22 January 2019.

73 Cf. Raskin (n 36) 326f.

74 See, e.g., the example of private arbitration used in Ursula Stein, *Lex Mercatoria – Realität und Theorie* (Vittorio Klostermann 1995) 35ff with further references; cf. Martin Fries, 'PayPal Law und Legal Tech - Was macht die Digitalisierung mit dem Privatrecht?' (2016) NJW 2860, 2861.

75 Cf., e.g., Michael del Castillo, 'Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration With DAO Proposal' (*CoinDesk,* 26 May 2016) <www.coindesk.com/damned-dao-andreas-antonopoulos-third-key> accessed 22 January 2019; see further Pietro Ortolani, 'Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin', (2016) 36 3 Oxford Journal of Legal Studies 595.

76 See, e.g., the overview of legal tech solutions in Germany on <https://tobschall.de/legaltech/> accessed 22 January 2019.

77 Werbach and Cornell (n 60) 105.

78 See, e.g., Samuel Issacharoff, 'Regulating after the Fact', (2007) 56 DePaul L. Rev. 375, 377ff with further references.

security vulnerabilities, which are also not entirely covered by existing legislation. An unmanageable amount of pre-contractual information, which is largely guaranteed to consumers by European law, for example, only serves its purpose to a limited extent. Especially in light of the fact that most consumers do not even read this information.[79] A more progressive option could be a mandatory code testing tool that checks the smart contract for security vulnerabilities.[80]

34 However, while such adaptations are mostly compatible with existing concepts of contract law, other aspects of smart contracts might not only challenge the existing contract law, but rather the concept of contract law as such. As the possibility to enforce legally unenforceable agreements through smart contracts shows, the technical possibilities of smart contracts can constitute a trusted third party. Even beyond legally unenforceable agreements, the self-execution of smart contracts will contribute to establishing them as a private regulatory framework.[81] As Thomas Hobbes pointed out already in 1651, one of the essential roles of law is to provide a system that allows the parties to have trust in receiving their performance under a binding agreement.[82] In some areas this role could be taken over by smart contracts in the future. In this respect, they are in line with the general increase in private legal rules and institutions which lead to a gradual loss of significance of state law.[83]

35 Additionally, smart contracts are not limited to national borders but are rather particularly well suited for international contracts and will in some way be ubiquitous. Just like many other digital achievements, they will mainly be influenced by their technical architecture and the individual actors who promote their use,[84] e.g. by providing smart contract templates. A parallel can be drawn, for example, to e-commerce, which is largely dominated by platforms.[85] The controversy behind the frequently quoted term "code is law", introduced by Lawrence Lessig, in fact gets to the heart of this matter.[86] In order to maintain legal values that are usually not provided by the market, i.e. by code, such as the protection of minorities and representation of public interests,[87] the concept of contract law will have to reinvent itself in parts.[88] This might include having different conceptual regimes for traditional contracts and encoded contracts.[89] As a symptomatic example of internet regulation,[90] the regulation of smart contracts will be an exceptionally difficult task.

79 See Ian Ayres and Alan Schwartz, 'The No-Reading Problem in Consumer Contract Law' (2014) 66 Stanford Law Review 545.

80 Spindler and Woebbeking (n 35).

81 This aspect of smart contracts has been described by several legal scholars using different terminological terms, cf., e.g., De Filippi and Wright (n 13) 5f, 194; see also Blemus (n 27) 14 with further references.

82 Thomas Hobbes, *Leviathan* (first published 1651, Penguin 1985) passim.

83 Volker Boehme-Neßler, 'Die Macht der Algorithmen und die Ohnmacht des Rechts' (2017) NJW 3031, 3033.

84 Boehme-Neßler (n 83) 3033; cf Lawrence Lessig, *Code: version 2.0* (Basic Books 2006) 123f.

85 Fries (n 74) 2861; Grundmann and Hacker (n 53) 274.

86 Lawrence Lessig, *Code and other Laws of Cyberspace* (Basic Books 1999) passim.

87 Boehme-Neßler (n 83) 3035; cf. Grundmann and Hacker (n 53) 293.

88 Cf. Boehme-Neßler (n 83) 3035; see also De Filippi and Wright (n 13) 173ff.

89 Cf. Roger Brownsword, 'The E-Commerce Directive, Consumer Transactions, and the Digital Single Market' 165, in Stefan Grundmann (ed), *European Contract Law in the Digital Age* (vol 3 Intersentia 2018).

90 Regarding the challenges of cyberspace regulation see e.g. Viktor Mayer-Schönberger and John Crowley, 'Napster's Second Life?: The Regulatory Challenges of Virtual Worlds' (2006) 100 Nw. U. L. Rev. 1775, 1802f; David R Johnson and David G Post, 'Law and Borders: The Rise of Cyberspace' (1996) 48 Stanford LR 1367, 1367; Joel R Reidenberg, 'The formulation of information policy rules through technology' (1998) 76 Texas LR 553, 553.

jipitec

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu