jipitec

4 | 2017

Volume 8 (2017)
Issue 4 ISSN 2190-3387

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 8 Issue 4 December 2017
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

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

Prof. Dr. Axel Metzger, LL. M.,
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

Articles

Editorial

A Christmas Gift

by **Séverine Dusollier**, Professor, Law School, SciencesPo Paris.

Recommended citation: Séverine Dusollier, Editorial: A Christmas Gift, 8 (2017) JIPITEC 255 para 1.

1 What could be a better Christmas gift than an extra issue of JIPITEC? Yes, you are not dreaming, you have in hands (or on your screen), a fourth issue of your favorite online journal, instead of the usual three per year. What else could you wish for, than spending the holidays curled up in your comfy armchair by the fire, with a cup of tea, coffee, or a glass of wine on the table, with your clients, students, and colleagues out of your mind until January, and finally some time to read scholarly articles in your field.

2 One of the biggest pieces (not of cake, that will come later) of this new issue is no doubt Josef Drexl's article on ownership of data. Drexl is looking at the (once announced, then possibly left aside - for the time being at least) project of the European Commission to adopt some legal protection for big data, in the form of an exclusive property right or other form of regulation, ensuring some control over data in order to make data economy thrive (or so they say). The EU 'Free Flow of Data' initiative was indeed ignited by a Communication that planned to address the issues of ownership and access to data. The specter of commodification of data, which was already fought against 20 years ago, when the sui generis right in databases was discussed, is coming back. Although the 'Free Flow of Data' draft Regulation published a few weeks ago seems to exclude property rights, it is not certain that it will not eventually return in some form or another.

3 Drexl's paper extensively reviews how the data should be regulated, looking at the issues of data ownership and access to data. The paper begins by pondering whether the question of ownership should be raised at all, and what the economic justification would be to add more protection over data than what is already provided by existing laws. Amongst the existing forms of protection, the article analyses sui generis protection in databases, trade secret protection, patent right, unfair competition law, a 'digital' property right, or factual and contractual protection. Then it turns to potential economic justifications for recognising data ownership, but has difficulty in finding any that would be convincing. Therefore, Drexl argues against the creation of a new system of data ownership. As to whether competition law could enhance better access to data, a thorough analysis of the EU competition case law reveals its many shortcomings as regards the data economy, due to its very dynamic nature. Instead the article pleads for state intervention to promote access to data, interoperability and portability, where public interest considerations should play a key role.

4 After such an intense reading, allow yourself a break to play with the new console your child received from Santa. When she has humiliated you (despite the fact that you were the best Mario Bros player in your class as a teenager), it would be a good time to come back and read the not-so-unrelated article by Krzysztof Gartska on digitised memories as personal and sensitive data, drawing on the fictional setting of a video game entitled Remember Me, that imagines a world in which human memories can be digitised. Not only your online movements, consumptions, communications, and interactions are recorded and processed by commercial entities, your memories could now be turned into assets too. In this science-fiction world (or perhaps a forecast into the future), are such digitised memories to be considered as personal data and what would that mean? When memories can be stored, shared, erased, or even hacked, issues of data processing

and security abound. This very exploratory article analyses some of them, most notably the possible qualification of digitised memories as personal data and as sensitive data for the purposes of the GDPR. Gartska's conclusion is that the definitions laid down by the GDPR are sufficiently technology-neutral to address any type of personal data, including what could come in the future, and already illustrated by dystopian games and narratives.

5 Science-fiction pieces like that are fun, but evidence-based scholarship equally carries virtue. This is what Stef van Gompel's article posits; deploring, as many others, what copyright lawmaking has become, he explores how a traditional doctrinal approach, which looks at formal consistency and legal-theoretical foundations, could gain from evidence-based policy supported by empirical research. To that end, the two approaches' strengths and weaknesses are assessed and a number of concrete recommendations are given to lawmakers, notably the need to remove unnecessary and unproven affirmations, such as the mantra of the need for a high protection of authors, that says nothing of how it would lead to a better copyright, or the liberation from international copyright norms, seen as imperatives that cannot be changed. Additionally, van Gompel suggests to include doctrinal principles related to social and fairness objectives among the evidence to be considered, and not to confine the deliberations about how copyright should be designed to economic evidence. To such end, all positions, from creators and rightholders to users and the public at large, should be considered without letting one prevail over another.

6 At that stage of your reading, your tea might have become cold and it will be time to enjoy a refill - maybe with one more piece of that fabulous cake that is left from Christmas Eve - before turning to the article of Eleonora Rosati on the legitimacy of enacting copyright exceptions limited to non-commercial use. She takes the freedom of panorama and quotation as examples that some national laws limit to non-commercial purposes with no corresponding requirement in the 2001 Infosoc directive, and asks whether that would be detrimental to the harmonisation objective of the directive. Her answer is affirmative, particularly as non-commercial or not-for-profit conditions are largely undefined, and such diversity in Member States might impair cross-border uses of copyrighted works. Rosati's conclusion is that Member States should not be entitled to limit the benefit of copyright exceptions to non-commercial uses, if it is not required at EU level.

7 Now the countdown to New Year's Eve is closer, those few days of rest have sharpened your mind and the numbers and figures of Bart van der Sloot's empirical study will come easy for you. Based on a study of around 1000 decisions of the European Court of Human Rights, this paper looks at whether and how harm is compensated and damages awarded in privacy cases. The assessment is based upon different factors, such as the country against which the complaint is directed, the type and number of applicants, the type of damage that is compensated, the type of privacy at stake, and the ground on which a violation is established, each of which resulting in statistical information and analysis thereof. Among the findings of the paper, one can see that in most cases in which a violation of article 8 ECHR has been found, damages were awarded, including for non-pecuniary damages, but for relatively small figures. The compensation of non-pecuniary damages has also increased over time. The amount of awards unexpectedly appears to depend upon the country that is held liable, or the type of privacy violation, as well as upon the section of Court delivering the decision, or the type of persons complaining of a violation (prisoners and migrants having been awarded more limited amounts of money). Van der Sloot's paper joins a promising line of research based on empirical and statistical evidence that could nourish our legal knowledge in privacy, intellectual property, and any other IT-related topic, which JIPITEC would be pleased to publish in the future.

8 The JIPITEC editorial team wishes you a very happy holiday and a fruitful year 2018. For those of you, who have deservedly spent the holiday without looking at your emails or internet and who only open this new issue coming back to work in January, we hope that reading this issue will be your first pleasure of the year!

Séverine Dusollier, December 2017

Designing Competitive Markets for Industrial Data

Between Propertisation and Access

by **Josef Drexl***

Abstract: As part of the project to establish a Digital Single Market, the European Commission has launched a 'Free Flow of Data' initiative. This initiative is meant to enhance the growth potential of the emerging data economy, which is characterised by the digitisation of production (smart factories) and the advent of digitised products such as smart—driverless—cars, or smart wearables that will be able to communicate with each other and the environment through the Internet of Things. Furthermore, the enormous amount of data generated and controlled by the industry could serve as a most valuable input for other new data-driven services and for applications in the public interest, such as the operation of smart cities, smart and resource-efficient farming, or measures to prevent the spread of infectious diseases. Obviously, this new data economy has to rely on the commercialisation of data. But what kind of regulation is needed in order to make the data economy work? Do we need new ownership rights in data? Or should regulation focus on access in order to make data as widely available as possible? The European Commission is currently trying to formulate answers to these questions. This article aims to assist the Commission by working on a pro-competitive framework for issues of both ownership and access. In so doing, this article undertakes two things: first, it analyses to what extent intellectual property laws already provide control over data and then discusses the need and justification for introducing new rules on data ownership. Second, it analyses whether EU competition law already provides remedies to promote access to data, and furthermore explores whether and under which conditions the introduction of new access regimes would be advisable. This article is to be considered as ongoing research. It does not yet take into account more recent developments in 2017.

Keywords: Data ownership; access to data; data sharing; data economy; data-driven economy; Internet of Things; data analytics; database rights; trade secrets protection; EU competition law; refusal to license; essential facilities; data portability

Recommended citation: Josef Drexl, Designing Competitive Markets for Industrial Data – Between Propertisation and Access, 8 (2017) JIPITEC 257 para 1.

A. Introduction

1 The advent of the data economy and the Internet of Things (IoT) is currently challenging regulators across the globe. Buzzwords such as 'big data' or 'data as the oil of the modern economy' are used everywhere, and questions like 'Who owns the data?' are not only asked by the media, but are also heard and taken up by decision-makers in the political arena.

2 In the EU, potential new regulation for the data economy, concerning both data ownership and access to data, is part of the Commission's current priority project to implement a Digital Single Market.[1] In May 2015, the Commission identified 16 key actions for the implementation of this Digital Single Market,[2] including the 'building of a data economy'. This 'action' is supposed to contribute to the third pillar of the Digital Single Market project, aiming at 'maximising the growth potential of the digital economy'.[3] More concretely, the Commission announced a 'Free Flow of Data' initiative for 2016, which would address in particular the restrictions on the free movement of data beyond the protection of personal data with the objective of enhancing the cross-border use of data in a world of big data and the Internet of Things. Yet the initiative also includes a mandate to look at the issue of ownership. The announcement reads as follows:

> *The Commission will propose in 2016 a European 'Free flow of data' initiative that tackles restrictions on the free movement of data for reasons other than the protection of personal data within the EU and unjustified restrictions on the location of data for storage or processing purposes. It will address the emerging issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data. It will encourage access to public data to help drive innovation.*[4]

3 As regards ownership, the mandate does not indicate the direction in which later regulatory actions may ultimately go. In the light of the objective to promote access to data, one could expect the Commission to consider whether existing 'ownership' regimes are in need of additional exceptions and limitations to promote access. This would have been in line with the debate in other fora, such as OECD in particular, where a study of 2015 highlighted the need to promote access to big data in order to generate maximum benefits for society.[5] Rather than taking data ownership as the starting point of the regulation of the data economy, the OECD study recommends developing and improving 'data governance regimes' that 'overcome ... barriers to data access, sharing and operability'.[6]

4 As regards the EU, however, the debate quickly shifted direction. While the responsibility to work on the initiative was allocated to the Digital Value Chain unit of DG CONNECT, which is also responsible for the open data policy of the EU as regards public sector information in particular, it was the German Commissioner Günther Oettinger responsible for DG CONNECT who publicly contributed to the impression that the Commission would soon propose legislation

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

This article complements the Position Statement of the Max Planck Institute: Josef Drexl, Reto M Hilty, Luc Desaunettes, Franziska Greiner, Daria Kim, Heiko Richter and Gintarė Surblytė, 'Data Ownership and Access to Data' (16 August 2016), available at: <http://www.ip.mpg.de/en/link/positionpaper-data-2016-08-16.html> (accessed 10 September 2016). The views expressed in this article are however only those of its author.

This article was first made available online as Research Paper No. 16-13 of the Max Planck Institute for Innovation and Competition Research Paper series on 8 November 2016. The text remains substantially unchanged. It does not take into account the debate following the EU Commission's Communication of 10 January 2017 on Building a European Data Economy, COM(2017) 9 final. On this Communication see the Position Statement of the Max Planck Institute: Josef Drexl, Reto M. Hilty, Jure Globocnik, Franziska Greiner, Daria Kim, Heiko Richter, Peter R. Slowinski, Gintare Surblyte, Axel Walz and Klaus Wiedemann, 'On the European Commission's Public Consultation on "Building a European Data Economy"' (26 April 2017) available at: <http://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Statement_Public_consultation_on_Building_the_EU_Data_Eco_28042017.pdf> (accessed 19 October 2017). On this, see also Josef Drexl, 'On the Future Legal Framework for the Digital Economy: A Competition-based Response to the "Ownership and Access" Debate', in Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Baden-Baden: Nomos, forthcoming) 222-43.

1 Implementation of the Digital Single Market is one of four 'priority projects' of the current European Commission under the aegis of President Jean-Claude Juncker. See Jean-Claude Juncker, 'My priorities', available at: <http://juncker.epp.eu/sites/default/files/attachments/nodes/en_01_main.pdf> (accessed 10 September 2016).

2 See Communication of the Commission of 6 May 2015 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—A Digital Single Market Strategy for Europe, COM(2015) 192 final. See also European Commission, 'A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen', Press Release of 6 May 2015, available at: <http://europa.eu/rapid/press-release_IP-15-4919_en.htm> (accessed 10 September 2016).

3 See Chapter 4.1 of the Commission Communication (*supra* n 2) at 14-15.

4 *Ibid*, at 15. (Emphasis added.)

5 OECD, 'Data-Driven Innovation: Big Data for Growth and Well-Being' (2015) 195-98, available at: <http://www.oecd.org/sti/data-driven-innovation-9789264229358-en.htm> (accessed 10 September 2016).

6 *Ibid*, at 195-99 (in particular at 198).

on a new 'data use right' (*Datennutzungsrecht*).[7]

5 The data economy and its regulation attract particular attention in Germany, where the industry is deeply involved in the development of new business models of the Internet of Things. In Germany, in 2011, the 'Industrie 4.0' initiative was launched as a joint initiative of the government, the private business sector and the public research sector to manage and promote a fourth industrial revolution characterised by the integration of manufacturing in modern information and telecommunications networks, including the Internet of Things.[8] This initiative not only aims at optimising the manufacturing process, whereby the product itself, in the various production phases, communicates with, and steers, the production process. It also targets the logistics sector, aiming to foster an 'Internet of Services' that builds on smart products as a basis for new kinds of services provided to consumers. This early initiative may also explain why, in Germany, legal regulation of the industrial dimension of the data-driven economy, namely, beyond the issues of protection of personal data in particular, attracted attention much earlier than in other parts of the EU, both from the academic community[9] and from the stakeholders' side. As regards the latter, the *Bundesverband der Deutschen Industrie* (BDI, German Industry Association) published a study on the legal ramifications of the data-driven economy that, *inter alia*, argued against the introduction of a new right of data ownership.[10] A report of the Bavarian Industry Association (*Vereinigung der Bayerischen Wirtschaft*) argued that ownership for single pieces of data and small datasets could lead to a scarcity of data and distort innovation through big data analytics.[11]

6 Indeed, scepticism about introducing a new intellectual property right expressed by the industry that is expected to rely on this right for protecting its own investments is not something that experts in intellectual property law would necessarily expect. However, the same scepticism was voiced by the representatives of the 'Industry 4.0' sector who were invited to a hearing of DG CONNECT on the 'legal regime fit for an efficient and fair access to and usage and exchange of data' in Luxembourg on 17 March 2016.[12] The hearing concentrated on the legal protection of the investment in data collection capabilities and the exploitation of the value represented by that data. The hearing was not least held for the purpose of learning more about the legal instruments that are used and needed to

7 See, for instance, 'Oettinger: Versicherungen brauchen mehr digitale Produkte', *Der Standard* (25 November 2015), available at: <http://derstandard.at/2000026414259/Oettinger-Versicherungen-brauchen-mehr-digitale-Produkte> (accessed 20 May 2016) (reporting on a talk by the Commissioner at a conference of the German insurance industry association in November 2015 where the Commissioner called upon the insurance industry to take part in the discussion on such a right). See also the association's website: 'Versicherungstag 2015: Es geht mehr denn je um den Kunden' (25 November 2015), available at: <http://www.gdv.de/2015/11/versicherungstag-2015-chancen-der-digitalen-welt/> (accessed 10 September 2016). The author of this paper personally attended another talk given by the Commissioner at a conference of the Forschungsinstitut für Wirtschaftsverfassung und Wettbewerb (FIW) in Innsbruck on 25 February 2016, where the Commissioner made similar statements. See 'Rede (Kommissar Oettinger) auf dem 49. FIW-Symposion (2016) in Innsbruck zur Digitalisierung' (25 February 2016), available at: <http://www.fiw-online.de/de/aktuelles/aktuelles/rede-kommissar-oettinger-auf-dem-49.-fiw-symposion-2016-in-innsbruck-zur-digitalisierung> (accessed 10 September 2016) (reporting on the Commissioner asking who owns the data that are produced by modern cars in a world of the Internet of Things). In a more recent speech at the occasion of a Commission conference on the 'Free Flow of Data' initiative, however, the Commissioner did not repeat this claim for a data usage right. See Günther Oettinger, Speech at the Conference 'Building European Data Economy' (17 October 2016), available at: <https://ec.europa.eu/commission/2014-2019/oettinger/announcements/speech-conference-building-european-data-economy_en> (accessed 30 October 2016).

8 See the public announcement of the initiative made on the occasion of the 2011 Hanover trade fair: Henning Kagermann, Wolf-Dieter Lukas and Wolfgang Wahlster, 'Industrie 4.0: Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution' (1 April 2011), available at: <http://www.vdi-nachrichten.com/Technik-Gesellschaft/Industrie-40-Mit-Internet-Dinge-Weg-4-industriellen-Revolution> (accessed 10 September 2016).

9 More in favour of such a right Herbert Zech, 'Daten als Wirtschaftsgut—Überlegungen zu einem "Recht des Datenerzeugers"' (2015) *Computer und Recht* 137; most recently see Herbert Zech, 'A legal framework for a data economy in the European Digital Single Market: rights to use data' (2016) 11 *J Int Prop L & Prac* 460; Herbert Zech, 'Data as tradeable commodity' in Alberto de Franceschi (ed.), *European Contract Law and the Digital Single Market* (Insentia: 2016 forthcoming) 51; against such a right Michael Dorner, 'Big Data und "Dateneigentum", Grundfragen des modernen Daten- und Informationshandels' (2014) *Computer und Recht* 617. See also Alberto De Franceschi and Michael Lehmann, 'Data as Tradable Commodity and New Measures for their Protection' (2015) 51 *Italian LJ* 51 (seemingly supporting the recognition of a 'data usage right').

10 Konrad Żdanowiecki, 'Recht an Daten' in Peter Bräutigam and Thomas Klindt (eds), *Digitalisierte Wirtschaft/Industrie 4.0*, Study of Noerr LLP for BDI (November 2015) 18-28, available at: <http://bdi.eu/media/themenfelder/digitalisierung/downloads/20151117_Digitalisierte_Wirtschaft_Industrie_40_Gutachten_der_Noerr_LLP.pdf> (accessed 10 September 2016).

11 Zukunftsrat der Bayerischen Wirtschaft, 'Zukunft digital—Big Data: Analyse und Handlungsempfehlungen (July 2016) at 99, available at: <https://www.vbw-zukunftsrat.de/pdf/big_data/vbw_zukunftsrat_handlungsempfehlungen_langfassung_v15_rz_web.pdf> (accessed 10 September 2016).

12 The author of this paper took part in this 'Round Table' as a representative from the academic community. The results of the event are documented in a synthesis report not publicly available of the Unit for Data Value Chain (available from the author).

implement new business models based on big data. Unanimously, the industry participants stressed that they were able to implement their business models involving data-sharing by relying on contract law. 'Ownership' was even considered a concept that does not fit the needs of the data economy; introduction of a new right was seen as a form of government intervention that needs to be avoided. At the same time the need to promote access, with a potential role of competition law, was discussed. Ultimately, the Digital Value Chain Unit's representative indicated that the Commission would come forward with policy conclusions in the form of a Communication, which was published in January 2017.[13]

7 There seem to be two obvious, yet related, reasons why the industry rejects the introduction of new property rights for data: first, many firms are producers of data and have to rely on access to data of other players at the same time. Hence, it is not clear to them whether the introduction of new rights would provide them with more benefits than drawbacks. Second, the criteria on who would qualify as the owner of the new right are not at all clear. Many stakeholders, in one way or another, contribute to the same data-based business model and may have very diverse kinds of interests. Therefore, allocation of data ownership is indeed a major issue.[14] This is also an issue of considerable complexity because of the particularities of the specific sectors. The interests of stakeholders regarding the data collected by the sensors of a car, in which public authorities also have an interest, so as to protect the environment or to increase driving safety, are likely to be different than those in the case of health-related data derived from blood tests of patients for which a patented diagnostic tool is used, which, taken together with similar data from other labs, may help authorities around the globe to fight the spread of infectious diseases. The difficult question to whom the new data ownership should be allocated led the BDI study to conclude that the legislature should refrain from creating such a right from the outset.[15] In such a situation it should not come as a surprise that firms, which cannot foresee, and do not have any legitimate expectation, that they will be recognised as owners of data rights, will be hesitant to support any additional legislation. If it was accepted that there should be ownership of everybody to whom specific data can be allocated, the result would be multiple ownership of the same data with considerable negative effects on access to that data.[16]

8 This article aims to produce additional insights on how the data economy should be regulated as regards data collected by the industry. Ideally, it will also assist the European Commission in its task of designing its regulatory approach to promoting the data economy in the interest of society. For that purpose, the article looks at the issues of both data ownership and access to data.

9 As a starting point, this article argues that the question 'Who owns the data?' is fundamentally misguided. This is so for two reasons: first, it skips the prior question of whether there is a need to recognise any ownership. There is no natural law that says that data as an asset, although it may have economic value, has to be owned by anybody. Rather, recognition of any new right should, as is the case in intellectual property in general, be considered a form of government regulation of the market, which is in need of a particular justification. In terms of data ownership, which enables its owner to commercialise data, this justification needs to be an economic one.[17]

10 The second reason is that identifying the owner does not resolve all issues of ownership. In the field of intellectual property law, the legislature has to decide upon a series of issues: first and foremost, the subject-matter of protection has to be determined. Hence, the law would have to clarify what is meant by 'data' in the context of 'data ownership'. And then there is the issue of 'how' ownership should be protected. In other words, the legislature has to decide on the scope of protection—namely, what kind of interests and uses are protected— whether there are certain exceptions and limitations that

13 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of The Regions Building A European Data Economy*, COM (2017) 9 final, Bruxelles, 10.1.2017. As mentioned, this article does not yet discuss this Communication. For further references see at n * above.

14 The OCED (*supra* n 5) at 196, lists ten different kinds of stakeholders. It thereby relied on literature—David Loshin, 'Knowledge integrity: Data ownership' (2002) (no longer available on the Internet)—that predates the big data debate and, in particular, does not yet take account of big data analyses and big data brokerage.

15 Żdanowiecki (*supra* n 10) at 28.

16 This could be considered a situation of a 'tragedy of the anti-commons' in which too many property rights in the same asset lead to inefficient underuse of that asset. See Michael A. Heller, 'Tragedy of the Anti-Commons: Property in the Transition from Marx to Markets' (1998) 111 *Harv L Rev* 621.

17 This distinguishes 'data ownership' from the protection of personal data. It is to be noted that data protection rules in the EU only protect natural persons. See 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 on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1. Corporate entities may also have an interest in keeping back information that has the potential of harming their 'corporate reputation'. However, this can be seen as part of their commercial interests. In this context, trade secrets rules may provide some protection. On this, see at C.II. below.

take into account conflicting interests and, finally, which remedies will be made available to the right-holder. In making such decisions on the framing of the new right's regime, the economic arguments that justify the recognition of a new right as such have to play a key role.

11 In addition, any new legislation on data ownership should take into account the public interest in maintaining competition in the market. Additional rights regarding data as an asset may enhance market power deriving from the control of data. As in other fields of intellectual property law, the guidepost should be that both property rights and competition pursue the goal of enhancing innovation.[18] If the data ownership right is supposed to create incentives to invest in new data-based business models by controlling the use of data, and if competition is designed to maintain competitive pressure on the right-holder to maintain its incentives to invest, the best approach will be to take the competition dimension into account as a core consideration for the design of the property rules. This approach has the advantage of reducing the need for later reliance on competition law as a countervailing legal regime. Accordingly, the interest in maintaining access to data in the interest of society would have to be one of the criteria that guide any future legislation on data ownership.

12 In the following, the article will first take a look at the phenomenon of the emerging data economy and how value is generated in that economy (section B. below). Then, it will explore to what extent there is already control over data, in the form of either factual control or legal control based on specific protection regimes (section C. below). Against this backdrop, it will be possible to discuss whether and to what extent there is an economic justification for additional protection (section D. below). Furthermore, the article will explore the different issues concerning the design of an additional protection regime (section E. below). Yet the analysis is not limited to the question of whether additional ownership rights are needed. Rather, in part F. this article will analyse and discuss legal regimes, including competition law and more targeted forms of legislation, to enhance access to data in order to promote a pro-competitive data economy.

18 See Communication from the Commission—Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements, [2014] OJ C 89/3, para 7.

B. The phenomenon of the data economy

13 For the purpose of this article, a number of particular features of the data economy need to be understood properly in order to answer the policy issues surrounding data ownership. This includes a description of the use of data as an asset in the data economy and the economic and societal benefits of that economy (part B.I. below), the phenomena of 'data' and 'big data' in this context (part B.II. below), specific features of how value is generated in this economy (part B.III. below), and finally the interests of specific stakeholders that need to be taken into account in designing any future legislative action (part B.IV. below).

14 All of these issues are closely linked to new business models that are currently evolving in very diverse sectors of the data economy. This means that the following analysis has to do with very dynamic phenomena of high complexity and variety. Anybody who engages in this topic has to understand what is actually going on in the market concerning the underlying business models; also, generalisations need to be considered with caution. This is already an important lesson for the legislature. Any rule that is adopted against the backdrop of one case scenario also has to fit other scenarios to which it may apply. In addition, property legislation in particular should not only respond to the needs of today's economy, but also the needs of tomorrow. This argues against precipitate legislative action, despite the enormous speed of the development of the data economy, at least as regards the recognition of new property rights without a clear understanding of the business models that will be affected now and in the future. Such new rights have the potential of increasing market power, creating barriers to access to important data and, ultimately, curbing rather than fostering the data economy.[19]

19 An example of such premature legislation was the introduction of the *sui generis* database right by the EU legislature in 1996. See Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, [1996] OJ L 77/20. Ten years after its adoption, the Commission had to admit that there was no evidence that the Directive had indeed produced the expected positive economic effects as regards the information market in the EU. The Commission even considered a withdrawal of that protection, without, however, recommending it. See DG Internal Market and Services Working Paper—First evaluation of Directive 96/9/EC on the legal protection of databases (12 December 2005), available at: <http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf> (accessed 10 September 2016).

I. Data as a most important asset of the data economy and the societal benefits deriving from it

15 In the data economy, data have become the key asset for conducting business. This explains why data are often called the 'oil' of the new economy.

16 Beyond the use of this buzzword, it is more important to understand why and how data are used. Different forms of use relate to different stages of the development of the Internet. At its first stage, the Internet was used as a tool for providing information. This was the time when politics started to realise that an 'information society' with new services was emerging that was in need of new legislation.[20] At this first stage of development the Internet emerged as an information and selling platform (web 1.0).

17 At the second stage, new business models developed that provided consumers with other kinds of services, yet still related to information, without charging them a price. These services, such as search engines or social platforms that connect people with people (web 2.0), were often exclusively financed by advertising. Whereas, at the first stage, information was largely limited to information as an object of the service; at the second stage, personal data became a most important input for new kinds of business models that were information-related. The advertising value of a service or platform increases with its attractiveness for private users who, in turn, provide its operator with personal data as the key input for such business models.

18 In the Internet of Things, physical objects get connected with each other and with the environment. This brings about another major boost of the data that are collected and an extension of the data that enter into big data collections and business models. At this stage of Internet development, any data that is collected by somebody for a particular purpose can become a most important asset for other economic players or public entities for very different purposes. For instance, smart cars nowadays collect data for steering driverless cars and for providing better and timely—even predictive—maintenance services. But cars may also register the driving habits of the driver, in which the insurance companies are interested, the geographical location of the car at a given moment can inform providers of geographic data, such as Google Maps, about a change of the direction of a one-way road, and inform the public authorities about the volume of use and traffic conditions of roads at a given time. The social benefits of data will even increase with the inclusion of the data in larger datasets that bring together data from different sources, such as from different car manufacturers to get a more comprehensive picture of the concrete traffic conditions in a particular geographic area. The innovative character of this kind of use of data consists in linking large datasets in order to answer many different questions based on mere correlations between different kinds of data (often called 'data mining') in the interest of individual businesses or the public.

19 In this big data world, it also seems that the role of the state is beginning to change. At an earlier stage of the development of the Internet, states started to realise that it is becoming increasingly important to grant private businesses access to publicly held data (so-called 'public sector information', PSI) for commercial re-use in order to promote new commercial information services.[21] Conversely, the modern private data economy is increasingly producing data from which big data analytics in particular can extract new knowledge that can optimise public decision-making—whether it is about increasing traffic security based on data collected by cars, protecting the environment, for instance, by relying on information that is collected by machines used in the agricultural sector, or revolutionising health care around the world by collecting and analysing the clinical, genetic, environmental, and behavioural data from myriad sources.[22] In other words, the public sector is a major contributor, as well as a beneficiary of the data economy and big data analyses.[23]

20 In sum, in the development of the 'data economy' a shift of focus can be observed. Whereas the business models of major Internet platform operators are built on the use of personal data and, accordingly, may give rise to particular concerns about effectively protecting the use of personal data, the data economy will no longer be limited

20 In the EU, see in particular Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), [2000] OJ L 178/1; Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, [2001] OJ L 167/10.

21 See Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, [2003] OJ L 345/90, as revised by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013, [2013] OJ L 175/1; consolidated version available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02003L0098-20130717&from=EN> (accessed 10 September 2016).

22 On the benefits for health care, see in particular the study by OECD (*supra* n 5) at 331-78.

23 The OECD argues that the governments should 'lead by example' in promoting data-driven innovation by granting access to public-sector information. See OECD (*supra* n 5) at 404-48.

to the use of personal data for advertising and marketing purposes. There are two more important innovation-driven features of the data economy that can be witnessed. On the one hand, in the era of the Internet of Things, data collection by sensors will allow consumers to be provided with innovative smart products and services that will increasingly replace traditional products. On the other hand, the data collected in this industry will be of particular utility to private actors in very different business sectors and to public entities. Hence, data collected by smart products will become an important input, both for other businesses and for the government.

II. What do we mean by data and big data?

21 Asking the question of who owns the data suffers from the terminological weakness of what is meant by the term 'data'. There are two aspects to the problem. First, more precision is needed in defining the individual data. The second aspect relates to the aggregation of larger datasets and their protection.

22 The first issue relates to the question of the potential object of protection of data. Take the following example: a smart car of manufacturer A, through the sensors attached to its dampers, locates a pothole. This information is not yet noticed by any natural person; however, it is stored in the form of digital data on a server of manufacturer A. If the law recognised ownership of A in this data, the question arises whether ownership relates to the pure digital dataset in the form of bits and bytes, or to the 'information' the digital dataset contains. This makes a major difference from a competition-oriented perspective. The pothole can of course be registered by the smart cars of different manufacturers (A and B) that follow each other. Hence, the 'information' in which the public road authority is interested could be extracted from two different (competing) datasets.

23 This example shows that the concept of data is in need of additional precision. When we use the term 'digital data', we typically refer to 'machine-readable encoded information'.[24] However, the interest in 'protecting data' relates to the information encoded in these bits and bytes. As regards this information, in turn, a distinction can be made in terms of semiotics between the different levels of information.[25] For data protection, the distinction between the syntactic and the semantic level is key. The syntactic level regards the representation of information in particular signs, for instance as a text, a photograph or a video. In contrast, the semantic level relates to the meaning. Take the example of a camera at a public square that produces a video. The syntactic information is the video as such, which can be stored on different carriers. In contrast, the meaning that can be extracted from that video, for instance, how many people or vehicles cross the square on a single day, is placed on the semantic level. These distinctions can be further illustrated by the example of a novel printed as a book. The book is the physical carrier of the information. The syntactic information consists in the text printed in a sequence of letters and words. The semantic information is the story told by the novel. If somebody does not speak the language in which the novel is written, to this person the information will only be accessible on the syntactic level.

24 Hence, whenever the law protects 'data', it has to make clear what it really protects. There is no general argument against protecting semantic information. Indeed, trade secrets protection and private data protection relates to the semantic level of information.[26] The know-how of a firm consists in technical knowledge; it does not matter whether this knowledge arises from a drawing, a text or a combination of both, or whether this knowledge is stored in a digital format or not. Similarly, individuals are protected against unauthorised processing of information relating to them, whether this information is contained in a text, photographs, or audiovisual recordings. In contrast, in the abovementioned example on the potholes in the street, it would be better to avoid protecting the semantic information the sensors of a car collect. Hence, the question of whether the law should protect the semantic or the syntactic information, or even only the integrity of the digital file, will depend on the circumstances. This analysis would seem to argue for context-specific regulation. Even a general regime on the protection of industrial data would thus appear problematic since, in some instances, protecting semantic information such as in the case of trade secrets seems the right approach, while protection of data collected through sensors in the public sphere should probably not be extended to the meaning these data are able to convey. To

24 Definition used by Herbert Zech, 'Data as tradeable commodity' in Alberto de Franceschi (ed.), *European Contract Law and the Digital Single Market* (Insentia: 2016 forthcoming) 51, at 53.

25 On this distinction see also Maximilian Becker, 'Rechte an Industrial Data und die DSM-Strategie' (2016/1) GRUR Newsletter 7, available at: <https://www.grur.org/fileadmin/daten_bilder/newsletter/2016-01_GRUR_Newsletter.pdf> (accessed 10 September 2016); Andreas Wiebe, 'Protection of industrial data—a new property right for the digital economy' (2016) *Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil* (*GRUR Int*) 877, at 881; Zech (*supra* n 24) at 53-54.

26 Art 4(1) General Data Protection Regulation (*supra* n 17) defines 'personal data' as 'any data relating to an identified or an identifiable person'.

draw the line between the two approaches is not an easy task. Constitutional rights can argue in favour of protecting semantic information, such as in the case of personal data. Yet in other instances constitutional rights and competition policy will argue against ownership in semantic information, if such protection has the potential of undermining the free flow of information.[27]

25 The second problem arises from the fact that firms do not only hold individual pieces of data. Data are collected and then included in larger datasets. This raises the issue of whether there should be protection of each and every data information or whether there should be protection of the whole dataset in its particular composition.

26 This second issue directs the attention to the features of big data, the technical features of big data analytics and, ultimately, big data business models. At the outset, it should be stressed that big data analyses are only one application where data held by one person is used by another person in the data economy. The purpose of big data analyses is to optimise decision-making. The decision-maker can be any person or entity, usually a firm or a public entity. The following three features are key to the technical understanding of big data: volume, velocity and variety (the so-called '3 Vs').[28] 'Volume' relates to the exploding volume of data that is produced by different sources, including the Internet of Things and social media. Big data is defined by the fact that the volume of data to be analysed transcends the current capacity of storage and processing systems. 'Velocity' relates to the dynamic nature of big data. Indeed, big data constantly changes as new data is produced. To keep up with the speed of this process is key in big data analytics because the users of the results of such analyses will usually have to rely on real-time analyses for decision-making in a constantly changing world. 'Variety' relates to a wide range of different kinds and formats of data. Data may originate from very different sources, such as machine sensors, websites or social platforms; it may be structured or unstructured; and it may consist in texts, pictures, audio or video. While it would be important to combine different kinds of data in big data analyses, the large variety of data constitutes a major technological challenge to big data analytics.[29]

27 These technical features also need to be taken into account when it comes to the policy decision of whether additional data ownership rights should be created. The general claim to be made is that data ownership should not create obstacles to big data analyses, because it is through these analyses that new insights and social benefits will be generated. The issue of volume indicates the difficulty of storing all data that needs to enter into an analysis on one server. This means that big data analyses may have to take place in a decentralised manner. Either the 'code has to be brought to the data' or individual datasets need to be screened first for the critical data, which is then transferred for the analysis.[30] In both cases, it is clear that the big data analyst is in need of access to different data sources and that the different data sources cannot *ex ante* be considered as substitutes for each other. Creating new data rights at the upstream level of holding such datasets could therefore considerably obstruct big data analyses.

28 Velocity may be an even more important feature to be taken into account for the regulation of ownership. Velocity indicates that 'data' should not generally be considered as a 'commodity' that

27 In this context, the *Magill* competition law case of the European Court of Justice (now Court of Justice of the EU, CJEU) should be recalled. Since British and Irish copyright law recognised copyright protection for the mere listings of TV programs, TV stations were able to monopolise the downstream market for printed TV programs and prevent the emergence of comprehensive TV guides combining the programs of different TV stations. The case gave rise to the EU case-law on refusal to license. For more detail see at F.II.1. and F.II.2. below. Copyright protection blocked access to the 'information' contained in the TV listings and, thereby, gave rise to dominance of TV stations in the upstream information market and allowed the TV stations to eliminate competition in the downstream market. See Judgment in *RTE and ITV v Commission* ('*Magill*'), C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98, [1995] ECR I-743. For this case, it can be argued that copyright went too far in the first place by blocking access to information. On this case see also at F.II. below.

28 See, for instance, Amir Gandomi and Murtaza Haider, 'Beyond the hype: Big data concepts, methods and analytics' (2015) 35 *Int'l J. Inf. Manag.* 137, 138; Stephen Kaisler, Frank Armour, J. Alberto Espinosa and William Money, 'Big Data: Issues and Challenges Moving Forward', (2013) *46th Hawaii International Conference on System Sciences* 995, available at: <http://www.computer.org/csdl/proceedings/hicss/2013/4892/00/4892a995.pdf> (accessed 10 September 2016); Daniel O'Leary, 'Artificial Intelligence and Big Data' (2013) *IEEE Intelligence Systems* 96, available at: <http://people.westminstercollege.edu/faculty/ggagne/fall2014/301/chapters/chapter1/mex2013020096.pdf> (accessed 10 September 2016); Paul Zikopoulos and Chris Eaton, Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming (2011). The first author to have hinted at these three features seems to be Doug Laney, '3-D Data Management: Controlling data volume velocity and variety' (2001), available at: <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf> (accessed 10 September 2016). From a competition law perspective see Daniel L Rubinfeld and Michal S Gal, 'Access Barriers to Big Data' (16 August 2016) at 8-9, available at: <http://ssrn.com/abstract=2830586> (accessed 10 September 2016).

29 On the technique and process of data analytics see Gandomi and Haider (*supra* n 28) at 140-143.

30 These two solutions are identified by Kaisler et al. (*supra* n 28) at 997.

can be traded like other commodities. Rather, the modern data economy typically has to rely on real-time information. Hence, a concept of ownership in data, similar to copyright in a work, which would invariably be protected for a fixed period of time, would not serve the needs of such data services and big data analytics. Big data analyses that are confronted with dynamic processes and have to serve a purpose in a dynamic environment, such as steering the traffic management system of a smart city, will have to rely on permanent access to real-time data sources. Ownership in individual data will hardly be able to constitute the backbone of such a service.

29 Velocity is closely linked to another 'V' that is increasingly mentioned as an additional feature of big data and which is key from a legal perspective, namely, 'veracity'.[31] Data needs to be reliable to serve the purposes of a data economy. Where real-time data are needed, but not delivered, the service also misses the requirement of veracity. From a legal perspective, veracity indicates that the supply of data should also come with particular responsibility.

30 In this regard, it is worth noting that the EU is currently moving in the direction of fixing uniform standards of 'quality' of 'digital content' that need to be respected if digital content is supplied under a contract with a consumer.[32] The Proposal for a Directive on the supply of digital content defines 'digital content' as '*data* which is produced and supplied in digital form, for example video, audio, applications, digital games and any other software'.[33] The Directive would have the effect of creating a harmonised regime of contractual liability for both physical goods, which are also often sold over the Internet, and data. This, however, does not automatically lead to the recognition of ownership in the underlying data.[34] Whether there is contractual liability if digital content does not meet the quality that is to be expected under the contract and whether the supplier transfers ownership in the framework of such a contract are two separate legal issues. Most importantly, ownership implies a third-party effect while the proposed Directive only creates rights and obligations between the parties to the sales contract.[35]

31 In addition, also as regards big data analyses, the difference between the syntactic and semantic level of data is to be taken into account. Big data analytics consists in reading large datasets to discover 'new' meaning—in the sense of (semantic) information—that has so far not been observed. Big data analytics acts like a person who is able to read the data in a different way by identifying correlations between different data—again in the sense of information—to draw conclusions from those correlations. Hence, the information that big data analyses produce is already hidden in the pre-existing datasets. However, it is big data analytics that allows us to discover this semantic information. This explains how problematic it would be to recognise protection of all semantic information contained in the pre-existing datasets for those who control access to these sets. It is indeed the contribution of the data analyst that leads to the discovery of that information and, hence, any right in this information should be vested in the data analyst[36] rather than the holder of the datasets that are analysed.

III. From value chains to value networks

32 For considering whether new property rights in data are to be recognised from a functional perspective, it is crucial to understand who generates economic value and, as a follow-on question, whether this contribution depends on the recognition of a property right. In this regard, it is important to understand that in the data economy, value is generated differently than in the traditional economy.

33 In the traditional economy, the still dominant paradigm relates to vertical value chains. Manufacturers purchase input for the production of goods in upstream markets and then sell them through distribution chains—often including wholesalers and distributors—to consumers. At each level of the production and distribution chain, some economic value is added.

31 An example is big data analytics in the healthcare sector; see Wullianallur Raghupathi and Viju Raghupathi, 'Big data analytics in healthcare: Promise and potential' (2014) 2(3) *Health Information Science & Systems* 1, at 2, available at: <https://hissjournal.biomedcentral.com/track/pdf/10.1186/2047-2501-2-3?site=hissjournal.biomedcentral.com> (accessed 10 September 2016).

32 Article 6 of the Proposal of Commission of 9 December 2015 for a Directive of the European Parliament and of the Council on certain aspects concerning the supply of digital content, COM(2015) 634 final.

33 *Ibid*, Art 2(1)(a).

34 See, however, De Franceschi and Lehmann (*supra* n 9) at 59-60 and 71 (relying on the corresponding rule contained in the previous draft for a Common European Sales Law and attributing a property dimension to this proposal).

35 As regards the recognition of ownership in the download of a computer program by the CJEU in the Judgment in *UsedSoft*, C-128/11, ECLI:EU:C:2012:407, paras 45-52, see at C.V. below. See also De Franceschi and Lehmann (*supra* n 9) at 60-63 (relying on this decision in their yet cautious support of data ownership).

36 Such information can constitute trade secrets. On trade secrets protection see at C.II. below.

34 In contrast, in a world of smart goods and the Internet of Things, economic value is increased in very complex and dynamic value networks, which can be disruptive for traditional value chains,[37] through collaboration of the different participants in the network. This paradigm shift from value chains to dynamic value networks is identified as a core feature of the current digital transformation of the industry.

35 Four sub-factors are relevant for this shift:[38] (1) *Improving decisions based on data:* sensor-generated industrial data and analysis of big data help firms optimise their decisions. For instance, predictive maintenance becomes possible. (2) *Full automation:* Automation through digital technology, including robotics, revolutionises production and the use of products (e.g. driverless cars). Automation increases the speed of production and decreases the likelihood of defects. (3) *Connectivity:* Objects and machines within the factory and beyond get connected over the Internet and allow supply and production to be steered from the perspective of the need of the customer, which results in quicker production and distribution while saving resources. (4) *Increasing role of Internet intermediaries:* The intermediaries from the Internet sector who have the best access to and knowledge of the needs of consumers and of controlling the data interfaces between different markets gain a competitive advantage in the industrial sector where smart products are produced. This explains why Google and other firms are today trying to expand their activities into the industrial sector. Google, or Alphabet as Google's parent company, may now already have considerable competitive power for entering the market for smart, driverless cars based on its control of geographic data, and may provide most efficient transport services to passengers who, in the future, will no longer buy their own cars but become passengers of Google transport services. At the same time, by expanding their activities to the production and operation of smart products, these Internet intermediaries will gain control over new sources of data.

36 Hence, whereas the digital transformation of the industry decreases existing entry barriers and may even force industrial incumbents out of the market, control over data enables firms originating in the Internet sector, such as Google, to enter into and gain considerable market power in a large variety of different markets for the production and operation of smart products. Recognition of data ownership may therefore have the unwanted effect of strengthening the market power of these firms even more, while, from a competition perspective, it would be wiser to promote access to data that is needed by other market players to operate in such markets.

IV. The interests of different stakeholders

37 The preceding analysis already provides some important insights into the interests of different stakeholders. This analysis underlines the observation in the introduction (at A. above) that industrial players who have already started to invest in the Internet of Things are reluctant to advocate data ownership.

38 The major technological challenges of the Internet of Things relate to big data analytics. This is the area where most investment is needed for tackling the technological obstacles to handling rapidly growing dynamic datasets and solving the problem of analysing a large variety of different kinds of data. However, such innovation is more likely to be fostered through copyright protection for the software solutions employed in the framework of big data analyses rather than through ownership in the data analysed.[39]

39 Moreover, it is to be acknowledged that the non-economic interests of natural persons in the use of their personal data deserve to be safeguarded, also in the data economy. While personal data protection needs to be taken into account, it does not argue as such against the recognition of an economic ownership right of a firm that collects data about the use of a smart product by a natural person. Both rights can coexist. This has the important consequence that rules on the protection of personal data can prevent a data owner from commercialising that data. The industrial holder of personal data can also respect data protection rules by making the data collected from individual natural persons available to third persons in an aggregated and anonymised form in larger datasets. To the extent that big data analytics manages to reproduce personal data, data

37 This has recently been highlighted by a study conducted by Roland Berger Strategy Consultants on behalf of Bundesverband der Deutschen Industrie (BDI). See Roland Berger Strategy Consultants and BDI, 'Analysen zur Studie "Die digitale Transformation der Industrie"' (February 2015) 4-8, available at: <http://bdi.eu/media/user_upload/Digitale_Transformation.pdf> (accessed 10 September 2016).

38 *Ibid*, at 8.

39 Another kind of protection would consist in patent protection for algorithms. However, this is rejected by Josef Drexl, Reto M. Hilty, Luc Desaunettes, Franziska Greiner, Daria Kim, Heiko Richter and Gintarė Surblytė, 'Data Ownership and Access to Data—Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate', paras 12-17, available at: <http://ssrn.com/abstract=2833165> (accessed 12 September 2016).

protection rules may apply again as regards the re-use of that data.

40 As regards personal data, it is important to note that the fact that a natural person is and will often be the source of specific data does not automatically argue in favour of allocating data ownership as an economic right to commercially exploit that data to this person. Protection of personal data is neither vested in the natural person for economic purposes, nor is it an absolute right.[40] Personal data protection does not allocate economic value.[41] Hence, there is room to grant economic rights of exploitation of data originating from natural persons to other persons or firms.

41 The same applies as regards the property of the purchaser of a smart product. The property in the car as a physical object does not automatically extend to the commercial exploitation of the data that are produced by the sensors of that car. The question of whether data ownership should be recognised, and for whom and with which scope of protection, should only be decided against the backdrop of economic welfare considerations.

C. Existing protection regimes as a basis for 'data ownership'

42 Already at the end of the preceding part, it was clarified that at least two rights that are recognised by law do not provide a sufficient basis for data ownership; namely, personal data protection and real property in a smart product that produces the relevant data. However, there are other legal regimes that could provide protection in favour of the firm that controls data. Most obvious candidates are database rights and trade secrets protection. Beyond this, in certain circumstances, the question may arise whether patent protection extends to data that is generated through a patented process. Moreover, one could also contemplate unfair competition rules and the like, as well as a generalisation of property in tangibles as a civil law concept. In sum, none of these regimes provides a convincing or comprehensive basis for data ownership. In contrast, it will be shown that factual control over data can enable the data holder to commercialise that data without additional legal protection by relying on contract law.

I. Database protection

43 At first glance, database rights present a most obvious property regime for controlling access to data.[42] However, this kind of protection has particular limitations that explain why it will often fail to provide protection to data for the new business models of the data industry.[43]

44 The EU legal regime for database protection provides for a two-tier system: Copyright protection is granted to creative databases;[44] *sui generis* protection is granted to databases based on 'substantial investment'.[45]

45 The availability of copyright protection can be excluded from the outset. Article 3(1) of the Database Directive clarifies that the character of a creative work defined as 'the author's own intellectual creation' has to relate either to the selection or to the arrangement of the database's contents. According to the CJEU this originality requirement is satisfied if 'through the selection or arrangement of the data which it contains, its author expresses his creative ability in an original manner by making free and creative choices ... and thus stamps his "personal touch"'.[46] Already this definition explains that the individual data as such will not be copyright protected. This is also explicitly confirmed by Article 3(2) of the Directive, which states that copyright protection for databases will not extend to the contents as such. Hence, even if data were included in a copyrightable database, such copyright protection would not extend to that data.

46 *Sui generis* database protection may at first glance provide a better basis for protecting data generated in a world of the Internet of Things.[47] However, this form of protection also has its limitations. They arise from both the subject-matter of protection and the scope of protection.

47 As regards the subject-matter of protection, a 'database' is uniformly defined as a 'collection of

40 See Recital 4 of the General Data Protection Regulation (*supra* n 17). See also Pamela Samuelson, 'Privacy as Intellectual Property', (2000) 52 *Stanford L Rev* 1125.

41 Zech (*supra* n 24) at 60.

42 Arts 7-10 Database Directive (*supra* n 19).

43 See also Wiebe (*supra* n 25).

44 Art 3 Database Directive.

45 Art 7(1) Database Directive. Note that both forms of protection may also coincide. A given database may be both creative and based on substantial investment.

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

47 It is even argued that the sui generis database right will often protect big data databases; see Giulio Corragio, 'Big data and IoT–a great match with troubles...' (19 June 2015), available at: <http://www.medialaws.eu/big-data-and-iot-a-great-match-with-troubles/> (accessed 10 September 2016).

independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means'.[48] Protection will also be granted if the arrangement and storage is accomplished by 'electronic, electromagnetic or electro-optical processes'.[49] Hence, collections of digital data can usually be considered as databases in the sense of the Directive.[50] However, a *sui generis* database right only subsists if 'there has been qualitatively and/or quantitatively a *substantial investment* in either the *obtaining, verification or presentation of the contents*'.[51] The CJEU has interpreted these requirements in a very restrictive way. It clarified that the investment has 'to refer to the resources used to seek out existing independent materials and collect them in the database, and not to the resources used for the creation as such of independent material.'[52] The CJEU explained this with the objective of the Directive to create incentives for the making of databases and not for the creation of the data that goes into the database.[53] Hence, a distinction is to be made between the 'creation' of the materials contained in the database and the 'obtaining' of these materials.[54] This leads to the conclusion that the creation of smart products with sensors that collect data should not be considered for the assessment of whether the investment in the database was 'substantial'.[55] The same applies to big data analyses. These may well require substantial investment. However, such analyses only lead to the creation of new data in the form of knowledge, which may then be included in databases. For the protection of these databases, the investment in the big data analyses is not to be taken into account.

48 As regards the scope of protection, it is important to note that the *sui generis* database right only protects the database as a collection of data and not the individual data. The Directive thereby aims to keep the (semantic) information that can be derived from the data in the public domain.[56] Extraction and re-utilisation of individual data only fall within the scope of protection of the database if these data form a 'substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database'.[57] The concepts of 'extraction' and 're-utilisation' further restrict the scope of protection. In particular, big data analyses, whereby the 'code comes to the data' in order to generate new information, will not lead to any 'extraction' since there will be no 'permanent or temporary transfer of all or a substantial part of the contents of a database to another medium'.[58]

49 In sum, it is quite obvious that the Database Directive is based on a database technology that no longer corresponds to the use of data in an era of 'Industry 4.0' or the Internet of Things. In particular, by protecting a collection of materials for a given period of time (15 years as of the completion of the database),[59] the concept of a database is much too static to adequately respond to the features of constantly changing datasets and real-time data services.

50 This latter point may raise the question of whether the Database Directive is in need of a reform. However, the fact that the Directive does not respond to the needs of the modern data industry in a technologically appropriate manner cannot by itself justify reforming the Directive by introducing a right of data ownership. Rather, such reform is in need of an economic justification, which is part of the analysis further below (section D. below).

II. Trade secrets protection

51 Trade secrets protection is another protection regime that inevitably comes to mind as regards the protection of data.

52 The EU has recently adopted a directive for harmonising the national rules on trade secrets protection.[60] As regards the modern data industry, this Directive may already be considered as technologically out-dated, since at the time of the preparation of the Commission Proposal, the implications of the new data economy were not yet fully perceived or understood.[61] As a consequence,

48 Art 1(2) Database Directive (*supra* n 19).

49 Database Directive, Recital 13.

50 Zech (*supra* n 24) at 70.

51 Art 7(1) Database Directive (*supra* n 19) (emphasis added). This means at the outset that there may be databases fulfilling the definition of a 'database' in the sense of the Directive that, however, are not protected since they meet the requirements neither for copyright-protected databases, nor for *sui generis* databases. Confirmed by the CJEU in its Judgment in *Ryanair v PR Aviation*, C-30/14, ECLI:EU:C:2015:10, paras 35-40.

52 Judgement in *British Horseracing Board*, C-203/02, ECLI:EU:C:2004:128, [2004] ECR I-2195, para 31.

53 *Ibid*.

54 *Ibid*, para 32.

55 See also Żdanowiecki (*supra* n 10) at 21.

56 See Zech (*supra* n 24) at 71.

57 Art 7(1) Database Directive (*supra* n 19).

58 Article 7(2)(a) Database Directive.

59 Article 10(3) Database Directive only takes changes to contents of databases into account to the extent that such changes amount to a new substantial investment, which leads to a revival of protection for 15 years.

60 Directive (EU) 2016/943 of the European Parliament and the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use or disclosure, [2016] OJ L 157/1.

61 See Proposal of the Commission of 28 November 2013 for a Directive of the European Parliament and of the

the text of the Directive is rather unclear as to what extent, for instance, data produced by smart products benefit from trade secrets protection.

53 In comparison to database protection, trade secrets protection has the obvious advantage of protecting the specific information. However, there are other shortcomings:

54 Most importantly, trade secrets protection relies on rather narrowly defined requirements for the subject-matter of protection. According to Article 2(1) of the Directive, the know-how or business information (1) needs to be 'secret' in the sense that it is not 'generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question'; (2) the information must have 'commercial value' because of its secrecy; and (3) it has to be subject to 'reasonable steps ..., by the person lawfully in control of the information, to keep it secret'. None of these three requirements can be easily applied in the context of data produced by sensors attached to smart products. First, while the secrecy could be confirmed for data that is produced by the machines inside a factory, data collected by smart cars on freely accessible roads could be collected by the cars of many manufacturers and, hence, will not fulfil this requirement.[62] Second, while data may nowadays have great commercial value, it is quite questionable whether it will always be possible to establish a causal link between the secrecy of the information and its commercial value. In the context of big data analyses, an individual piece of information may appear quite trivial, but particular value may arise from correlations with other data.[63] Third, it is very unclear which steps will be required of the person in control to keep the information secret.[64] Fourth, where data is generated in a network of different entities connected through a value network, it will be particularly difficult to allocate protection to a single person controlling the secret.[65]

55 Yet another question is whether the subject-matter of protection needs to be interpreted narrowly in the light of the objectives of the Directive. The Directive pursues the goal of promoting the competitiveness and innovative strength of businesses through protecting secret information.[66] However, data are nowadays largely produced as a by-product of smart machines and goods, whereas these data can be commercialised in completely different markets and for completely different purposes (not least in the public interest). Here, data is largely used by the data holder as an asset for generating additional income. In addition, protection of the data as trade secrets will not always promote innovation through the holder of that data. Rather, the challenge will often consist in promoting access to that data for other firms and public entities that may generate additional knowledge from that data through big data analyses. This argues for making a distinction between information that serves the core business of the holder of data, such as personal data held by Internet platform operators, as the backbone of the underlying business model, as well as data generated through machine sensors that are designed to be immediately used for the production process on the one hand, and other data, which are rather a by-product of the firm's core business, on the other hand.

56 Finally, it should be noted that trade secrets protection is much narrower in scope than an exclusive data use right. It does not protect against any use of the data, but requires 'unlawful' conduct which, to summarise the different provisions of the Directive, can be regarded as contrary to honest commercial practices.[67] Hence, the Trade Secrets Directive only establishes a system of liability for specific tortious conduct and not a property rights system.[68] However, such further limited protection can be considered as better suited to serve the purposes of the data economy, by focussing on the particular way in which a third party has specifically acquired access to the data instead of granting exclusive protection against the use of data. Such exclusive property protection would easily conflict with the fundamental right of freedom of information.

III. Patent law

57 In limited sets of cases one could even consider protection based on patent law. The reason for this is that the scope of process patents also extends to 'products' that are obtained through that process. For instance, in the European Union, Article 25(c) of the—yet not effective—Agreement on the Unified

Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM(2013) 813 final. See also Wiebe (*supra* n 25) at 880 (pointing out that the drafters of the Directive did not have big data in mind).

62 In this context, it is important to note that independent discovery of the same information will not lead to unlawful acquisition of the information. See Article 1(3)(a) Trade Secrets Directive.

63 See Zech (*supra* n 24) at 63 (therefore criticising Recital 8 Trade Secrets Directive according to which trivial information should not be protected).

64 On the difficulties to keep information secret in a network environment, see Wiebe (*supra* n 25) at 880.

65 See also Wiebe (*supra* n 25) at 880.

66 See Trade Secrets Directive, Recital 1.

67 See, in particular, Art 4(2)(b) Trade Secrets Directive.

68 See also Drexl et al (*supra* n 39) at paras 18-20.

Patent Court stipulates that a process patent also provides the right to prevent a third party from 'offering, placing on the market, using, or importing or storing for those purposes a product obtained directly by a process which is the subject-matter of the patent'.

58 The question in this regard is whether 'data' can be a 'product' that is obtained by using a process patent.[69] This question would become relevant for instance where data is produced in a factory in applying a patented production method or, maybe more relevant, in the context of a process patent applied in medical diagnostics. In the latter case, the patent owner would also 'own' the 'result' of the diagnosis.

59 However, at the outset, such protection would only become relevant where the patent is used without the consent of the right-holder. Only if the patented process is used without a licence does the patent holder have a right to prohibit the commercialisation of the product as the offspring of the process.

60 The reason why the legislature extends the protection of process patents to the commercialisation of products is that process patents are much weaker than product patents. The owner of a product patent enjoys full protection against price competition from imitators in the product market. In contrast, the holder of a process patent runs the risk of having to compete with firms that offer essentially the same product manufactured with an alternative process. Extending protection to the products that are produced with the process assimilates process patents to product patents regarding the economic incentives arising from the patents. It also addresses the problem that third parties could otherwise legally serve the market with products produced abroad by applying the process if the process patent is only protected in the importing country.

61 However, already as a matter of principle, it does not seem appropriate to extend patent protection to information as the product of a process patent. Moreover, German courts seem to deny protection for information that is derived from a process patent. An interesting decision in this regard is the one by the District Court of Düsseldorf in the *Hunde-Gentest* case.[70] In this case, the process patent for a genetic test for dogs was protected in Germany, but not in Slovakia. The defendant, who previously applied the test in Germany, moved the testing to Slovakia to avoid a patent infringement. Therefore, the Court was only requested to decide whether the plaintiff can rely on a process patent to prevent the defendant from communicating the test results to Germany. The Court denied such protection, arguing that the test results as pure information cannot be considered the product of the process. The Court noted that, since information is directly accessible for humans without any further technical process, information as such lacks technicity and therefore cannot be patented. Yet the Court refrained from arguing that the 'product' of a process needs to be patentable by itself in order to be protected within the scope of the process patent.[71] Rather, the Court showed great sensitivity for the free flow of information. It rejected protection so as to avoid using patent law as a kind of trade secrets protection. In particular, the Court stressed that patent law should not support a claim to ban communication of the test result to anybody in Germany, which, in the last resort, would even include denying a person who knows about the test result entrance to German territory.

IV. Unfair competition law and similar protection regimes

62 In many jurisdictions, unfair competition laws and similar protection regimes, such as the tort of misappropriation in common law countries, may provide subsidiary means of protection against free-riding where other protection mechanisms are not available.

63 However, whether such a role should be attributed to these general principles or laws as regards the holding of data, is again a policy issue which should only be answered in the affirmative if there is sufficient economic justification for protection against free-riding (see section D. below). Free-riding as such should not be considered a violation of the law unless it undermines incentives for investment in the production of the asset that is copied.

69 On the similar issue whether patent protection for a computer-based process for producing aesthetic creations extend to these creations see Jean-Marc Delthorn, 'Councours de droits sur les œuvres numériques—Le cas des creations issues de procédés brevetés', (2016) 60 *Propriétés intellectuelles* 285.

70 *Landgericht Düsseldorf* of 16 February 2010, Case 4b 0 247/09—Hunde-Gentest, available at: <https://www3.hhu.de/duesseldorfer-archiv/?p=813> (accessed 10 September 2016). See also Oberlandesgericht München (Higher District Court Munich) of 22 October 2015, Case 6 U 4891/14, (2015) *Beck-RS* 18783.

71 This is also the view of the EPO. See EPO, Decision of the Enlarged Board of Appeals, G 1/98, Transgenic plant/NOVARTIS-II, [2000] OCJ EPO 111, at 138. The Enlarged Board of Appeals confirmed the availability of process patents, including protection of the products deriving from the process according to Art 64(2) EPC, even in a case where the product would be a plant, which is excluded from patentability under Art 53(b) EPC.

V. 'Digitisation' of the civil law concept of property?

64 Civil law countries are not unlikely to discuss nowadays whether the concept of property found in the national Civil Code, which is usually limited to the ownership of tangible items and land, should be opened, namely, in a move to 'digitise the Civil Code', to also include data. For instance, in 2016, the *Deutsche Juristentag*,[72] which is the most important private discussion forum for legal reform in Germany, bringing together law professionals from all different sectors, considered whether German civil law is in need of a 'digital up-date'.[73]

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

66 Hence, the question of whether civil law is in need of being 'updated', should be considered carefully and within the specific context of protection. To transfer the principles of contractual liability developed for the sale of tangible goods to defects of digital goods, is one thing;[74] to recognise a property right for holders of data with exclusionary effects on third parties is another thing. In Germany, the debate is mostly triggered by certain limitations of tort law. Under Section 823(1) German Civil Code, there is only a claim for damages if somebody injures the 'life, body, health, freedom, property or another right' of someone else.[75] Courts have continuously extended the range of 'other rights', to include, for instance, the general personality right, but they have also limited those rights to 'absolute rights'. This is why it is now also discussed whether courts should recognise 'data ownership' as another absolute right to protect the integrity of datasets against injuries committed by third parties. For instance, the need for such protection is quite evident when computer viruses delete large and valuable datasets, while the physical carrier and its functions remain intact. The downside of this is that recognition of such a right in the framework of Section 823(1) Civil Code would also provide for injunctive relief to prevent injury. For that purpose, German courts rely on an analogy to Section 1004 Civil Code, the basis for injunctive relief in case of unlawful interference with property.

67 Injunctive relief raises the more important question regarding the extent to which the scope of protection of such data ownership is to be assimilated to property in tangible objects. Property in tangibles basically provides two sub-rights, a right of integrity and a right to exclude others from any use.[76] The debate on data ownership is inspired by the lack of protection as regards the integrity of data, whereas the recognition of a right to exclude other persons from *any* use of the data would amount to a very powerful intellectual property right that would have the potential of undermining the free flow of information.[77] Also, from an economic standpoint, a right to exclude others from the use of data is less needed than in the case of tangibles. Data are not rivalrous; hence, someone else's use of the same data does not prevent the 'owner' from using these data. Accordingly, from an economic perspective, it is easier to justify protection of the integrity of data than to provide full protection, including injunctive relief, as regards the use of data.

68 This debate on extending the property concept to digital data was more recently also inspired by the *UsedSoft* decision of the CJEU.[78] In this case, the Court explicitly recognised 'ownership' of the person legally downloading a computer program from the Internet. However, this holding was limited to the application of the exhaustion rule in the Computer Programs Directive.[79] Exhaustion of the distribution right under copyright law requires a first 'sale' of a copy of the work through the right-holder or with her consent. The CJEU defined a 'sale' as 'an agreement by which a person, in return for payment, transfers to another person his rights of *ownership*

72 The Deutsche Juristentag convened in Essen on 13-16 September 2016.

73 The debates at the Deutsche Juristentag revolve around *Gutachten* (expert reports), which are usually prepared by law professors. The 'digital update' of the German Civil Code is assessed in the *Gutachten* by Florian Faust, *Digitale Wirtschaft—Analoges Recht—Braucht das BGB ein Update? Gutachten A zum 71. Deutschen Juristentag* (Munich: C.H. Beck, 2016), also available at: <http://static1.1.sqspcdn.com/static/f/1376130/26847040/1455040340113/Faust+Digitale+Wirtschaft+Analoges+Recht+Gutachten+fur+den+71.+DJT.PDF?token=73St8IVwwV4tYnJQSVMQJmH3F8c%3D> (accessed 10 September 2016).

74 See the Commission Proposal for a Directive (*supra* n 32).

75 English translation of the *Bürgerliches Gesetzbuch* available at: <http://www.gesetze-im-internet.de/englisch_bgb/> (accessed 10 September 2016).

76 As regards the right to exclude under German law, see Sec 903 Civil Code. On the distinction between the three different rights of property regarding data ownership, including (1) possessing data—with the possibility to exclude access—, (2) using data, and (3) destroying data (right of integrity), see Zech (*supra* n 24) 56-57.

77 See also Wiebe (*supra* n 25) at 882. (considering whether recognition of data ownership would lead to a paradigm shift in protecting information).

78 Judgment in *UsedSoft* (supra n 35).

79 See Art 4(2) Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, [2009] OJ L 111/16.

in an item of tangible or intangible property'.[80] By recognising ownership in the digital copy of the program, which is provided to a customer on a permanent basis,[81] the Court managed to transfer the concept of exhaustion to the digital field. Hence, in *UsedSoft*, the CJEU did not recognise any general concept of data ownership.[82] Rather, the Court only relied on ownership in a digital download to limit the exclusivity of the copyright as another property right. We can learn from this judgment that limited recognition of property rights can also have a liberalising effect and thereby promote the free movement of data in the digital economy. However, such recognition should not be generalised by arguing in favour of allocating ownership involving third-party effects wherever persons are legally in permanent control over the use of any data. This may well have the opposite effect of hampering the free flow of data and information in the data economy.

VI. Factual exclusivity and contract law

69 Despite the uncertainties and shortcomings of the different protection regimes, the players of the data economy do not seem to suffer from the lack of recognition of general data ownership. The reason is that markets can also develop with relatively little legal exclusivity where access can effectively be controlled by technical means.[83] Factual exclusivity has the potential of forcing parties into negotiations and can trigger transactions in very similar ways as in the case of intellectual property.

70 Such data contracts based on the factual holding of data are therefore meant to grant access to these data.[84] However, this does not exclude agreement on certain limitations of the use of data. Accordingly, contract law may exercise even stronger restrictions on the use of data than a new ownership agreement that could provide for mandatory exceptions and limitations.[85]

71 A very prominent example of an area where markets for immaterial exploitation emerge with very little legal exclusivity is the marketing of sports rights. There are only few jurisdictions which provide special intellectual property rights for the audiovisual exploitation of sporting events.[86] Other jurisdictions manage to provide the same conditions for markets for sports rights with comparable value streams without such legislation. The reason for this is that the organisers of such events can control access to the premises of the sporting events and thereby charge a price from the broadcaster that is allowed to produce the broadcast.[87] Of course, there is a risk that third parties will use the broadcasts without authorisation. However, it suffices in this regard that the broadcasting corporation that was granted access to the event is protected by its investment by copyright, or at least its original related right, in the broadcast.

72 As regards the data economy, this example of the sports rights may explain that, even where misappropriation by third parties is a concern, there is no need to recognise ownership of the data holder as long as the investor in access to the data—such as the big data analyst—disposes of an intellectual property right that prevents third-party use, such as the copyright in the software tools for analysing big data. The data holder itself will regularly be able to exclude others from access through technical means, including technical protection measures. Rules of criminal law that make unauthorised access to data a crime, such as data or computer espionage, can further strengthen factual exclusivity without recognition of ownership in the sense of private law.

D. Potential justifications for recognising data ownership

73 Against the backdrop of the uncertainties and shortcomings of existing protection regimes, we now turn to the question of whether there is an economic justification for the recognition of data ownership. In this regard, the analysis can rely on insights from intellectual property scholarship.

80 *UsedSoft* (*supra* n 35) at para 42.

81 *Ibid*, at para 45.

82 This is also confirmed by authors who rely on this judgment to argue in favour of a concept of general data ownership. See De Franceschi and Lehmann (*supra* n 9) at 60-63.

83 See also Żdanowiecki (*supra* n 10) at 25.

84 See Zech (*supra* n 24) at 59.

85 On the question whether promoting access may hence justify introduction of a data ownership see at D.V. below.

86 The most prominent example is French law. Arts L333-1 through L333-5 Sports Code (*Code du sport*) vest the sports associations with an exclusive right of audiovisual exploitation. Original French text of the *Code du sport* available at: <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071318> (accessed 10 September 2016).

87 See also Thomas Margoni, 'The Protection of Sports Events in the EU: Property, Intellectual Property, Unfair Competition and Special Forms of Protection' (2016) 47 *IIC* 386 (arguing that, in principle, the combination of the exclusivity of the sports venue and contract law is capable of making markets for sports rights work).

I. Incentives for generating and collecting data

74 The standard argument in favour of recognising intellectual property rights is based on a utilitarian incentive theory. Intellectual property is designed to promote innovation. However, the subject-matter of protection of these rights, such as inventions and works of creativity, is characterised by the features of public goods. Without the recognition of legal exclusivity, everybody else would be able to free-ride by copying and, consequently, nobody would be willing to invest in the production of such public goods.[88]

75 As demonstrated further above, the generation and collection of data allows for very new and innovative business models that lead to large gains in allocative efficiency in manufacturing and maintenance, as well as far-reaching social benefits based on big data analyses. Hence, there is a case for also fostering incentives for generating and collecting the underlying data. However, it is less clear whether, for that purpose, data ownership is required. In this regard, the incentives of different players need to be analysed.

76 There is always some human act that can be found at the very beginning of the generation of data and the commercial exploitation of these data. A manufacturer may decide to employ machines and robots that are equipped with sensors to control and steer the production process. The owner of a smart car decides where to go with this car and where the car will register data about the density of traffic or the physical conditions of the road. A patient provides the blood for a blood test, the result of which may go into datasets that are subsequently analysed. In all of these cases, the relevant person would and should certainly know about the generation of the digital data, and may even have to give her consent based on the rules on data protection. However, additional ownership in the data is not necessary as an incentive to generate such data. Hence, in principle, it is possible to conclude that there is no need to vest the person at the beginning of the value chain with exclusive rights to exploit that data as a means to create incentives for the generation of that data.

77 The same holds true for the next step of exploitation. The data produced by a smart car will be transferred to the manufacturer of that car. The car manufacturer will be sufficiently motivated to generate data that will guarantee smooth operation and maintenance of the car. Generation of that data is very much part of the firm's business model. Furthermore, the potential of follow-on markets creates sufficient incentives for collecting the data, whether database rights are available or not, even in cases where the main business model does not require the data to be stored on a permanent basis.

78 Nor are additional incentives needed as regards the business model of Internet platform operators (e.g., search engines, social media etc.), for which the collection of personal data is the very core of the success of the underlying business model. Yet the fact that firms nowadays know that, in an emerging data economy, any data may become interesting and that they may be able to commercialise that data based on factual exclusivity, it cannot be argued that there is suboptimal generation and collection of digital data. In general, data are not a scarce resource.[89] The sheer volume and variety of big data constitute the basis but also the particular challenge of big data analytics.

79 Hence, there is not sufficient evidence of the need of data ownership as justified by the incentive theory concerning the generation and collection of data. However, there could be a need for more incentives to invest in tools for technologically challenging big data analyses. Within the value stream of exploiting data, data analyses generate major social value by producing new knowledge and thereby optimise decision-making in many fields. However, although the evolving business models of big data analyses may still be in need of further research, it seems that data ownership will not be the appropriate mechanism for protecting the interest of big data analysts. Access to data held by others should be more of a concern to big data analysts than acquiring ownership in data. It is more important for big data analysts that the data they have access to respond to the challenges of velocity and veracity than having claims against third parties for unauthorised use of the data they produce. Since, in many instances, real-time data is key, data analysts do not have to be so much afraid of competitors' free-riding. What counts more is getting access to the various datasets from which they can gather new knowledge. As regards the other side of the market, namely, the firms and public entities to which big data analysts provide new knowledge for optimising decision-making, data ownership will not be needed either. Such relationships will often be based on contracts for services through which customers are supplied with accurate knowledge at a given point in time. From a competition perspective, the core question is whether data analysts need to rely on data ownership in competition with other data analysts.

88 On the public goods theory for intellectual property, see, in general, William M. Landes and Richard A Posner, *The Economic Structure of Intellectual Property Law* (Cambridge, MA and London, UK: The Belknap Press of Harvard University Press, 2003) 12-16.

89 See also Becker (*supra* n 25) at 7.

This question has to be answered in the negative. Data analysts will not gain a competitive edge by 'owning data' at the expense of their competitors. Rather, they will prevail in competition if they manage to have better access to the various sources of big data, for which they will not rely on ownership but contractual business relationships with the holders of such datasets, on the one hand, and the effectiveness and accuracy of their big data analyses, on the other hand. As regards the latter, it is more important that big data analysts control the technology for big data analysis. For this, they will rely on copyright protection in the software infrastructure and possibly technical know-how rather than data ownership.[90] The same holds true for firms that deliver—typically software-based—tools for big data analysis of other firms.

80 At the last stage, the customers to whom information is delivered based on big data analyses are not in need of data ownership either. To the extent that these data are kept secret and the data analysts are under a contractual obligation to keep that information secret, this information may enjoy trade secrets protection. Public entities as customers of big data analysis services will be less likely to have an interest in keeping the result of big data analysis secret. In the framework of emerging laws on open data, public institutions may even be under an obligation to provide access to the data both to the public and, pursuant to public-sector-information (PSI) laws, for commercial re-use by private actors.

II. Incentives for the commercialisation of data

81 Another and more modern justification for property rules is the goal of creating incentives for the commercialisation of the subject-matter of protection. In the context of patent law, this is often called the 'prospect theory'—in contrast to the traditional incentive theory, whereby the latter is designed to reward those who invest in the generation of the subject-matter for that investment.[91]

82 In general, innovation does not end with the generation of the subject-matter of protection and the acquisition of the IP right. Innovation will only serve society if it reaches the market. And quite often more investment will be needed for the commercialisation of the subject-matter of protection than for its generation.

83 A good example of this can be observed in the pharmaceutical sector. The major investment that goes into the development of drugs relates to the financing of the lengthy and risky clinical trials, which typically take place after the filing of patents. Indeed, in order to protect investment in the clinical trials against free-riding by others, the pharmaceutical company is in need of patent protection prior to making that investment. In most cases, the patent holder will also be the firm that conducts the clinical trials and brings the product to the market. However, the patent holder may also decide to license the patent to another company that, based on that licence and with the prospect of having a secured market later on, will make the investment in developing the drug.

84 Similarly, investment in the commercialisation of copyrighted works is not typically effectuated by the creator, but by the representatives of the copyright industries, such as publishers and producers. Only in countries that follow a work-made-for-hire doctrine will the latter be considered initial copyright owners, whereas in other countries they can rely on exclusive copyright licences or, at best, related (neighbouring) rights.

85 These examples show that the original right does not necessarily have to be vested in the person who makes the investment in the commercialisation. The licensing system, based on contract law and exclusive licences, can provide for the same incentives. Granting the original right at the stage of the creation of the content, however, may produce additional distributional effects. The copyright protected in favour of the creator may generate additional income for the creator, at least if there are additional rules in place that guarantee fair remuneration.

86 As regards the data economy, however, no case for recognising data ownership can be identified based on the goal of producing additional incentives for the commercialisation of the data. The major argument is that the holders of data do not have to be afraid that competitors will free-ride on investment in the commercialisation of their data. Likewise, there is not any particular risk that the data will be copied by competitors for the purpose of substituting the data holder's offer, nor does the grant of access to the data to others, such as big data analysts, involve particular investment by the data holders.

87 Nor are the big data analysts unable to recoup their investment in the commercialisation of their data

90 Against a justification of patent protection for the algorithm, see Josef Drexl et al. (*supra* n 39), paras 12-17.

91 The foundations of the prospect theory were laid by Edmund Kitch, 'The Nature and the Function of the Patent System' (1977) 20 *J L & Econ* 265. On a more modern market-related patent theory that departs from the classical reward theory, see also Daniel F Spulber, 'How Patents Provide the Foundation of the Market for Inventions' (2015) 11 *J Comp L & Econ* 271.

without data ownership. They are much more likely to rely on the control of their software solutions to protect their innovation under competitive conditions.

88 The situation is likely to be different as regards data brokers. Data brokers can play an important role in the enabling of big data analyses in particular.[92] Data brokers may also act as aggregators of datasets. Property rights have the potential of stabilising their activities. However, these brokers can also rely on factual exclusivity regarding the control of datasets that are transferred to them. Concerning situations where real-time data is key, data brokers are less likely to act as intermediaries that buy and resell identifiable datasets. They are more likely to act as agents that bring together providers of large and dynamic datasets with customers that are interested in services that build on big data analyses. Such brokers will enable direct transactions between data providers, on the one hand, and big data analysts and their customers, on the other hand. To do this, they are not in need of property rights in the data.

III. Data ownership as a means to stabilise transactions

89 Property rights can also stabilise and, thereby, facilitate transactions. Conversely, this is an effect which cannot be provided in the framework of trade secrets protection. Transactions on trade secrets suffer from major instability. Every sharing of trade secrets increases the risk that the information will ultimately become publicly available with no possibility for the holder of the trade secret to act against the re-use of that information.[93] Accordingly, recognition of data ownership is advanced as a means to facilitate trading with data as a commodity. The argument is that, even where there is factual exclusivity, without ownership there are no direct remedies against unauthorised use by third persons once the data has been disclosed.[94]

90 Yet considering the risk that business models will be undermined by unwanted free-riding in an environment in which the availability of real-time data is key, this argument of stabilising transactions will hardly ever be very convincing.

IV. Legal certainty

91 Another argument relates to legal certainty. Clear attribution of ownership can enhance legal certainty by informing the stakeholders about their rights and obligations.

92 This, however, is not very convincing as regards data ownership either. On the one hand, new property rights will always give rise to additional conflicts and litigation. At the same time, allocation of property rights may not be so clear at all. As regards data ownership that is recognised independently of factual control over data in an environment where individual data may constantly be integrated and arranged in different datasets, data ownership is more likely to reduce transparency and increase the risk of unintentional infringement of rights.

V. Ownership as a means to enhance access

93 A final potential justification for data ownership may look counterintuitive at first glance, but in particular deserves closer attention.

94 As has already been explained above in the context of the discussion of the *UsedSoft* decision of the CJEU,[95] property rights regimes can also be used as a means to enhance the free flow of data. In this decision, a limitation of copyright protection regarding digital downloads was used as a means to promote free circulation of digital copies of computer programs.

95 This example shows that general recognition of property rights can also make sense where factual exclusivity is already particularly strong. Adoption of a fully-fledged rights regime can include far-reaching mandatory exceptions and limitations that cannot be set aside by contractual restrictions.[96] For

92 See Federal Trade Commission, 'Data Brokers—A Call for Transparency and Accountability' (2014), available at: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> (accessed 12 September 2016). The business models of data brokers were however heavily criticised in the US in particular, where those brokers have contributed to the spread of personal data and provided uncontrolled access of the government to personal data. See Chris J. Hoofnagle, 'How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Enforcement' (2004) 29 *NC J Int'l L & Com Reg* 595.

93 According to Art 3(3) of the new EU Trade Secrets Directive the 'use' of trade secrets is only unlawful under rather restrictive conditions, namely, when the user has acquired the information unlawfully or is in breach of a confidentiality agreement or any other agreement on how to use the information. Once the trade secret has become known to third persons, these persons can lawfully use the information.

94 See, in particular, Zech (*supra* n 24) at 60.

95 At C.V. above.

96 See also Becker (*supra* n 25) at 9 (assuming that the industry may even refuse to claim new legislation on data ownership since such legislation could provide more access than they

instance, such exceptions and limitations can also be found in the French legislation on the exclusive right of sports associations as regards the audiovisual exploitation of sporting events.[97] Hence, such ownership systems could provide better guarantees for access than reliance on general contract law based on the unrestricted principle of freedom of contract.

96 However, this approach is not without alternatives. Access can also be guaranteed by special legislation on access that takes precedence over contractual restrictions. As regards the commercial exploitation of sporting events, such access rules can be included in the general media law. Current EU law also enhances access to information held by public bodies. Thereby, the European rules on public sector information do not have to recognise ownership of public bodies in the information they hold in order to regulate the principles that apply to the licensing of the commercial re-use of such information.[98]

97 An interesting case is also presented by the current proposal of the Commission to introduce an unwaivable exception to copyright protection for carrying out text and data mining for the purpose of scientific research.[99] This proposal seems to prove the case that exceptions promoting access to data can easily be drafted within existing ownership systems. However, separate access legislation on data mining could also be drafted by building on the model of the proposal with application beyond copyright and with regard to other interests whenever the data holder has granted access to somebody in the framework of a contractual agreement. To do this there is no need to recognise data ownership up front.

98 An additional argument against adopting ownership as a means to enhance access arises from challenges regarding the form of regulation of such exceptions or limitations. There are two approaches, both of which are problematic. The first approach consists in a general clause similar to the fair use exception of US copyright law.[100] This approach has the advantage of general applicability but the disadvantage of lack of precision. It would hence cause legal uncertainty, give rise to legal disputes and potentially favour the interests of those parties that have less of a problem to finance litigation. As regards data ownership in particular, this approach has the additional drawback that it would have to be formulated in an extremely general way in order to be adaptable to the very different sectors of the data economy. Hence, it is very doubtful whether such a 'fair use' clause would really be able to enhance access in practice.

99 The second approach would consist in formulating a precisely defined exhaustive catalogue of exceptions and limitations that takes care of specific countervailing interests. However, this would require the legislature to fully anticipate the interests of a large number of potential stakeholders in highly diverse sectors of a data economy that is only just emerging.[101] There is a clear risk that legislation on exceptions and limitations would largely be postponed to the future, while the legislature would immediately adopt a strong rights system that goes beyond the restrictions data holders can implement under contract law. In sum, this approach would entail the risk of largely hampering the free flow of information without sufficient remedies for addressing problems of access.

100 In addition, balancing conflicting interests is more difficult for the legislature, where the question of who should be the owner remains a most difficult issue.[102] Whomever the legislature singles out as the right-holder, this will produce an additional negative impact on the interests of other stakeholders and may intensify a conflict of interests. In contrast, by choosing the alternative approach of balancing factual control over data by access-only legislation, the legislature will react to the conflict as it arises from the specific context of the market without intervention.

101 In sum, it seems more advisable to prefer an approach of progressive adoption of access regimes as part of sector-specific regulation. Such an approach could still develop principles and guidelines that emerge over time and ultimately rely on general models of regulation.[103]

102 It can be thus concluded that no reasons can be identified that would argue in favour of introducing data ownership in favour of any of the stakeholders.[104]

E. Problems related to the design of the rules on data ownership

103 Since there is no clear case for introducing legislation on data ownership, the question of how to design such legislation is not even relevant. Yet,

currently are willing to provide under contract law).

97 See Arts L333-6 through L333-9 *Code du sport*.

98 See PSI Directive (*supra* n 21).

99 Art 3 Commission Proposal of 14 September 2016 for a Directive of the European Parliament and of the Council copyright in the Digital Single Market, COM(2016) 593 final.

100 See Sec 107 US Copyright Act.

101 On the many and very context-dependent stakeholders in the data economy see at B.IV. above.

102 See at E.I. below.

103 On this see at F.IV. below.

104 Also against adopting legislation on data ownership, Wiebe (*supra* n 25) at 884.

some challenges regarding such legislation should nevertheless be addressed since, in the current debate, it seems that these challenges are not sufficiently discussed[105] and, consequently, largely underestimated when the idea of data ownership is advanced.[106] There are many reasons why the design of such protections is enormously complex. Several dimensions of this problem can be identified:

I. Complexity of the legal issues

104 For any intellectual property rights system, a decision has to be made on what subject-matter is to be protected, on who should own the right, and on the scope of protection, including the exceptions and limitations. As to the latter aspect, a decision is to be made regarding the terms of protection.

105 As regards the subject-matter of protection, it has already been mentioned that the law has to decide whether data should only be protected on the syntactic or also on the semantic level. The latter should rather be avoided because of the risk of obstructing the free flow of information.[107] However, the question still remains whether data can be protected as 'raw data' on the syntactic level. This is questioned because data is in need of specification on the semantic level in order to qualify as subject-matter of protection beyond the encoding in the form of bits and bytes.[108] If, however, protection was granted on the semantic level, the very practical problem is to identify whether information is 'new'.[109] Another issue is whether data ownership should relate to individual data or datasets in their entirety. The latter would follow the example of the Database Directive with all its shortcomings, namely, that it fails to protect the individual data. Yet, if each and every individual piece of data were protected, data ownership of individual persons in a world of big data would disappear like drops of rain in the sea. Such a system would present major challenges in terms of its governance and of the enforcement of myriad individual rights, not to mention the challenges for users in the context of rights-clearing.

106 As regards potential owners, it has been shown in this analysis that in a complex world of networks where a considerable number of different players collaborate in generating value, not least by contributing their data, the allocation of data ownership is particularly difficult.[110] Furthermore, if everybody contributing to the generation of data in a value network is vested with ownership, this allocation could easily run the risk of creating too many property rights, which would block efficient exploitation of big data in particular.[111] The proposition to vest consumers with the ownership of their personal data in order to enhance trading with that data as a commodity[112] does not explain why allocating the economic value to consumers can be justified from an economic perspective.[113]

107 Moreover, the definition of the scope of protection also remains a difficult task. It is not clear at all in which situations there is a particular risk that the need for investment will be distorted by the free-riding of third parties. The proposal to limit protection to the copying of encoded information, while allowing for the re-generation of the same data,[114] would only confirm that data should not be protected on the semantic level of information.

108 The definition of the subject-matter of protection, the identification of the owner of the right and the scope of protection will be most relevant for finally identifying the need for exceptions and limitations. In the light of the large number of stakeholders, it would be particularly difficult to clearly identify the conflicting interests and to design rules for balancing these interests.

109 The interaction between all of these issues reaches an enormous level of complexity, which argues in favour of preferring legislation on access regimes to the implementation of a fully-fledged new ownership system.[115]

105 See, however, the discussion of a data producer right by Zech (*supra* n 24) at 74-78.

106 This is also true for EU Commissioner Oettinger. His idea of a 'data use right' does not explain what this right should protect, who should be the owner and how far protection should go.

107 See also Zech (*supra* n 24) at 74 (delineating his data producer right only on the syntactic level). For a review of different proposals see Wiebe (*supra* n 25) at 882.

108 Wiebe (*supra* n 25) at 883.

109 See Wiebe (supra n 25) at 882, highlighting that this requires a showing that the same information has not been stored before in form of 0s and 1s. In addition, it ought to be remembered that the same information can be represented differently on the syntactic level, for instance, in a different language or a different form (eg, a video and not a text).

110 This is considered a main counterargument against devising a property right in data according to Wiebe (*supra* n 25) at 883.

111 See also Wiebe (*supra* n 25) at 883 (against co-ownership because of the conflicting interests).

112 See, in particular, Zech (*supra* n 24) at 60.

113 This is also conceded in principle by Zech (*supra* n 24) at 69.

114 In this sense Wiebe (*supra* n 25) at 882.

115 See also discussion on adopting an ownership regime as a vehicle for promoting access through exceptions and limitations at D.V. above.

II. The one-size-fits-all issue

110 In addition, legislation on data ownership would have to respond adequately to very diverse circumstances in which data is generated and used in the future. The data economy and the use of smart products are predicted to enter all different fields of modern life. However, data collection as regards the operation of smart cars is very different from the processing of data in the healthcare sector. Whether it is possible *ex ante* to conceive uniform rules on the subject-matter of protection, the person owning the rights and the uses that will be covered by the right, while the peculiarities of different sectors are delegated to exceptions and limitations, remains rather doubtful.[116]

III. The dynamic character of the data economy

111 Several times it has been underlined in this analysis that the data economy and big data in particular, is not about stable datasets but about the 'moving target' of highly dynamic data. 'Velocity' and 'veracity' are a fundamental concern in this economy.

112 This however questions the very appropriateness of a property approach to regulating that economy. IP systems are largely based on the paradigm of protecting intangible assets, such as technologies in particular, that play a role as input in the production of physical goods. Such a paradigm does not seem to fit a world in which customers have to rely on real-time and accurate information as an input. This contradiction becomes most obvious if one addresses the issue of the terms of protection. In an environment where it is key to capture the moment and where being late leads to wrong decisions, asking the question of how long data should be protected will simply miss the needs of this economy. Rather, the starting point of any legislation should be a clear analysis of the emerging new business models and the question of what kind of protection firms need in order to make their business models successful in competition with other firms and in the overarching interest of society.

113 As a matter of principle, contract law seems to provide the better regime for such protection. It allows the parties to specifically design the rights and obligations as needed for making new business models work. Contract law provides the parties with the possibility to experiment with different arrangements over time and with the flexibility to adapt to different circumstances in very different sectors of the data economy.

116 Similar doubts are expressed by Wiebe (*supra* n 25) at 884.

F. Regulating access to data

114 However, contract law cannot be expected to make the data-driven economy work without frictions. Contract law will only work in instances where the holder of data has an economic interest in sharing the data with others and where the bargaining power of the contracting parties is equally strong. Hence, the question arises whether government and legislative action is needed to promote access.

115 From the outset, it has to be clear that a refusal to grant access by itself is not sufficient to justify intervention. In line with the rationale of trade secrets protection, such refusal should not be considered illegitimate where exclusive control over data provides firms with a competitive edge over others and, thereby, creates the necessary incentive to invest in data-based business models. This also means that the leading firms of the data economy such as Google and Facebook should not blindly be forced to share their user data, the most valuable asset they have to conduct their business.

116 Striking the balance between access to and legitimate control of data is hence a most difficult task. The field of law that first comes to mind to tackle the issue is competition law. In this regard, a more thorough analysis of competition law is needed in order to assess competition law's potential to provide a workable access regime. For this purpose and as a preliminary clarification, it is important to place competition law as a tool for enforcing access to data in the context of the current competition policy debate on big data (section F.I. below). This will be followed by an analysis of the potential application of rules of EU competition law to refusals to grant access to data (section F.II. below). This analysis will help in discussing additional actions that could enhance access to data (sections F.III. and F.IV. below).

I. The current competition law debate on big data

117 The debate and literature on how and whether competition policy should react to the advent of big data has exploded within a remarkably short period of time.[117] The discussion is mostly driven by the enormous success and expansion of firms in the digital economy such as Google or Facebook, whose business models are largely built on the control of user data. There is in fact growing awareness that control over big data should play a more prominent

117 Among the major and most recent contributions from competition law scholars are Rubinfeld and Gal (*supra* n 28); Maurice E Stucke and Allen P Grunes, *Big Data and Competition Policy* (Oxford: Oxford University Press, 2016).

role in assessing market power and dominance, not least in the framework of mergers.[118] The EU merger cases of *Google/DoubleClick*[119] and *Facebook/WhatsApp*[120] are among the first cases where control over user data in terms of 'data concentration'[121] was taken into account for assessing the effects of mergers on the online advertising market.[122] Yet in both cases the Commission held that the emerging data concentration was not sufficient to significantly impede competition in this market.[123] The growing role of data in the digital economy has also convinced competition law enforcers to further develop their policies as regards the impact of control over data on competition.[124]

118 Yet this discussion on how competition law should react to the challenges of the data economy and big data is based on a particular perspective. First, control over data is considered to be a potential competition problem. This corresponds to the general role of competition law to ban anti-competitive conduct. Second, the focus is very much on market structure, market power and dominance,[125] as well as on market entry barriers arising from the control of big data.[126] This is explained by the fact that anti-competitive effect, especially in unilateral conduct cases, depends on the ability to behave independently of the competition.

119 Within the framework of the current 'Free Flow of Data' initiative of the Commission, however, the role attributed to government is a more proactive one of industrial policy. The question is not only how to protect the free market economy against anti-competitive conduct of firms. Rather, the question is what can be done in order to promote the digital economy.

120 In this regard, competition law has certain advantages but also shortcomings. On the positive side, competition law is in principle applicable to all sectors of the economy that are currently undergoing a digital transformation. Competition law can work as a platform on which legislatures can build to formulate more targeted, sector-specific rules whenever competition law does not provide sufficient remedies. In addition, competition policy and law can also prevent the legislature from excessive intervention. In instances where there is no identifiable harm to competition, policy makers will have to look for an alternative justification for adopting access rules.

121 On the negative side, competition law is likely to be too limited to provide sufficient remedies. As regards its substantive criteria, competition law only reacts to one particular kind of market failure. Intervention is only justified where there is identifiable harm to competition. While the outer boundaries of what can be considered such harm is not at all clear, there are kinds of market failures that cannot specifically be addressed by competition law. For instance, in a world of big data analytics involving techniques of data mining by searching datasets for correlations, negotiations about access to data may simply fail because of information asymmetries regarding the value of the data.[127] From an institutional

118 See, for instance, Inge Graef, 'Market definition and market power in data: the case of online platforms' (2015) 38 *World Competition* 473.

119 Commission Decision of 11 March 2008, Case No COMP/M.4731—*Google/DoubleClick*, available at: <http://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf> (accessed 10 September 2016).

120 Commission Decision of 3 October 2014, Case No COMP/M.7217—*Facebook/WhatsApp*, paras 164-67 and 181-91, available at: <http://ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.pdf> (accessed 10 September 2016).

121 *Facebook/WhatsApp* (*supra* n 120) para 164.

122 From the perspective of the data economy, the Commission Decision of 4 September 2002, Case No COMP/M.6314—*Telefónica UK/Vodafone UK/Everything Everwhere/JV*, available at: <http://ec.europa.eu/competition/mergers/cases/decisions/m6314_20120904_20682_2898627_EN.pdf> (accessed 10 September 2016) may even be more interesting. In this case, the Commission assessed the impact of the joint venture for the introduction of an electronic payment system ('mobile wallet') on the market for data analyses.

123 In *Facebook/WhatsApp*, the Commission specifically looked at WhatsApp as a potential source of user data for better targeting Facebook's advertising activities. It finally concluded that even if Facebook implemented such a policy post-merger, it would only control a small share of user data on the Internet as a resource for online advertising. See *Facebook/WhatsApp* (*supra* n 120) paras 180-89.

124 See, in particular, the joint policy paper by of French and German competition authority: Autorité de la concurrence and Bundeskartellamt, 'Competition Law and Data' (10 May 2016), available at: <http://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2> (accessed 10 September 2016).

125 In their joint policy paper on data, the French and German competition authorities devoted the whole second half to the role of data for assessing market power. See Autorité de la concurrence and Bundeskartellamt (*supra* n 124) at 25-52.

126 See, in particular, the thorough analysis of potential barriers to entry caused by big data by Rubinfeld and Gal (*supra* n 28).

127 This is known as the 'information paradox'. Contractual negotiations on data as a commodity can easily fail because the purchaser, not knowing which information can be extracted from the data, will not be able to assess the value of the data. If, however, the data is made accessible to the prospective purchaser for solving the information problem, the purchaser will no longer be willing to pay for access. The 'information paradox' was first 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) 609. But it is also to be noted that markets can provide solutions to

perspective, competition law enforcers are able to ban identifiable anti-competitive conduct, but they are not well equipped for regulating markets *ex ante* by imposing positive rules of conduct in the form of behavioural remedies that require on-going monitoring.

122 Hence, already based on these general observations, it is very likely that actions will be needed that go beyond competition law. But competition law should be placed at the beginning of the following analysis (section F.II. below). Competition law thinking as a market-compliant approach will however also prove important for devising additional pro-competitive regimes that promote access to data (sections F.III. and F.IV. below).

II. Addressing refusals to grant access to data under EU competition law

123 EU competition law has not yet developed specific case-law on access to data in the data economy that is only now about to emerge. However, as the following analysis will show, the practice on refusals to deal and, more concretely, refusals to license can produce some indications on how to assess future data-related cases. At the outset, it should be noted that it is not important whether data to which access is requested is protected by intellectual property (IP) rights or not.[128] Even in cases in which neither IP protection nor trade secrets protection is available, but the holder of data can rely on factual exclusivity provided particularly by technological protection measures, a refusal to grant access can be captured as a refusal to deal under competition law. For the assessment of such cases, under Article 102 TFEU, the question is whether the holder of data is market dominant and whether the refusal to grant access to data constitutes an abuse. These issues will be addressed in the framework of the following review of the existing case-law.

124 The three major cases that established the foundations for assessing refusals to license, namely, *Magill*,[129] *IMS Health*[130] and *Microsoft*,[131] are all, in one way or another, 'information-related'. Beyond these three cases, the following analysis will also take into account the more recent *Huawei* case, which dealt with a refusal to license a standard-essential patent (SEP).[132]

1. The requirement of dominance

125 For cases regarding access to data in the context of the currently emerging data economy, *Magill* and *Microsoft* are most suitable precedents. In both cases, the holder of information that was indispensable for entering a downstream market refused to grant access to that information. In *Magill*, the TV stations broadcasting in the Republic of Ireland and Northern Ireland refused to grant a copyright licence for their TV listings and thereby excluded a publisher from the market who intended to offer comprehensive TV guides to consumers. *Microsoft* is perhaps an even better precedent for refusals to grant access to data because, in this case, the interoperability information for the Windows operating system as such was not freely available to the competitors in the market for work group server operating systems.[133] Yet *Magill* laid the foundations for dealing with the issue of information-based dominance. The Court convincingly stated that, due to copyright protection, the TV stations were the only source of the relevant information and that, therefore, the three TV stations had to be considered as *de facto* monopolists with regard to the information contained in their respective TV listings.[134] The situation in *Microsoft* was very similar. However, market dominance did not arise from an IP right, but from the fact that Windows, based on network effects, had emerged as a *de facto* standard in the market for operating systems, which made the

the information paradox. For instance, data analysts can be appointed as trustees to do tests on the utility of datasets for the purposes of a prospective customer to assess the value of the dataset, without providing direct access to the information contained in the datasets to this customer.

128 In the *Microsoft* case, which was on access to the interoperability information contained in the Windows program, both the Commission and the General Court (GC, former Court of First Instance) left open whether this information was IP-protected or not and applied the test developed by the Court of Justice of the EU (CJEU) for refusals to license an IP right. See Judgment in *Microsoft v. Commission*, T-201/04, ECLI:EU:T:2007:289, [2007] ECR II-3601.

129 *Magill* (*supra* n 27).

130 Judgment in *IMS Health*, C-218/01, ECLI:EU:C:2004:257, [2004] ECR I-5039.

131 *Microsoft* (*supra* n 128).

132 Judgment in *Huawei*, Case C-170/13, ECLI:EU:C:2015:477.

133 Art 6 Computer Programs Directive (supra n 79) allows for decompilation of an existing computer program where this is necessary to obtain interoperability information for the purpose of establishing interoperability for an independently created computer program. However, this exception and limitation is insufficient in a modern software environment, where the interoperability information can constantly be changed by updates. Hence, competition law may still be needed to order the dominant holder of a computer program to provide access to the interoperability information. Recital 17 of the Computer Programs Directive explicitly safeguards the applicability of EU competition law in such instances.

134 *Magill* (*supra* n 27) para 47.

interoperability information an indispensable input for offering interoperable programs that would run on Windows.

126 The two cases demonstrate that it is easiest to show dominance in data-related cases where the petitioner seeks access to concrete information that is indispensable for doing business in a market.

127 More typical for the data-driven economy are however cases in which somebody, such as a big data analyst, seeks access to large datasets for purposes of data mining. In the light of its utility, namely, to rely on statistical correlations among different pieces of information contained in larger sets of aggregated data for generating new knowledge, such datasets have to be considered a kind of resource which is distinct from concrete semantic information such as in the case of *Magill*. Yet the test of *Magill*, as an expression of general competition law principles, can be adapted to meet the challenges of cases that deal with access to large datasets to enable big data analyses. The test in both cases is whether the respective dataset can be considered the 'only source' of the resource.

128 This leads to the issue of substitutability of datasets. The fact that data are non-rivalrous and, therefore, individual data could be found in various datasets seems to count against dominance. Whether datasets are substitutable or not will depend on the concrete circumstances, including the very nature of the information contained in the data. If, for instance, a supplier of parts wants to have access to the data collected by the end manufacturer after the sale of the final product to control the quality of its parts, the end producer's datasets will indeed be the only source of that data. However, if a city is in need of information about the qualities of streets which is collected by smart cars, different car manufacturers may be able to provide access to that information through their datasets. The reason is that the latter kind of information is freely available in the public in the first place, and, hence, can be duplicated in the datasets of any other data collector. Publicly accessible information is by nature non-rivalrous[135] and can therefore be registered by anybody in a digital format.

129 Yet assessing dominance in a world of big datasets by using the concept of substitutability remains a most difficult task, since even the petitioner for access, such as a big data analyst, will often only have a vague understanding about the kind of data contained in the dataset and about which data will produce the most valuable new information based on observable correlations.

130 However, larger collections of data will generally guarantee a higher level of accuracy of the new information, since such information derived from correlations of data within such datasets is based on statistical likelihood. Hence, just as in the case of multisided platform markets, the collection of datasets for the purpose of enabling big data analysis may exercise particular network effects and enhance market power of the firm that controls access to the larger dataset.[136] The same may occur in the case of data-sharing platforms. An example of such a platform is provided by the joint venture of the three German car manufacturers, Daimler, BMW and Audi, that acquired Nokia's digital map HERE as an important element of their systems for autonomous driving. For instance, such digital platforms could be used for collecting and exchanging real-time information about the weather conditions of roads. The quality and reliability of such an information-sharing platform would obviously increase with the number of cars contributing information to this system. Accordingly, the three car manufacturers should have a strong self-interest in convincing other car manufacturers to join the system.[137] At the same time, this may tip the market and give rise to market dominance of the joint venture.

2. The four requirements for abuse according to Magill and IMS Health

131 The two cases of *Magill* and *IMS Health* have established the European test for assessing whether a refusal to license constitutes an abuse. In *IMS Health* this test was phrased as one with three cumulative conditions, which, however, contained the additional underlying condition that the resource to which access is sought be indispensable for conducting a business.[138] In *Microsoft*, the General Court rephrased this test in a better and more structured way.[139] According to the Court, the following four conditions for a refusal to license need to be fulfilled in order to present 'exceptional circumstances' for considering the refusal an abuse:

135 The character of non-rivalry of data is also highlighted by Autorité de la concurrence and Bundeskartellamt (*supra* n 124) 36-37.

136 See also Rubinfeld and Gal (*supra* n 28) at 42.

137 Indeed, when the *Bundeskartellamt*, the German competition agency, cleared the acquisition under German merger control law, it specifically considered that other car manufacturers would not be excluded from participating in the system. See Bundeskartellamt, 'BMW, Daimler and Audi can acquire Nokia's HERE mapping service' (6 October 2015), available at: <http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2015/06_10_2015_HERE.html?nn=3591568> (accessed 10 September 2016).

138 *IMS Health* (*supra* n 130) para 38.

139 *Microsoft* (*supra* n 128) para 332.

(1) *The refusal relates to a product or service that is indispensable to the exercise of a particular business in a related (secondary) market;*

(2) *The refusal excludes effective competition in that related market;*

(3) *The refusal prevents the emergence of a new product for which there is consumer demand;*

(4) *The refusal is not objectively justified.*

132 In applying these conditions to refusals to grant access to data and larger datasets in particular, several issues arise:

133 First, as regards the indispensability requirement, a problem arises when data relate to information that it is publicly accessible but can only be found in a digital format in the datasets of one undertaking. Since registration and digitisation makes the information retrievable and treatable, including for purposes of big data analysis, the digital data should be considered a product with added value that differs from the original, publicly accessible information. Accordingly, the holder of the digital data in such a situation can indeed be considered a monopolist and, hence, a potential addressee of Article 102 TFEU. However, this does not automatically mean that the data is also 'indispensable' in the *Magill/IMS Health* sense, since anybody else including the petitioner could also register the same information in a digital format.

134 For understanding the concept of indispensability, the judgment in *Bronner* is most relevant; although the case did not deal with access to data but access to a nationwide home delivery scheme for newspapers. According to the CJEU in this case, access to a resource of a competitor cannot be considered indispensable if there are no 'technical, legal or even economic obstacles capable of making it impossible, or even unreasonably difficult' to duplicate the resource.[140] Thereby, the Court showed reluctance to accept the argument of lack of economic viability too easily. The Court stressed that it is not enough to show that duplication of the resource would not be economically viable against the benchmark of the petitioner's scope of business in the secondary market.[141] Rather, the question is whether it is economically viable to create the resource 'for production on a scale comparable to that of the undertaking which controls the existing product or service'.[142]

135 This seems to indicate an objective standard for indispensability that does not depend on the size of the petitioner's business and that imposes on the petitioner the burden to make the same investment as the one made by the dominant undertaking. Regarding cases on refusal to grant access to data, this may well mean that indispensability cannot be argued where the information as such is freely accessible and it is only a matter of registering the data in a digital form. On the other hand, it would be easier to argue indispensability where data is generated through business models that are characterised by strong network effects such as search engines and Internet platforms like the HERE data-sharing system described above. The possibility to duplicate similarly large and valuable datasets is excluded by the economic characteristics of these markets.[143]

136 Second, the requirement of excluding competition in a secondary market qualifies the European rule on refusal to licence as one, which is based on a leveraging and exclusion theory. This presupposes that the dominant firm is also active as a competitor in the secondary market. This, however, will frequently not be the case when firms refuse access to data. It is a typical feature of the new data economy that data is collected for one purpose, such as enabling predictive maintenance services, but turns out to be interesting for very different purposes pursued by other firms of a very different sector and even the government. In such instances, the European rule on refusals to license and refusals to deal, as developed in the abovementioned case-law, would not apply.

137 More recently, in the *Huawei* judgment, the CJEU clearly indicated that the 'cumulative' *Magill/IMS Health* conditions are not the only 'exceptional circumstances' to make a refusal to license an abuse. the CJEU accepted that exceptional circumstances are also present in the case of a refusal to license an SEP if (1) the standard was fixed by a standardisation body[144] in return for which (2) the patent holder has irrevocably committed to license on fair, reasonable and non-discriminatory (FRAND) terms.[145] Since the Court did not reiterate the condition of exclusion of competition in a secondary market as part of the description of these exceptional circumstances, the question may be asked whether a refusal to license or a refusal to deal can also be considered abusive if the dominant firm is not vertically integrated. However, the *Huawei* decision itself presents many uncertainties in this regard, because the Court in its reasoning still indicates that harm to competition

140 Judgment in *Bronner*, C-7/97, ECLI:EU:C:1998:569, [1998] ECR I-7791, para 44.

141 *Ibid*, para 45.

142 As rephrased in *IMS Health* (*supra* n 130) para 28, with reference to *Bronner* (*supra* n 140) para 46.

143 This problem of 'access to data', though not in the context of the indispensability test, is also addressed by Autorité de la concurrence and Bundeskartellamt (*supra* n 124) at 38.

144 *Huawei* (*supra* n. 132) para. 49.

145 *Ibid*, para 51.

is conceived as harm through exclusion of a competitor in a downstream market. In particular, the Court reasoned that 'the fact that the patent has obtained SEP status means that its proprietor can prevent products manufactured by competitors from appearing or remaining on the market and, thereby, reserve to itself the manufacture of the products in question'.[146] From this, one could conclude that exclusion of competitors in a secondary market also remains a requirement in SEP cases. This would indeed be correct if one accepted the conservative approach to competition law, according to which competition law can only promote innovation indirectly, namely, only in cases in which there is identifiable harm to competition through exclusion.[147] In contrast, the Commission also argued a violation of Article 102 TFEU in the *Rambus* case against a non-vertically integrated SEP holder who tried to extract excessive royalty rates from the implementers in a case of patent ambush.[148]

138 This debate, however, may not be very relevant for cases on access to data. The reasons for this are twofold. First, those cases do not involve SEPs related to standards adopted by a standardisation body. Hence, the alternative 'exceptional circumstances' accepted in *Huawei* will not apply. Second, the alternative, dealing with refusals to grant access to data by non-vertically integrated data holders as a pure case of exploitative abuse in the form of excessive pricing under Article 102 lit. a) TFEU, would turn competition law enforcers into general price regulators. Fulfilling such a role would particularly be difficult in cases on access to data in which the parties also encounter major information problems as regards the economic value of data contained in large datasets. Accordingly, it is very unlikely that a claim of abuse of market dominance will be successful in a case where access to data is sought and the holder of those data is not a competitor of the petitioner in the secondary market in which the petitioner wants to use those data. This would exclude reliance on competition law in two very important sets of cases. The first case concerns big data analysts who seek access to data for purposes of data mining. The holders of such data will typically not be active as competitors in the market of providing new information generated through big data analyses. The second case regards cases where the government seeks access to data in the public interest. In such cases, a secondary market is missing in the first place, since the government will not make use of that data as an undertaking in the sense of EU competition law.

139 Third, the question is whether the requirement of the prevention of a new product (so-called 'new product' rule) also applies to cases of a refusal to grant access to data. According to the General Court in *Microsoft*, this is an additional requirement that only applies to cases involving the refusal to license an intellectual property right, but not to general refusal-to-deal cases.[149] As demonstrated further above,[150] it is very unlikely that data are already protected by intellectual property rights. The judgment in *Magill*, where access to the relevant information was controlled by a copyright, can only be explained by the very low standards of copyrightability under the British and Irish copyright case-law of that time, which most likely can no longer be maintained against the backdrop of more recent copyright decisions of the CJEU.[151] To the extent that there is trade secrets protection, the question is still left unanswered by the European Courts whether the test on refusals to license an IP right would also apply.[152] Yet if the European legislature decided to create a new intellectual property right in data, this may well make it more difficult to control access to data based on European competition law since, then, there should be less doubt as to whether the additional requirement of the prevention of a new product applies.

146 *Ibid*, para 52.

147 This is indeed the approach advocated by Pablo Ibáñez Colomo, 'Restrictions on Innovation in EU Competition Law' = LSE Law, Society and Economy Working Papers 22/2015 (2015), available at: <http://ssrn.com/abstract=2699395> (accessed 14 May 2016).

148 Commitments Decision of the Commission 9 December 2009, Case COMP/38.636—*Rambus*, available at: <http://ec.europa.eu/competition/antitrust/cases/dec_docs/38636/38636_1203_1.pdf> (accessed 10 September 2016). The Commission's approach is supported by Josef Drexl, 'Innovation as a Parameter of Innovation and its Implication for Competition Law Application', Paper presented at the 11th ASCOLA conference (30 June 2016) (forthcoming) (in favour of protecting dynamic innovation competition beyond cases involving exclusion).

149 *Microsoft* (supra n 128) para 334.

150 At C. above.

151 The CJEU requires that there be scope for the author to make 'free and creative choices', by way of which the author 'stamps the work created with his personal touch'. See Judgment in *Football Association Premier League and Others*, C403/08 and C429/08, ECLI:EU:C:2011:631, [2011] ECR I9083, para. 98; Judgment in *Painer*, ECLI:EU:C:2011:798, [2011] ECR I12533, paras 89 and 92; Judgment in *Football Dataco v Yahoo! UK* (*supra* n 46) para 38.

152 In 2005, under the impression of the *Microsoft* case, the Commission argued that applying the standard developed for refusals to license an IP right 'may not be appropriate' in cases on a refusal to grant access to interoperability information that is protected as a trade secret. See Commission, 'DG Competition discussion paper on the application of Article 82 of the Treaty to exclusionary abuses' (December 2005), available at: <http://ec.europa.eu/competition/antitrust/art82/discpaper2005.pdf> (accessed 10 September 2016). For arguments in favour of such a distinction see Gintarė Surblytė, *The Refusal to Disclose Trade Secrets as an Abuse of Market Dominance—Microsoft and Beyond* (Berne: Staempfli, 2011) 173-210.

140 More specifically, in the context of the data-driven economy, many complex issues would arise in applying the new-product rule. From the outset, it is to be remembered that this rule presupposes that both the data holder and the petitioner for access are competitors in the same secondary market. Only under this condition does the question make sense whether the petitioner for access would offer a 'new' product as compared to the product of the dominant firm. In cases on access to data, the product offered by the entity that seeks access to data can be enormously diverse. If it is about use of the data by big data analysts, the new product will consist of new knowledge or information, which may then be offered in a secondary information market. How to apply the concept of a 'new product' in relation to different information is rather unclear. To argue that the information produced by the petitioner differs from that produced by the data holder may seem convincing at first glance. However, this is less clear in the light of the rationale of the new-product rule, which is based on a balancing of the interest in protecting competition with the interest in protecting the intellectual property right. Accordingly, the new-product rule was devised to guarantee that the IP right, which is meant to promote innovation, can only be restricted if the petitioner for the licence is also an innovator.[153] However, whether the generation of (any) new information can be considered innovation, remains rather doubtful. Of course, data may also be used to offer diverse goods and services in secondary markets. Access to data may especially lead to the improvement of goods and services. Yet it is not settled whether any improvement of a product can be considered a 'new' product. In *Microsoft*, the General Court seemed to argue this way by pointing out that, according to Art 102 lit. b) TFEU, there is not only an abuse when the dominant undertaking limits production, but also in the case of a limitation of 'technical development' to the prejudice of consumers.[154] It is to be noted that the new-product rule would also exclude application of competition law to public entities that seek access to data in the public interest where these entities do not engage in any economic activity in the sense of the concept of an undertaking under EU competition law.

141 Fourth, as regards potential justifications, it is still very unclear whether and what kind of efficiencies can be considered in the framework of an efficiency defence in cases of a refusal to grant access to data.[155]

153 See *IMS Health* (*supra* n 130) paras 48-49.

154 See *Microsoft* (*supra* n 128) para 648.

155 See only Stucke and Grunes (*supra* n 117) ch 19 (at 302-12) on 'data-driven efficiency claims' (however with a particular focus on the efficiency defence in merger control law).

142 In sum, the analysis of the case-law on refusals to licence under EU competition law produces a number of limitations und uncertainties.The requirement to show market dominance based on control over larger datasets presents particular challenges for assessing whether different datasets can be considered as substitutes. The case-law so far can only be applied with certainty to vertically integrated data holders, while, in many instances, the petitioners for access and the data holder will not be competitors in any markets. The case-law will not provide any remedy when government bodies seek access to data in the public interest. The rule on exploitative abuse (Article 102 lit. a) TFEU) will hardly fill the gap since it would require competition law enforcers to act as price regulators where it is extremely difficult for the parties themselves to assess the value of data. Hence, this analysis highlights the shortcomings and uncertainties of the current state of competition law to provide adequate remedies against refusals to grant access to data in the data-driven economy.

3. Access to indispensable tools for data treatment

143 The analysis so far has concentrated on access where data or whole datasets are an indispensable input. However, the European case-law on refusals to license has more to offer.

144 In *IMS Health*, the CJEU used the *Magill* judgment as a template for assessing a case that nevertheless presented very distinct features.[156] The reason for doing this was that an intellectual property right, namely, a copyright protecting a database, was at stake and this made *IMS Health* a refusal-to-license case similar to *Magill*.

145 As a precedent for cases relating to the data-driven economy, it should however be noted that the subject-matter of copyright protection in *IMS Health* was characterised by a particular functionality. The so-called 1860-brick structure, representing a map of Germany subdivided into 1860 geographical sectors, was used as a tool for collecting and treating data on the sale of drugs. IMS Health was dominant in the service market for the collection of sales data to assist the pharmaceutical companies in designing their marketing activities. A smaller competitor encountered major problems entering the market with its own 'structure' since the pharmaceutical companies refused to work with a different structure. The reason for this was that IMS Health's brick structure had emerged as a *de facto* standard in the industry, which led the smaller competitor to simply use the 1860-brick structure; this competitor was

156 *IMS Health* (*supra* n 130).

then sued by IMS Health for copyright infringement in Germany. In this context, the question arose whether the defendant could rely on a competition-law defence.

146 By only looking at the fact that the brick structure was protected by copyright law, the CJEU missed the point that the case was indeed one on *de facto* standardisation regarding the tools used in the relevant service market for collecting data. Therefore, the distinction between two related markets, the upstream licensing market and the downstream product market, as well as the application of the leveraging theory based on an extension of market dominance from the upstream to the downstream market, appears rather formalistic.

147 As regards cases on access to data, *IMS Health* produces the particular insight that the tools for treating data have a tendency to emerge as *de facto* standards since they allow data to be communicated between the different market participants involved at the different levels of the value chain of treating and analysing data. Use of the same tools in the industry will produce positive network effects. On the downside, *de facto* standardisation will create access problems regarding the use of these tools. These tools will regularly be software-based and hence protected by copyright law. Market participants that are not allowed to use these tools will encounter difficulties to enter the market for the treatment of such data.

148 The *IMS Health* judgment would directly apply to such cases. From a competition policy perspective, the CJEU should have given more weight to the fact that the IP right controlled access to a standard with a foreclosure effect on competitors. This places cases such as *IMS Health* in between *Magill* and *Huawei*.[157] The question in such cases is whether the new-product requirement makes sense in the first place.[158] Also in *Huawei*, the CJEU did not require the prevention of a new product for considering the refusal an abuse.

149 Of course, the better option would be to promote standard-setting through standard-setting bodies and licensing of such standards regarding the tools for data treatment on FRAND terms. To the extent that such standards will emerge, the *Huawei* judgment would become directly relevant.

157 *Huawei* (*supra* n. 132).

158 This has already been questioned by Josef Drexl, 'Intellectual Property and Antitrust Law. IMS Health and Trinko—Antitrust Placebo for Consumers Instead of Sound Economics in Refusal-to-Deal Cases' (2004) 35 *IIC* 788.

4. Learning from the judgment in Huawei

150 Indeed, the judgment in *Huawei* can also provide inspiration for dealing with cases on access to data. As regards SEPs, the problem is that patent holders enter into a FRAND commitment *vis-à-vis* the standard-setting organisation (SSO) when the patents are notified as standard-essential, but later no agreement can be reached between the patent owner and the standard implementer on the concrete royalty rate. Such disputes are prone to being affected by strategic behaviour by either party of the licensing negotiations. Since rights-clearing is enormously difficult in the telecommunications industry, which is characterised by several thousands of declared SEPs held by multiple right-holders, to require users to wait with implementation until they have cleared all rights would considerably delay implementation of the standard in the industry. At the same time, the FRAND declaration creates a legitimate expectation that the licence will be granted. However, once the user has started to implement the standard by producing standard-compliant goods, the SEP holder may try to extract excessive royalty rates by challenging the implementers with claims for injunctive relief (so-called 'patent hold-up'). Conversely, if injunctive relief is not granted at all, implementers can be tempted to reject any licence offer as non-FRAND-compliant so as to avoid any payment (so-called 'patent hold-out'). In order to strike a balance of interest, in *Huawei*, the CJEU devised a framework for negotiations that includes duties of both parties,[159] and this may help the parties reach an agreement without having to call upon the courts or arbitration tribunals to make a decision on the appropriate royalty rate.

151 In a data-related access dispute, one of the major difficulties may be that the parties are not easily able to agree on price. Hence, devising a negotiation framework for the parties similar to *Huawei* may assist the parties to reach an agreement. Such schemes could be implemented through private institutions—by way of private ordering—or through state regulation. This leads the analysis to the design of additional legislative measures to promote access.

III. Access regimes for existing contractual relations

152 As regards access regulation, a distinction can be made as to whether the parties already entertain a contractual relationship or not. Problems of access to data may also arise within existing contracts. The typical justification for legislative

159 *Huawei* (*supra* n. 132) paras 60-68.

intervention in contractual relations beyond the realm of competition law is unequal distribution of bargaining power.

153 Unequal bargaining power is addressed by different parts of the law. In particular, the EU has adopted such rules on consumer contract law in the form of the Directive on Unfair Contract Terms.[160] The Directive's scope of application is broad enough to also control standard contract terms on the treatment of data. However, there are also particular shortcomings. First, the Directive's general clause on unfair terms does not provide any guidance on how to assess clauses that relate to the collection and use of data. The indicative list of unfair contract terms in the Annex to the Directive does not respond at all to the modern challenges of a data economy. Second, since the application of the Directive is limited to consumer contracts, it fails to create a European legal framework for addressing the regulation of access to data in B2B cases.

154 However, as regards both B2C and B2B relations, there are alternative ways to address cases of unequal distribution of bargaining power.

155 As regards consumers, there is a considerable overlap of consumer law with data protection law. The rule on data portability in Article 20 of the General Data Protection Regulation[161] can rather be considered as one of consumer protection than of data protection. While the relevant data covered by Article 20 is personal data as protected by the Regulation in general, the purpose of the data portability provision is not to protect the individual's moral interests. Rather, the rule is designed as an access rule that will enable the individual to switch to other suppliers where access to the data is crucial for competition to work.[162] The German *Monopolkommission*, which, as a commission of competition experts, fulfils an advisory role to the German government, supported the right to data portability by stressing that it has the potential to help the individual overcome a lock-in effect[163] and to react to the problem that businesses, without ownership regulation in place, often claim control over personal data as part of their contractual arrangements.[164]

156 This rule was inspired by the situation of platforms, including social platforms that rely on user data. Yet it will prove particularly effective in the context of new data-driven business models built on the collection of data. For instance, car insurance companies have already begun to lower premiums of customers who accept digital registration of their driving habits.[165] The possibility to switch to another insurance company will be considerably enhanced by the possibility to use such data to prove that the customer is indeed a careful driver.

157 Since this rule on data portability constitutes a most suitable form of pro-competitive regulation, there is no reason why the right to data portability should be limited to personal data.[166] The lock-in effect is not necessarily restricted to such data.[167] Beyond consumer contracts, a lock-in problem can also arise with regard to industrial data where suppliers want to take data with them concerning the quality and longevity of their parts after the termination of the supply contract with the manufacturer of the final product. Hence, data portability rules should also be considered for industrial relations.

158 Yet use of access to data as regards the relationship between suppliers and an end producer could also be addressed as part of specific competition

160 Council Directive 93/13/EEC of 5 April 1993 on unfair contract terms in consumer contracts, [1993] OJ L 95/29.

161 General Data Protection Regulation (*supra* n 17).

162 The pro-competitive character of this provision was specifically highlighted and praised prior to the adoption of the Regulation by the German Monopolkommisson (Monopolies Commission) in its Special Report of 2015. See Monopolkommission, 'Competition Policy: The Challenge of Digital Markets', Special Report No. 68 (2015) paras S15, S37 and S105, available at: <http://www.monopolkommission.de/images/PDF/SG/s68_fulltext_eng.pdf> (accessed 10 September 2016).

163 *Ibid*, at para S105.

164 *Ibid*, at para S106.

165 On this see, for instance, Adam Tanner, 'Data Monitoring Saves Some People Money On Car Insurance, But Some Will Pay More' (2 September 2013), available at: <http://www.forbes.com/sites/adamtanner/2013/08/14/data-monitoring-saves-some-people-money-on-car-insurance-but-some-will-pay-more/#7bc2c423264a> (accessed 10 September 2016).

166 The French Parliament has just adopted a provision on data portability that builds on Art 20 General Data Protection Regulation (*supra* n 16) in Art L 224-42 of the *Code de la consommation* (Consumer Act) through the so-called *Loi Lemaire* (*Loi pour une République numérique*; Law for a digital Republic). The law was adopted by the *Assemblée nationale* on 20 July 2016 and finally approved by the French Senate on 28 September 2016; available at: <https://www.senat.fr/leg/tas15-131.html> (accessed 30 September 2016). See comments on Art 12 in the English Explanatory Memorandum, available at: <https://www.republique-numerique.fr/pages/digital-republic-bill-rationale> (accessed 10 September 2016).

167 Indeed, the new French portability rule is not limited to personal data. The new Art L 244-43-3 of the Code de la Consommation (Consumer Code), as amended by the *Loi pour une République numérique*, seems to apply to any data provided by a consumer. However, the rule is also more restricted than the General Data Protection Regulation in that it only applies where data are provided to an online service communication service provider (*fournisseur d'un service de communication au public en ligne*). This rule seems to apply to social platforms in particular, but not necessarily to a car insurance company, as in the example mentioned above.

law regulation. Regulation of supply traditionally forms part of the Block Exemption Regulation in the Motor Vehicle Sector.[168] In times of the advent of autonomous driving, a modernised regulation could also address the treatment of data on the functioning of the vehicle between the supplier of parts and the manufacturer of the vehicle. There is a particular risk that the latter, by relying on superior purchaser power, will implement contract terms on data treatment concerning parts that disadvantage the supplier. The question will be how to implement such rules within the framework of the Regulation. While the Regulation will continue to build on the market-share approach as a basis for the block exemption, restrictions regarding the access of data to the disadvantage of the supplier, including a restriction on data portability, could be included in the black list of hard-core restrictions. However, for formulating such a rule, precision is needed in order to clearly delimit the non-exempted clauses from those that can be exempted. In particular, one could imagine a rule that a supply contract cannot be exempted if it does not include a rule on free-of-charge data-sharing with the supplier concerning the functioning of the parts delivered by the supplier. Such a rule is justified by the fact that both parties belong to the same network that contributes to the generation of economic value.[169]

159 Of course, the issue of access to data by a supplier of parts is not specific to the motor vehicle industry. Hence, the Commission should consider creating a generally applicable access regime in favour of suppliers in the framework of its block exemption regulations.

160 Finally, the legislature is free to draft targeted rules that would ban contractual restrictions on the use of data under particular circumstances. The already mentioned Commission's proposal for an un-waivable copyright exception for text and data mining for purposes of scientific research provides such an example, which could be extended beyond the realm of copyright and applied for other purposes.[170] In this regard, Article 3(1) Commission Proposal for a Directive on Copyright in the Digital Single Market requires that a research organisation wanting to conduct text or data mining have legal access—typically based on a copyright licence—to the relevant subject-matter.

168 Commission Regulation (EU) No. 461/2010 of 27 May 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted Practices in the motor vehicle sector, [2010] OJ 129/52.

169 On the new paradigm of 'value networks' see at B.III. above.

170 See at n 99 above.

IV. Access regimes outside of existing contractual relations

161 Regimes for access to data outside of existing contractual relations are more difficult to devise. In this field, a more cautious approach is needed in order to avoid excessive intervention in the market economy. In addition, the particularities of very different sectors where data is currently starting to play a major role in generating economic value from the outset seems to argue against a regime of general applicability. On the other hand, designing regimes for access to data is not an unprecedented exercise for legislatures. Existing models can be considered and discussed for cautious generalisations and potential transfer to other sets of cases.

162 In any event, devising access regimes outside of existing contractual relations depends on using certain criteria to balance the interests involved between exclusivity and access. Such criteria can be discussed as the kind of information contained in data, the identity of the data holder and the business model through which it generates data and, finally, the person or entity seeking access and the kind of use this petitioner is intending.

1. Kinds of information

163 As regards the kind of information contained in data, a first distinction could be made between information access to which is in the public interest—such as information that helps to fight infectious diseases—and other information in which there is only a commercial interest. Such a distinction, however, is very difficult to make, since information that seems commercial at first glance may still help the state to make decisions in the public interest. Hence, as regards 'public interest data', it is better to address this issue further below in the framework of the discussion of who is seeking access to data and for which purpose the data will be used.

164 Yet there are examples where access to information is promoted by specific legislative means based on the nature of the information. This is the case in particular as regards scientific information contained in publications. Access to such information is often controlled by academic publishers who seek an exclusive licence also with regard to the digital exploitation of the publications. In contrast, governments increasingly promote open-access publications. The tools used in this regard can be very diverse.[171] One approach consists of setting

171 As regards the European open access policy see Commission Recommendation of 17 July 2012 on access to and

financial incentives. In instances where the scientific information is the result of government-funded research, a commitment to open-access publication of the recipient can be made a requirement for the grant decision.[172]

165 Furthermore, open-access regimes can also be promoted through copyright law. In Germany, the legislature recently adopted a so-called 'secondary publication right', which vests the author with an un-waivable right to make the work available online after an embargo period of 12 months if the publication is the result of research activity that is at least 50 per cent publicly funded and provided that the second publication does not serve any commercial purpose.[173] The French legislature has just introduced similar legislation as part of its '*Loi Lemaire*' (*Loi pour une République numérique*).[174]

166 Such a secondary publication right is characterised by making use of the interest—namely, in reputation—of one stakeholder, namely, the author, to promote open access against the interests of another stakeholder, namely, the publisher. In doing so it indirectly benefits users, who get unrestricted benefits. Hence, this model has the advantage of promoting open access much more effectively than by requiring each and every user to claim access. This model could be transferred to other sets of cases where there is conflict of interest between two parties contributing to the information and where one party in contrast to the other is interested in open access. One such case regards libraries and other cultural heritage institutions that cooperate with private businesses such as Google in the digitisation of their public domain materials and works. While the private partner would usually be interested in exclusive exploitation, the cultural heritage institution will typically prefer open access.[175]

167 It is also to be noted that particular access features of the secondary publication right are also shared by the data portability rule of Article 20 Basic Data Protection Regulation (see section F.III. above). Moreover, in the latter case, two persons contributing to the collection and generation of digital data have opposing views on access of third parties to the data. In both cases, the law strengthens the rights of the person in favour of access, which will indirectly benefit third parties. From this perspective, these rules can be qualified as enacting partial, pro-access property rights. The legislature refrains from creating an exclusive ownership right relating to personal data under the Basic Data Protection Regulation that would allow the owner to prevent third parties from using those data,[176] but still promotes access of third parties based on the rights of the person from which the data originate. The un-waivable right is limited to the right to make the data available to third parties. In this context, also the recognition of copyright exhaustion for downloads of computer programs by the CJEU in the *UsedSoft* case comes to mind.[177] In this case, 'access' in form of tradability of the programs was enhanced by recognising ownership in the digital of the program downloaded by the licensee.

2. The data holder and its business model

168 Another distinction can be made concerning who holds the data and what business models they use. Access can be promoted by legal regimes that focus on particular groups of data holders.

169 Legislatures can in particular promote access to data where data is held by public institutions as part of an open-data policy. At the EU level, the Public Sector Information (PSI) Directive of 2003, in its revised version of 2013,[178] provides an evolving approach for the EU to overcome resistance among public bodies in the Member States to make data more accessible to the private sector.

170 As part of the *Loi pour une République numérique*, the French legislature has just taken further steps to make data more broadly available by going beyond public institutions. The Law adopts the concept of 'data in the general interest' to expand the open-data policy to private entities such as public service concession holders or entities that receive state

preservation of scientific information, C(2012) 4890 final.

172 This is also the policy applied by the EU within its Horizon 2020 research funding programme. See European Commission, 'H2020 Programme—Guidelines on Open Access to Scientific Publications and Research Data in Horizon 2020', Version 3.1 (25 August 2016), available at: <http://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/oa_pilot/h2020-hi-oa-pilot-guide_en.pdf> (accessed 10 September 2016).

173 Sec 48(3) German Copyright Act (entry into effect on 1 January 2014).

174 See Art 17 *Loi pour une République numérique* (*supra* n. 166); see also comments on Art 9 in the English Explanatory Memorandum (*supra* n. 166). The French provision however provides for an embargo period of 24 months, instead of 12 months, for publications in the human and social sciences.

175 In this context, see also Art 11(2a) of the PSI Directive (*supra* n 21). As regards public-private partnerships of cultural institutions with private entities for the digitisation of cultural resources, this provision limits the grant of an exclusive license for the re-use of the digitised version to 10 years.

176 Similarly, the un-waivable secondary publication right does not prevent the author from granting an exclusive licence covering the publication right to the publisher.

177 *UsedSoft* (*supra* n 35).

178 PSI Directive (*supra* n 21).

subsidies.[179] In the first case, the concession holder is under an obligation to provide all data collected in the framework of the concession to the public authority in a digital format. In the second case, the recipient of the subsidy is under an obligation to provide all essential data as stipulated by the grant agreement in a digital, reusable and exploitable format to the authority.

171 In all of these instances, the state appears either as the source, or as an intermediary for making data available to the public. However, the more difficult question is whether such access rights can also be devised with regard to fully independent private data holders. In this instance, for any access regime, a fundamental distinction could be made according to the features of the business model the data holder applies. In the first case, the creation of a dataset is only a by-product, and the commercialisation of the data in downstream data markets is not part of the main business of that entity. This is the case, for example, where a car manufacturer collects geographic data through the cars' sensors for the purpose of predictive maintenance, but other firms or the state would be interested in getting access to that data. In such cases, the private entity may anyhow be willing to grant access in order to generate additional income, but the parties may still be unable to agree on access due to information problems. Intervention in the form of access regimes that provide for a framework of negotiations, mediation and arbitration will not reduce in any way the data holder's incentives to generate the data.

172 The situation is however very different in the second case, where the collection of the data constitutes a key element of the business model in competition with other firms. Examples are in particular the business models of search engines or social platforms, such as Facebook, which build on the control of user data to compete more effectively in the market for online advertising. Access regimes should not facilitate access of weaker competitors to data where control over such data constitutes the most valuable asset for competition.

173 The same argument applies to the tools for collecting and processing information, in particular as regards big data analytics, since these tools are of crucial importance for the commercial success of big data analysts. However, where such tools become the standard for collecting and processing information, as explained above,[180] access regimes may be justifiable also from the perspective of sound competition policy.

179 Arts 10 and 11 *Loi pour une République numérique* (*supra* n 166).

180 At F.II.3 above.

3. The person seeking access and the intended use of the data

174 In particular, access to data is justifiable where public entities seek access for the fulfilment of tasks in the public interest. In the light of the large benefits deriving from big data analytics, which could help optimise public policies and decisions of the state in many regards, this sub-category for which access regimes could be implemented seems most important.[181] Such regimes could be implemented at the different levels of government through sector-specific regulation. Sector-specific regulation appears as the road to take, since the security interests of the state will most likely need different rules than the prevention of infectious diseases, the protection of the environment or the functioning of smart cities or traffic control systems.

175 As explained above,[182] this is a field in which the competition rules on refusal to deal will hardly be able to promote access.

176 Going yet a step further, access based on public interest does not have to be limited to public entities as petitioners of access. An example of an access regime in the public interest providing for access to data in favour of even competitors is provided by the REACH Regulation.[183]

177 This Regulation has the objective of ensuring 'a high level of protection of human health and the environment, including the promotion of alternative methods for assessment of hazards of substances, as well as the free circulation of substances on the internal market (...)'.[184] To enable the assessment of these hazards, the Regulation's registration provisions require manufacturers and importers to generate data on the substances they manufacture or import. To meet these obligations the manufacturers and importers have to submit a dossier that contains the relevant information to the European Chemicals Agency (ECHA). Registered substances are allowed to circulate within the internal market.[185]

181 See in this context in particular the study of OECD (*supra* n 5).

182 At F.II.2 above.

183 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, [2007] OJ L 304/1; consolidated version available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02006R1907-20150601&from=EN> (accessed 10 September 2016).

184 Art 1(1) REACH Regulation.

185 Recital 19 REACH Regulation.

178 Such assessment of hazards may also require the manufacturers or importers to conduct new tests.[186] Tests may include animal testing.[187] But the REACH Regulation tries to avoid testing with vertebrate animals by recourse to alternative test methods wherever possible.[188] As part of the regulatory framework for preparing and submitting a registration, Articles 27 and 30 REACH Regulation implement a scheme for information sharing that pursues the particular objective of avoiding animal testing.[189] More concretely, the potential registrant is under an obligation to request a sharing of information from previous registrants as holders of studies, whether these studies include tests with vertebrate animals or not. Thereby, the Regulation also takes into account the interest of the previous registrant in fair compensation for the testing it has already undertaken.[190] For that latter purpose, the owner of the existing study has to determine the costs of sharing the information in a 'fair, transparent and non-discriminatory way'.[191] Under this scheme, the parties are expected to enter into an information-sharing agreement.[192] In case such an agreement cannot be reached, the REACH Regulation provides for default rules. The potential registrant can inform the ECHA about the failure to reach an agreement.[193] Then, within one month, the ECHA gives the potential registrant permission to refer to the information requested in its dossier, provided that it has paid the previous registrant a share of the cost incurred. At the same time, the Regulation confirms the right of the previous registrant to claim a proportionate share of the cost. This amounts to an equal share of the cost if the previous registrant makes the full study report available to the potential registrant. This right of equal cost sharing is enforceable before the national courts.[194]

179 In sum, the REACH Regulation builds on particular features that could be used as guidance for similar legislation in other fields. First, a duty to share information is formulated against the backdrop of a particular public interest in avoiding the duplication of the generation of information. In this context, it is important to remember that, in contrast, the rules on refusal to deal under EU competition law following the CJEU's *Bronner* judgment do not exempt the petitioner from making the same investment as the holder of the essential facility.[195] Hence, the REACH Regulation facilitates access to information beyond the remedies available under competition law. Second, the subject-matter of access consists in identifiable information similar to the competition law cases in *Magill* or *Microsoft*. However, it is to be discussed whether this model could also be applied to cases where somebody seeks access to large datasets for the purpose of undertaking big data analyses or engaging in data mining. It seems that, to the extent that there is a particular public interest in obtaining access, such broader access regimes are also justifiable. Third, the REACH Regulation relies on a framework of contractual negotiations. It thereby favours a pro-market solution over direct government intervention. The detailed rules of the REACH Regulation are very context-specific; but the negotiation framework could be adapted to other sector-specific circumstances. Fourth, the data-sharing agreement also requires agreement on the price or compensation to be paid for the sharing of information. The REACH Regulation thereby relies on concepts that resemble the FRAND concept as used in particular by standard-setting organisations in their IP policies concerning SEPs.[196] However, the REACH Regulation is more concrete about the base for calculating the compensation, relying on the cost for undertaking the relevant study.[197] Fifth, a negotiation-based access regime will only work where the law offers a default rule 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. This default rule also has to include procedures of judicial enforcement through state courts or arbitration tribunals in case no agreement can be reached.[198]

186 Recital 26 REACH Regulation.

187 Such testing has to be conducted in conformity with Council Directive 86/609/EEC of 24 November 1986 on the approximation of laws, regulations and administrative provisions of the Member States regarding the protection of animals used for experimental and other scientific purposes, [1986] OJ L 358/1.

188 Recital 47 REACH Regulation.

189 See also Recital 49 REACH Regulation.

190 Recital 50 and 51 REACH Regulation.

191 Arts 27(3) and 30(1)(2) REACH Regulation.

192 More concrete rules on the standards of negotiations are contained in the Commission Implementing Regulation (EU) 2016/9 of 5 January 2016 on joint submission of data and data-sharing in accordance with Regulation (EC) 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), [2016] OJ L 3/41.

193 Art 27(5) REACH Regulation.

194 Arts 27(6) and 30(3) REACH Regulation.

195 See at F.II.2. above.

196 FRAND licensing is considered as a general solution to overcome barriers to entry by Rubinfeld and Gal (*supra* n 28) at 37.

197 In contrast, R&D costs are not an appropriate standard for calculating the value of a patent. There is agreement to the extent that the royalty base should relate to price of the product in which the technology is implemented. However, there is disagreement as to whether the royalty should be calculated as a percentage of the often very complex end product, or as a percentage of the smallest salable unit.

198 Note that the default rule is very weak in the case of SEPs for which the patent holder has committed to FRAND licensing. The problem here is that the default rule is not based on statutory rules but private ordering through the IP polices

180 The question may still be whether and to what extent an access regime like the one contained in the REACH Regulation could also be implemented for cases in which there is no additional public interest. Indeed, such an access regime would make sense if it is devised as a non-mandatory procedural framework for negotiations on access to information. For designing such a general framework, it would be wise to assess the effectiveness of models such as the REACH Regulation or the most recent experience with the negotiation framework devised by the CJEU in *Huawei* for the case of SEPs. Such schemes could especially be applicable for cases in which the holder of information publicly commits to grant access to data on FRAND terms. It is yet another question whether such a scheme should be implemented by the EU or national legislatures, or by way of private ordering, in particular through industry associations that provide for commercial arbitration. The European Union could cooperate with the latter institutions to promote such non-mandatory arbitration on access disputes.

G. Conclusion

181 This article shows that existing EU rules, as regards both protection of data holders and access to data based on EU competition law, are applicable in principle to the data economy. However, in particular the rules of the Database Directive, the brand-new Trade Secrets Directive, and EU competition law, present considerable uncertainties as regards their application to the data economy. These uncertainties cannot be expected to be clarified quickly by the European Courts.

182 Yet, although the Trade Secrets Directive was not drafted to meet the needs of the data economy, trade secrets protection can provide a sound approach to protecting firms in the data economy to some extent. Rather than recognising exclusive control over any use of protected information, as would be typical for intellectual property regimes, EU trade secrets law implements a tort law approach that bans specific conduct related to the acquisition, dissemination and use of trade secrets that can be considered as unfair. It is thereby better suited to balance the interest in protection and in free flow of information than the property approach.

183 While a clarification of the scope of trade secrets protection regarding data as it is collected and used in the data economy would certainly be welcomed, the analysis shows that there is no case for creating a new system of data ownership. Apart from the fact that the key issues to be addressed—namely, regarding the subject-matter of protection, the identity of the data owner, and the scope of protection—are of enormous complexity, the analysis does not produce any evidence for a need or an economic justification for such legislation. In principle, in the data economy, no incentives are needed for generating and commercialising data. Data holders are able to charge a price for making data available to third parties based on factual control over data, supported by technical protection measures.

184 Hence, the question remains as to whether there is a need for legislation on access. In principle, the legislature could also promote access through un-waivable exceptions and limitation as part of a comprehensive legislation of data ownership. However, this article favours stand-alone access regimes. This latter approach better suits the dynamic development of the data economy, which most likely will only gradually inform the legislature about impediments to access while business models develop. In contrast, immediate adoption of an integrated ownership system would result in general recognition of exclusive control, whereas unfounded trust in adequate operation of a fair-use provision or postponing legislation on targeted exceptions and limitations would fail to address the additional limitations on the free flow of information generated by new data ownership.

185 In principle, access can also be sought under EU competition law. However, this law shows considerable shortcomings as regards the data economy: first, the requirement of market dominance in Article 102 TFEU considerably limits the scope of application of this rule and requires an often burdensome assessment. Second, it is quite uncertain to what extent Article 102 TFEU can be applied in cases in which, as will be frequently be the case, the data holder is not competing with potential customers in downstream data-related markets. Of course, Article 102 TFEU can also be relied upon to remedy excessive pricing. However, competition law enforcers can hardly be expected to act as price regulators in the data economy, which is characterised by information problems and huge uncertainties regarding the value of data. This puts the state as a frequent end user of data services in a particularly uncomfortable situation. Where the state has to rely on access to privately held data and big data analyses to optimise its decisions for fulfilling tasks in the public interest, it does not act as an undertaking in the sense of competition law and,

of standard-setting organisations. To bring more precision to the concept of what FRAND actually means may raise competition concerns in the sense of an anti-competitive price agreement. Hence, the default rule is ultimately in need of judicial interpretation of the FRAND concept by courts. Hence, FRAND licensing of SEPs does not provide a perfect model for regimes to enhance access to data.

hence, the rules on refusals to deal based on theories of exclusion and leveraging of market dominance by vertically integrated firms will not apply from the outset.

186 Yet the state, including the legislature, could promote access to data in a pro-active and pro-competitive way. Where different stake-holders contribute to the generation of data and information and only some of these contributors are interested in promoting access, the legislature can decide to particularly vest these persons with rights to enforce access against the interests of the other stakeholders. Examples of this are the secondary publication right of authors of scientific publications and data portability rights. The latter can enhance competition where factual control of other parties creates a lock-in effect. Block exemption regulations can take care of conflicts over access to data between suppliers and end producers. The state can promote access as part of its funding policy and even when granting subsidies. More importantly, there is a case for implementing sector-specific access regimes in the public interest. While it is hard to conceive a general legal framework for access of the state to data in the public interest, progressive sector-specific legislation in diverse fields of law, including environmental law, public health law, medicinal law or road traffic law, can develop models for access regimes over time.

187 Public-interest considerations can also play a role where private parties seek access to information. European competition law sets a rather high threshold for a duty of a dominant firm to share an essential resource by requiring the person seeking access to make at least the same investment in duplicating the resource that was made by the holder of the facility. There is a case for access regimes below this threshold where additional public interests, such as in the case of producing data through animal testing or clinical trials with human beings, or the interest in promoting scientific research, argues against duplication of already available data.

188 A main barrier of access is uncertainty about the information contained in large datasets, the new information that can be drawn from existing data through data mining and big data analytics and, hence, the value of data and the appropriate price to be paid for access. The so-called information paradox makes it particularly difficult to agree on the price of access to information in contractual negotiations. Access regimes should address this issue by favouring a consensus-based approach to regulating prices. Where pubic interest or competition law justifies access, a cost-based approach to assessing the royalty rates seems most appropriate.

189 As regards access negotiations between private parties, the Commission could support schemes of private ordering that enable private initiatives to pool data of multiple data holders.[199] The Commission could also cooperate with institutions that have experience with arbitration to build up schemes for mediating negotiations on data licensing.

190 The functioning of the data economy will also depend on the interoperability of digital formats and the tools of data collecting and processing.[200] The relevant tools have to rely on interoperability and, hence, the markets for such tools will typically be characterised by network effects. In this regard, the Commission can cooperate and support industry initiatives for standardisation of these tools, whereby those initiatives should also develop disciplines that promote access to the standardised tools. Accordingly, these needs of the data economy should also be taken into account as part of the Commission's competition policy regarding standardisation agreements. The Guidelines on Horizontal Co-operation Agreements already recognise the principle that standard-setting organisations should require participants to commit to license their IP rights in the standard on FRAND terms in order to make the standard broadly accessible.[201] This approach is superior to *de facto* standardisation, not only because it will enhance quick and general data sharing based on interoperability of data across borders and across sectors,[202] but also in the light of the fact that EU competition law has so far not developed appropriate disciplines through its case-law on refusals to license regarding the access problems arising from *de facto* standards.

199 This also has a competition law connotation, as demonstrated by the rules on information sharing in the Communication from the Commission—Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, [2011] OJ C 11/1, paras 55-110.

200 See the standardisation issues regarding data and big data analysis mentioned in Communication from the Commission—ICT Standardisation Priorities for the Digital Single Market (19 April 2016), COM(2016) 176 final, p. 9.

201 Horizontal Cooperation Guidelines (*supra* n 199) para 285.

202 Commission Communication on ICT Standardisation Priorities (*supra* n 200) at 9.

From Cyberpunk to Regulation

Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law

by **Krzysztof Garstka***

Abstract: Every new medium through which information can be communicated is likely to bring new challenges for the established data protection laws and paradigms. In the light of progressing research aimed at deciphering the human brain, this article seeks to analyse the General Data Protection Regulation's ability to respond to the possible appearance of memory digitisation technology. To this end, the article draws on the fictional setting of a PC game entitled Remember Me, where such a technology was developed and embraced by the society. In an exploratory analysis, the GDPR's definitions of personal and sensitive data are tested regarding their ability to remain "technology-neutral" in the face of an information technology capable of identifying individuals in unique and unprecedented ways. The article confirms the Regulation's preliminary potential to accommodate the studied invention and proposes an interpretation of the corresponding articles of the GDPR, aimed at the adequate protection of data subjects.

Keywords: Personal Data; Sensitive Data; General Data Protection Regulation; Digitised Memories; Sensen

Recommended citation: Krzysztof Garstka, From Cyberpunk to Regulation – Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law, 8 (2017) JIPITEC 293 para 1.

A. Introduction

1 The General Data Protection Regulation (GDPR)[1] was adopted on the 27th of April 2016, over twenty years after its predecessor, the Data Protection Directive (DPD).[2] One may wonder whether this lengthy legislative gap is based on the premise that during the last two decades, there were not many changes in the technological realm regulated by those two instruments. This is certainly not the case, as the opposite occurred. The more plausible explanation is one put forth by Bygrave, who wrote that the legislative process leading to the enactment of the DPD "took over five years and was subject to hefty debate and frenetic lobbying"[3], characteristics he

* PhD, LLM, LLB. Information Governance Research Associate at the Centre for Intellectual Property and Information Law, Faculty of Law, University of Cambridge; member of the Trinity Hall.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Bygrave L, *Data Privacy Law: An International Perspective* (2014) OUP, at p. 6.

also found in the development process of the GDPR and other data protection instruments. Undoubtedly, this area of law can be seen as very volatile and one in which achieving consensus on regulatory steps might take many years.

2 Consequently, it seems that the GDPR is going to be the main data protection instrument in the EU for quite a while, maybe for another twenty years. Hence, it is particularly crucial to turn the academic attention in its direction, in order to assess the likelihood of Regulation's success as a key regulatory response to the vast array of data protection challenges faced, currently and in the future, by Europe's information society.

3 It goes without saying that the immediately valuable and required writing in this field should focus on the technological *status quo*; and indeed, multiple academics approached the GDPR from this angle.[4] Nevertheless, from the perspective of IT law scholarship, it might be worth occasionally looking towards certain selected visions of the future. After all, multiple technological developments of the digital age - which posed new, considerable regulatory challenges, catching the established legal frameworks by surprise - were predicted in science-fiction literature and cinematography.[5] Cyberspace itself – which continues to create new challenges of the discussed kind – is a term coined in a 1980s short story *Burning Chrome*, written by probably the most appropriate author to be referred to in this paragraph, William Gibson. In his works, the network in question is already omnipresent in society, much like and beyond what it is today.

4 Among the various genres of science-fiction, the one represented by Gibson is probably the most deserving of IT lawyers' attention. This genre is called cyberpunk, and revolves around the visions of a not-so-distant, dystopian, urban future where technology permeates every aspect of human life (not necessarily making it better) and where corporations hold much of the real power in the world. The impact of information technology on both society and the individual often plays a key, underlying role in many cyberpunk novels.

5 This is where this article takes a second detour towards the unconventional. Instead of reaching out to a cyberpunk novel or short story, the creative work chosen to shed a futuristic light on the GDPR is actually a video game. Its title is *Remember Me*, and it was developed and released by Dontnod Entertainment in 2013. Following the protagonist "memory hunter" Nilin, the game paints a vivid and sophisticated image of a world in which human memories can be digitised; and through this image, explores a plethora of social, economic, cultural and personal consequences of the said invention. As it will be seen, the nature of those consequences (described in a latter section of this piece) brings data protection issues to mind almost instantly, and prompts the question of whether the GDPR would be able to accommodate the arrival of memory digitisation technology.

6 It is a question which might be even more deserving of attention if certain current directions of scientific research are taken into account. For example, a team of researchers from Harvard Medical School used fMRI (functional magnetic resonance imaging) to discover how our hippocampus "replays experiences during quiet rest periods", and how such experiences are prioritised.[6] A group of US and Japanese scientists recently discovered how long-term memories are created and stored in mammal brains,[7] and Facebook is intensely attempting to create the technology which could detect what we say silently in our heads.[8] While direct memory digitisation has not yet appeared (especially not in the way it did in the world of *Remember Me*), there is a growing body of research consciously or unconsciously approaching this invention.

7 Consequently, it can be stated that this exploratory piece can be seen as aimed at two symbiotic, mutually supportive goals. Firstly, it seeks to test the degree to which the GDPR is technology neutral, by pitting it against a novel, strongly disruptive technology. Secondly, the article strives to begin the search for an appropriate regulatory response to the potential invention of memory digitisation, a search conducted within the realm of EU data protection law – where the GDPR is the key, flagship instrument. Hence, while the discussed technology would be certain to bring a host of regulatory challenges to multiple branches of law and legal instruments, the article focuses on

4 See e.g. Vanberg AD and Unver MB, 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' (2017) EJLT 8(1), at p. 1; Bolognini L and Bistolfi C, 'Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation' (2017) C.L.S. Rev. 33(2), pp. 171-181; or Kornbeck J, 'Transferring athletes' personal data from the EU to third countries for anti-doping purposes: applying Recital 112 GDPR in the post-Schrems era' (2016) I.D.P.L. 6(4), pp. 291-298.

5 Though there were of course many failed predictions of this kind – at the time of writing, we haven't colonised Mars, flying cars do not fill the city skylines, and aliens have not emerged from the outer space (probably due to the fear of being non-compliant with the GDPR).

6 See <https://www.biorxiv.org/content/early/2017/08/06/173021> (last accessed on October 12th, 2017).

7 See <http://science.sciencemag.org/content/356/6333/73> (last accessed on October 12th, 2017).

8 See <https://techcrunch.com/2017/04/19/facebook-brain-interface/> (last accessed on October 12th, 2017).

data protection matters. Conversely, while GDPR's degree of technological neutrality could be explored with multiple, as of yet fictional technologies (such as swapping bodies, teleporting, or uploading one's consciousness online), this article is focused on *Remember Me's* memory digitisation technology, which by itself provides a wide array of relevant legal challenges. The two adopted research aims are strongly intertwined, and lead the article to adopt the following structure. Section B describes in detail the game world's memory digitisation technology (called Sensen), as well as its applications in the city of Neo-Paris (where action takes place). Section C introduces the GDPR and analyses the first crucial challenges, which the Sensen technology would bring in front of this key legislative instrument. Section D concludes the article with a preliminary suggestion that digital memories could indeed be accommodated within the scope of the Regulation.

B. Sensen technology and the world of Remember Me

I. Introducing the world and the invention

8 Some of the readers who are less familiar with the state and variety of modern PC games might be asking themselves at this point, how is the author going to extract a sufficient amount of useful, relevant information from a PC game? After all, it is not a book, where information is laid out in written phrases, in an approachable format, ready to be used by researchers. The response to this concern is that many contemporary games, especially those with a role-playing component, developed a conceptual and storytelling depth which might be compared to that of the more conventional literary works. It suffices to mention that the script for Witcher 3 (a major role-playing PC game, winner of multiple Game of the Year awards) amounted to 450,000 words, roughly four times more than the average novel.[9] And given that the budget for gaming productions can reach truly colossal levels (Grand Theft Auto V's amounted to $250 millions[10]), one could expect that a sufficient part of this money reaches script writers, who are then able to create – for the relevant titles – worlds, stories, characters and dialogues of correspondingly high quality and robustness. Moreover, the interactive element of games might facilitate understanding certain concepts, from a different (not necessarily better, of course) angle than when they are presented in the books. *Remember Me* provides the player (or researcher) with a lot of material – not only through dialogues and general interactions with the denizens of Neo-Paris, but also through a range of Mnesists, "memory journals" found in-game, which provide ample information on the historical, technological, sociological and cultural background of the game world. As it will be shown, the game contains more than enough information for the purposes of this article, which relies on particular Mnesists as direct points of reference.[11]

9 Onto the storyline background - the year is 2084, in a bustling city of Neo-Paris,[12] which arose on the ruins of old Paris, destroyed during the war. The city revitalisation process progressed in parallel to the development and implementation of the Sensen - an invention based on a brain implant (connected directly to the spinal cord),[13] which isolates the human memories from the "hard drive" of the human brain and allows the user to perform a range of activities on his or her memories. First of all, the implant enables the *storage* of memories on external hard drives. Just like with normal digital files, a person can choose to store the copy of a memory, or move the original from the brain to the digital drive. Secondly, with Sensen, memories can be *shared* – either directly, between the two users, or by uploading a memory and sharing it through a network of choice. Thirdly, memories can be *erased* – a person may choose to isolate a specific memory and delete it, again, either directly from the brain or from the external hard drive. Finally, human memories can be *hacked* – while this possibility was not initially predicted by the Memorize corporation (in-game entity, whose main product is the Sensen implant),[14] the holes in Sensen's security were soon

9 See <https://www.pcgamesn.com/the-witcher-3-wild-hunt/the-script-for-the-witcher-3-has-over-over-450000-words-4x-larger-than-the-average-novel> (last accessed on October 12th, 2017).

10 See <http://www.ibtimes.com/gta-5-costs-265-million-develop-market-making-it-most-expensive-video-game-ever-produced-report> (last accessed on October 12th, 2017).

11 As not every reader wishing to consult the mnesists might have the time and will to look for them in the game, the following Wiki page gathers all in-game mnesists: <http://dontnodentertainment.wikia.com/wiki/List_of_Mnesist_Memories_in_Remember_Me> (last accessed on October 12th, 2017).

12 It is quite an interesting coincidence, that a game raising such potent matters of data protection was developed and located in France, a country with a very well-established data protection framework and a proactive approach, seen, for example, by requesting Google to implement nominative deindexing on a global scale – see the judgement in *Google Inc v CNIL* (2017) Conseil d'État, Section du contentieux, 10ème – 9ème ch. réunies, décision du 19 juillet 2017.

13 Mnesist – First Sensen Prototype. It has to be mentioned here that the game does not clarify whether each Sensen is connected to Internet/another central hub all the time – what would have very significant implications, including for data protection law and obligations.

14 Mnesist – Sensen 6: Response to the Memo Criminals.

discovered, allowing not only for the extraction, but also for *changing* or *remixing* the very content of human memories.

II. Sensen's applications

10 In the world of *Remember Me*, the technological possibilities outlined above have been realised in a myriad of ways. For the purpose of this section, they are divided on personal, commercial, state, and criminal uses.

11 Among the personal uses of Sensen by the citizens of Neo-Paris, three stand out in particular. The first and most popular one is backing up memories. A range of memory banks appeared, and their users may store memories there, for any future uses.[15] The second personal use, which was demonstrated in-game is sharing of memories, either between physically proximate users (e.g. family members, lovers, friends),[16] or with others, for example through the use of next-generation social networks. For the third and final example, some citizens embraced the practice of removing memories from their brains, as a way of reinventing themselves.[17]

12 The commercial applications of Sensen are quite evident in the world of *Remember Me*. Apart from the memory banks and next-generation social media platforms, the best example of a new business relying on memory digitisation are the operators of secondary markets for memories, where people can sell their own memories and buy those which were created in others' minds.[18] The most striking demonstration of this "commercialisation of memories" takes place when Nilin, the protagonist, is passing by a vending machine with memories and witnessing a man buy a memory of (someone else's!) first kiss, like a can of coke.

13 As the game plot centres on the Memorize corporation, there is comparatively less information on the use of Sensen technology by public bodies. However, the two examples which do appear in *Remember Me* are definitely noteworthy. The first one is tied to the prison authorities and the prison system *per se*. On arrival to La Bastille, Neo-Paris' main prison, the inmates are deprived of nearly all their memories – these are returned upon the completion of a sentence.[19] Apart from the punitive element, this is supposed to decrease the likelihood of escapes, the assumption being that someone who hardly knows who they are is unlikely to possess the will to attempt a break-out. The second use covered in this section is related to the military sector. According to one of the Mnesist journal entries, a practice emerged within the military, of wiping the traumatic memories from soldiers' brains in order to avoid Post-Traumatic Stress Disorder (PTSD). This process is supposed to have been automated and occur almost immediately, with a backup copy of the memory being nonetheless retained for later review by military officials.[20]

14 The final, potentially criminal dimension of Sensen's use (or misuse) is focused on hacking into the user's memories, for the purpose of extracting or changing them. This practice is the domain of freelancers, also known as the memory hunters – Nilin, the protagonist, being one of them.[21] On one occasion, she alters the memory of a dispute between a man and his wife, so that the man is convinced that he killed his wife at the end of the argument, which ultimately leads to his suicide.

15 These are the key uses of Sensen encountered during the course of the game; the scope of this technology's potential application is of course much wider. It is enough to mention the impact it could have on the sector of state and commercial surveillance and monitoring, making the PRISM system publicised by Edward Snowden[22] look like a harmless database of gherkin sales. Not to mention the revolution which Sensen would trigger within the sector of Big Data analytics.[23]

16 For the final point in this section, it is worth underlining how prevalent Sensen became in the world of *Remember Me*. Practically everyone has the implant plugged in, and those without it (either due to lack of funds or the will to embrace the Sensen) have virtually become second-class citizens.[24] An in-game Mnesist aptly compares this situation to that of social networks in the early 21st century;[25] and it could be added that the similar development might be currently occurring with regards to smartphones or digital literacy in general, for example within older age groups.

15 Mnesist – First Civilian Application.

16 Memorize commercial/game trailer - <https://www.youtube.com/watch?v=Aij7dNUHQ9M> (last accessed on October 12th, 2017).

17 Mnesist – First Civilian Application.

18 Mnesist – Globalization.

19 Mnesist – La Bastille.

20 Mnesist – First Military Application.

21 Mnesist – Hunt Glove.

22 See <http://www.bbc.co.uk/news/world-us-canada-23123964> (last accessed on October 12th, 2017).

23 A term denoting a high computing power-supported search for factual connections and patterns within large datasets.

24 Mnesist - Globalization of Sensen.

25 Mnesist - Globalization of Sensen.

C. General Data Protection Regulation applied to Sensen technology

17 Should the Sensen technology come to appear in the real, non-virtual world, it would certainly be capable of improving and positively revolutionising various aspects of human life. However, it would be similarly certain that such a development would carry a myriad of new regulatory challenges. Among them, those pertaining to the field of data protection would be one of the first ones begging for adequate, balanced, and comprehensive answers – can GDPR, in its current state, be seen as capable of providing those? How far is this instrument "technology-neutral" – as the regulatory keyword goes – towards the new formats of information that may contain personal data?

18 In order to fully answer these questions, a wide array of challenging, demanding research inquiries would have to be conducted. This paper approaches the questions which would arguably have to be answered first – the ones concerning the classification of Sensen memories as personal and/or sensitive data within the definitions of arts. 4 and 9, respectively, of the GDPR. The said definitions stand as gateways to the realm of rights and obligations aiming to protect the (personal) data subjects. Rights such as the right of access to information (art. 15), the right to rectification (art. 16), or the right to erasure (art. 17), data processing obligations based on principles established in art. 6, would, together with all other relevant provisions, be enabled only if the digitised memories were to be found as lying within the definition of art. 4, and in case of certain stronger protection measures, within that of art. 9. GDPR's veil of protection against the negative consequences of Sensen uses described above (such as inadequate commercialisation of data, or novel security threats, to mention the very first few) would hinge on those preliminary questions – hence, it is most fitting to dedicate this article to such a path of inquiry.[26]

19 One additional disclaimer has to be made; while considering the indicated definitions from the perspective of secondary "memory subjects" (ie. those who appear in someone else's memories) would be a very interesting endeavour, this article – due to its exploratory character – focuses its analysis on the primary memory subjects, that is those whose brain created the later digitised memory.

26 This is without denying that multiple subsequent legal dilemmas would be requiring academic attention, such as the application of the domestic purposes exception, set out in art. 2(c) of the GDPR, (as supported by rec. 18), the distinction between the "right to be forgotten" and the "right to forget yourself in the context of Sensen, and the shape of exemptions for detecting and preventing crime.

I. Digitised memories as personal data

20 The preliminary question approached by this paper is whether digitised memories, as presented in the world of *Remember Me*, could be classified as personal data at all. Art. 4(1) of the Regulation defines the latter concept as "any information relating to an identified or identifiable natural person". The notion of identifiability is of key importance in this sentence, and hence, it is necessary to consider whether a human memory could be seen as being related to an identified or identifiable individual. According to recital 26 of the GDPR, when considering this matter, "account should be taken of *all the means reasonably likely to be used*,[27] such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." While the definition emerging from art. 4(1) and recital 26 is a broad and open one, the first provision offers a list made of two groups of factors which, if present, would tip the scale towards the fulfilment of the discussed criterion.

21 The first group of factors contains specific forms of identification, starting with the individual's name. A Sensen memory file, which would be labelled with such a name would pass the test in a straight-forward manner. However, if such a label would be missing or adequately anonymised, the more interesting dimension of this inquiry begins. The content of the memory itself could contain an individual's name – the memory might include someone hearing his name spoken, it might include someone typing his name into an online form, it might even include someone *thinking* his name, or being sufficiently conscious of it, so that an external party accessing this memory through their Sensen could tell that it is a memory of someone bearing the name in question.

22 The second factor from the first group is an identification number. Like an individual's name, it could appear as a label attached to the memory file; but it could also appear within the memory itself. For example, this could be a memory of someone completing their tax paperwork, or looking at their ID or driving licence when perusing through their wallet. However, there would arguably be a lower presumed chance of such presence than in the case of an individual's name, which is more often found in everyday, casual use.

27 (Emphasis added). The recital offers further guidance with regards to the reasonability criteria in this sentence - "To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". GDPR, supra fn. 2, rec. 26.

23 The next factor indicated in the provision is location data. Apart from metadata,[28] which could be tied to the memory (e.g. which brick and mortar memory bank was used to deposit the memory), the potential for identifying an individual by location-related information present in the memory can be seen as particularly high, even when we merely consider the visual dimension. Seeing one's home, place of work, or favourite pub can already give a good indication of who the person is – and if that information is combined with additional sources of data; for example, land registries or direct inquiries, the probability is quite high indeed. Certainly, it is possible to imagine a memory of someone in a locked, indistinctive room, staring at a blank wall, not thinking about anything; but this would in all likelihood be an exception.

24 The last identifier from the first group of factors is an "online identifier". Apart from labels, such as a next generation social media account name, or a memory bank account name, there would be a low, yet possible likelihood of this criterion being fulfilled – imagine someone's memory of playing an online game, which requires creating a dedicated account or a virtual character, imagine this person looking at his character's/account's name, receiving chat messages addressed to his online name. Out of the four factors from the first group, it seems plausible to state that name and location data would most likely be present in memory files, followed by online identifiers, and, finally, identification numbers. Of course, this is an estimate based on the idea of information present in an average person's memories – there could very well exist individuals escaping this prediction due to the uniqueness of certain aspects of their lives.

25 The second group of factors indicated in art. 4(1) is less focused on specific forms of identification, and more on various broader aspects of one's identity. The first such aspect which, if present, can serve as a factor turning a piece of information into personal data is labelled as physical identity. Setting aside any supplementary descriptions of a memory file (e.g. "memory of a male, height - 185 cm, weight - 80kg"), its content would almost always disclose information of the discussed kind. Firstly, it could be due to visual information – imagine someone looking at himself/herself in a mirror, looking at their own hands while doing something, or looking at their clothes in the morning. Such a mode of identification could be seen as supported by Article 29 Working Party's *Opinion 02/2012 on facial recognition in online and mobile services*, which stated that "when a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data".[29] The Opinion indicates that several parameters ought to be considered in order to verify whether data falls within such a case, such as quality of the image, or the use of a particular viewpoint[30] – factors that could very well be applied to digitised memories. However, the non-visual factors present in this new medium could also be quite informative for the discussed purpose, in a manner thus far unknown to personal data definitions. Consider an individual "playing" someone else's memory in their own Sensen; the former person would be able to hear the tone of the latter's voice, feel one's smell, feel the recorded individual's weight etc.

26 The next factor in this set is physiological identity. The Oxford Dictionary defines the term "physiological" as "relating to the branch of biology that deals with the normal functions of living organisms and their parts".[31] Taking this into account, a Sensen memory could potentially reveal quite a lot about an individual's living functions and physiological conditions. Setting aside the obvious scenarios, such as a memory of a cold or a visit to a doctor, a memory could contain a set of factors (e.g. specific cough, the feeling of slight nausea, specific texture of the tongue) which, if examined by a medical professional, could point (for example) to a specific medical condition suffered by an individual.

27 Following physiological identity, art. 4(1) moves on to elevate one's genetic identity in a similar fashion. Definition of genetic data from art. 4(13), as complemented by recital 34 of the Regulation, is that of "personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question".[32] Assuming that the Sensen tech would allow for the digitisation of memories without the inclusion of any biological material from the brain, such memories would not automatically point towards the genetic identity criteria. As for the content of memories, in contrast to many instances previously discussed in this section, it would most likely be exceedingly difficult to find memories containing genetic data.

28 Metadata can be defined as secondary data, describing another set of data.

29 Article 29 Data Protection Working Party, *Opinion 02/2012 of the on facial recognition in online and mobile services* (2012) 00727/12/EN, WP 192, at p. 4. The Working Party is an influential advisory body which "provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States" (see <https://edps.europa.eu/data-protection/data-protection/glossary/a_en>).

30 *Opinion 02/2012*, supra fn. 30, at p. 4.

31 See <https://en.oxforddictionaries.com/definition/physiological> (last accessed on October 12th, 2017).

32 GDPR, supra fn. 2, rec. 34.

28 Moving forward, mental identity is indicated as another possible path to the realm of personal data. Digital memories would be extremely likely to contain such information, almost always offering a unique insight into one's mental state and identity. Private journals and video logs would pale in comparison.

29 Economic identity, another example from the provision, would similarly be very likely to be revealed by one's digitised memories. What one is wearing in the memory, what belongings he/she has in his/her house, what car one is driving, how much money does one have in his or her bank accounts etc. All those factors would likely reveal a lot about one's economic status and perspectives. Of course, there could be memories which are devoid of such information; imagine a millionaire swimming in a communal swimming pool, not thinking about his possessions and financial standing, and not wearing swimming shorts made by Armani with Swarovski crystals. Nevertheless, the chances of at least some relevant information being contained in an average digitised memory would be quite high.

30 The two final indicated factors are a person's cultural and social identity – for the purposes of this section, it is possible to consider them in one paragraph. Both would have a good chance of being conveyed by a Sensen memory. Apart from visual representations, such as clothing (think about the memory subject wearing a Jewish kippah or a t-shirt with one's favourite rock band logo on it), the memory could include someone going to work, church, a music concert, and other places holding the potential to reveal one's cultural and/or social identity.

31 One of the key thoughts emerging from the analysis conducted in this section is that if the content of memories was to be considered in deciding whether a digitised memory constitutes personal data, whether it is in fact a piece of information relating to an identified or identifiable natural person, there would be a tremendous amount of different possibilities, tipping the art. 4(1) scales in one direction or another. With Sensen memories, the context, or rather content of a memory could be extremely important, as it was shown above. After all, human memories can be as diverse as human life itself.

32 Nevertheless, the argument put forth in this article is that due to the very high probability of at least some aspects of the art. 4(1) test being fulfilled – most notably with regards to the individual's name and location data, as well as physical and mental identity – digitised memories *should be* regarded as personal data, *without* the need for an evaluative inquiry of the memory's content. Difficulties with the information vs. medium dichotomy are not unprecedented in the field of data protection law – following Bygrave, "as biological material is increasingly mined for information, justifying a distinction between the former and the latter – that is between the medium and the message – becomes more difficult".[33] The functional approach, guided by the need to provide adequate protection to Sensen memories' data subjects, justifies in this particular case focusing art. 4(1) on the medium, instead of the message – and the CJEU decision in case C-582/14, *Breyer* could be seen as supporting this conclusion. In the cited judgement, an IP address (whether dynamic or static) was found to constitute personal data[34] – variables such as which websites was the individual browsing with the IP address at hand had no impact on the indicated finding. Adopting such an approach in relation to Sensen could, among multiple others, oblige the data controllers to implement special technological and procedural safeguards to memory repositories, without the need to confirm first that each hosted memory does in fact contain personal data. Additionally, an evaluative inquiry of the memories' contents would itself present additional concerns tied not only to the efficiency of the legal framework, but also to the right to data protection and the right to privacy. In contrast to (for example) video files, digitised memories would be almost certain to carry some form of a personal stamp of the kind matching those listed in article 4(1).

33 There is, however, a potential challenge to the reasoning of the preceding paragraph. What if the memory in question is fake? What if it was e.g. altered by one of the memory hunters? Even worse, what if an individual does not know that his memory was altered, or maybe he unknowingly bought a fake memory at a vending machine akin to those in Neo-Paris, and with time started to treat it as his own, merged it with his other, own, pure memories? Additionally, what about the practice of covering up one's personal data (e.g. in order to avoid digital surveillance), well described in Brunton and Nissenbaum's book *Obfuscation: A User's Guide for Privacy and Protest*?[35] It is possible to imagine wary citizens altering the copies of their memories stored in a memory bank or uploaded to a dedicated social network. Would all those kinds of memories still qualify as personal data even if the factual connection would be false?

34 In order to answer this question, it is worth reaching back to the fundamental aims of data protection law, and contrasting them with those of the law of defamation. In the latter branch of law, truthfulness of information plays a key role – in

33 Bygrave, supra fn. 4, at p. 126.

34 Case C-582/14 *Breyer v Germany* (2016), at para [49].

35 Brunton F and Nissenbaum H, *Obfuscation: A User's Guide for Privacy and Protest* (2015) MIT Press.

the UK, for example, truth is a defence to a claim in defamation.[36] This is because the regulatory goal at hand is protecting the citizens' reputation from being tarnished by false statements; and if a statement made about someone is true, their legally perceived reputation is not harmed.[37] The situation is different with data protection law. It is aimed at protecting the data subjects from harm, which might be inflicted as a result of other people accessing and using the former's personal data. Data protection law is principally not concerned with the truthfulness of information – in order to fall within the GDPR's scope, it is sufficient for information to "relat(e) to an identified or identifiable natural person".[38] Hence, there is a strong argument to consider the indicated examples of fake/remixed Sensen memories as personal data. Such an approach can be supported by a comparison to the phenomenon of the so-called "fake nudes", based on spreading falsified nude pictures of celebrities, where e.g. an actor's face is Photoshopped onto a naked body.[39] In such a scenario, the information is clearly false – however, he/she is clearly identifiable from the picture, and deserves the protection of measures bestowed by the GDPR. Even if we take into account the sophisticated obfuscation measures, with data subjects anonymising their memories before uploading them online, such persons should not be losing the shield of data protection, especially given the fact that it would be extremely difficult to ascertain that a memory has been *actually* cleared of any indicators of personal data.

35 While the issue of straight-forward "truthfulness" of Sensen memories could be solved in the manner outlined, it should be acknowledged that the emergence of fake memories could potentially undermine our understanding of *identity* and its presumed integrity, with potential consequences for the notion of *identifiability*. Consider the earlier mentioned possibility of someone purchasing another's memory and then appropriating it, starting to perceive it as his own. If that memory is then shared further, for example on an online repository, will it be identifying the source person (in whose brain the memory was created) or the purchasing person, due to e.g. being changed/personalised in the latter's mind? Will it identify both at the same time? *Remember Me* does not suggest an answer here, and much more importantly, it is not known how such a situation would play out in the real world, should the memory digitisation technology come to appear. One could hope that criminalisation of involuntary memory alterations, coupled with a way to somehow "watermark" the externally obtained memories could help in mitigating the risk of such conundrums arising. However, it is very much possible that aside from the technological experts and IT lawyers, the regulators would have to also turn towards the philosophers exploring the theories of essentialist and constructive identity in a novel and very challenging setting.

36 Without doubt, the emergence of various forms of fake/swapped memories described above could bring a host of considerable problems in front of the regulators, extending far beyond data protection law. However, even if the scenario from the end of the previous paragraph is taken into account as a potential, currently unsolved dilemma, it still seems that analysing the *content* of memories for uniquely identifying information or for truthfulness, as a preliminary condition to classify them as personal data, would most likely be disproportionate, inefficient, and against the main aim of data protection law.

II. Digitised memories as sensitive data

37 Assuming that the conclusions of the previous section are embraced, and digitised memories are found to be personal data *per se* within the meaning of article 4(1), a predictable, subsequent question appears – should such memories be treated as one of the categories of "sensitive" or "special" data, warranting additional protection? In order to answer this question, this section must turn towards article 9 of the GDPR.[40]

38 Article 9 of the Regulation prohibits (subject to several, important exceptions – most notably, consent)[41] the processing of certain types of personal data which, as recital 51 explains, merit special protection due to the significant risks they might pose to data subjects' fundamental rights and freedoms, and risks corresponding to the processing of such data. Article 9 sets out seven categories of the described data, in a closed list - as in section C.I of this paper, it is worth considering Sensen memories in the context of each category. The first of the seven is data which reveals the data subject's

36 See section 2 of the Defamation Act 2013 c. 26.

37 See *McPherson v Daniels* (1829)10 B. & C. 263, at 272.

38 Art.4(1) of the GDPR.

39 See <http://theconversation.com/celebrity-fakes-where-porn-meets-a-sense-of-possession-20829> (last accessed on October 12th, 2017).

40 Art. 10, focused on processing of personal data relating to criminal convictions and offences, would be relevant in this context as well, but for the purpose of this exploratory article, only art. 9 is considered, due to the variety of data categories it contains.

41 GDPR, supra fn. 2, art. 9(2)(a). Again, considering the application of art. 9(2) exceptions to Sensen memories would be a most worthy endeavour, one which unfortunately does not lie in the scope of this article.

racial or ethnic origin. It is fairly easy to imagine how nearly every memory would include information disclosing one's racial origin – the sight of one's hands is a perfect example. Ethnic origin could be slightly less straight-forward, but also very probable, being communicated through one's clothing, accent, as well as thoughts and conversations.

39 The second path to the "special category of data" status leads through personal data revealing one's political opinions. It seems quite likely that Sensen memories could hold the records of conversations on political matters, especially due to the fact that this term is not limited to e.g. the critique of political parties, but can be seen as including any matters "associated with the governance of a country or area",[42] or even of a group within the society. In our daily lives, such conversations tend to weave their way in, wherever we go. It might of course happen that a person successfully avoids any political conversations – however, this is where Sensen creates a unique possibility of the discussed disclosure occurring nevertheless. By providing an insight into one's mind, this technology could reveal the data subject's conscious and subconscious reactions to certain overheard conversations and even witnessed events. By way of example, imagine someone looking at a damaged road and cursing silently at the lack of action from the city council – this could then be seen as a political opinion.

40 The third category is that of data revealing an individual's religious or philosophical beliefs. Sensen memories would have a good chance of containing such information, in a similar manner to cultural and social identity, as discussed in section C.I above. This reasoning can be seen as further supported by the Art. 29 Working Party's *Opinion 02/2012 on facial recognition in online and mobile services*, which stated that if digital images "are going to be used to obtain ethnic origin, religion or health information", then they are to be treated as a special category of personal/sensitive data.[43] Sensen memories could be seen as capable of containing, in a way, such digital images. However, the context of religious and philosophical beliefs demonstrates particularly well how a more direct and unprecedented path to disclosure could be found with the Memorize corporation's technology. Imagine someone praying in a church: the memory of this event – upon being loaded into another person's Sensen – could show that the person does not believe in the words he or she recites. Or for another example, consider a memory of a parent lecturing his or her child that they should not have hit the boy who was bullying them, while thinking "well done kid, that'll teach him". While social and cultural identity could also be disclosed in this intrinsic manner, the context of religious or philosophical beliefs is arguably more often tied to the individual's inner thoughts.

41 Next, art. 9 prohibits the processing of personal data revealing an individual's affiliation to a trade union. In contrast to the previous three, this special category of data would be rather unlikely to be found within the digital memories, unless a person would be, for example, a very active trade union member.

42 The fifth category is one concerned with the processing of genetic or biometric data with a purpose of "uniquely identifying" a natural person. This term indicates the identification of a specific person, not as a member of a group, but as e.g. Mr. John Smith. Considering genetic data in this context first – as it was argued in section C.I above, it is rather unlikely that Sensen memories would include genetic data as understood within the Regulation. In order to see whether the same would be likely for biometric data, it is necessary to turn towards the definition of such data, laid out in art. 4(14) of the Regulation. By virtue of this provision, biometric data is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person" – characteristics which have to allow for or confirm the unique identification of that person. Examples indicated in the text of this provision are facial images and dactyloscopic data.

43 There is a very strong argument in favour of seeing Sensen memories as likely carriers of biometric data, much in the same manner as they are likely to carry data about one's physical and physiological identity (as it was discussed in section C.I above). "Specific technical processing" (as present in art. 4(14) of the Regulation) could be found in the very process of memory digitisation. Unique identification could be based on, again, the memory of someone looking in a mirror, but also on an external party knowing the data subject very well and being able to piece together various physical and psychological details appearing in the memory, to become certain that this is a memory of one specific individual. This piece-together approach could be particularly true with regards to the third listed subtype of biometric data, that is behavioural characteristics. While two people's memories of a similar event (e.g. getting on a bus) might seem almost the same, they are likely to be riddled with small, sometimes unnoticeable details, which can add up to a unique pattern of behaviour, readable by someone with the right knowledge and/or technology. Indirect support for this line of interpretation can be found in the Art. 29 Working Party's *Opinion 8/2014 on the Recent Developments on the Internet of Things*, which stated that data originating from devices belonging to the

42 See <https://en.oxforddictionaries.com/definition/political> (last accessed on October 12th, 2017).

43 *Opinion 02/2012*, supra fn. 30, at p. 4.

"Internet of Things" category "may allow discerning the life pattern of a specific individual or family – e.g. [through] data generated by the centralised control of lighting, heating, ventilation and air conditioning".[44] Sensen memories could be used to a similar end.

44 The next special category of data set out in art. 9 of the GDPR is data concerning health. When discussing physiological data, section C.I of this article demonstrated how deeply and uniquely the Sensen technology could, on multiple occasions, convey information about one's medical conditions. To reiterate: it could be possible to discover the relevant memories of events which occurred in public (e.g. someone coughing during a garden party), to uncover facts kept hidden by the data subject (e.g. a cancer diagnosis), and finally, to analyse memories containing medical information about which the data subject has no idea – but which could be uncovered by a medical professional or an appropriate algorithm, or both combined. A comparison can be made here to so-called Quantified Self devices, measuring numbers we generate through our daily activities (e.g. calories consumed, mood state data, blood oxygen levels, steps taken etc.). The earlier mentioned *Opinion 8/2014* of the Art. 29 Working Party noted that such devices "are mostly registering data relating to the well-being of the individual".[45] While this is not seen by the Opinion as "health data" *per se*, it "may quickly provide information about the individual's health as the data is registered in time, thus making it possible to derive inferences from its variability over a given period".[46] This reasoning could very well be embraced in the context of Memorize's technology.

45 The final category of data covered by art. 9 is data about a natural person's sex life or sexual orientation. Akin to many previous subtypes of data covered in this section, it could also be seen as likely to appear within the digitised memories, on multiple, progressively deeper levels. First, one's memories could contain representations, verbal or in writing, made by that person with regards to his or her sexual preferences. Then, a person's memory could contain details of private, even secret life – examples being memories of sexual intercourse or browsing of adult content online. Finally, memories could contain inner thoughts and physiological reactions which the person might not even be aware of or interpret as tied to sexual preferences or orientation.

46 Therefore, we may return to the key question underlying this section – should Sensen memories be seen as sensitive data? The answer proposed by this paper is a definite yes. In a similar manner to conclusions drawn in section C.I, the key reasoning underlying the proposed stance is based on the high likelihood of multiple special categories of data being encountered within the digitised memories – most notably data revealing racial and ethnic identity, biometric data uniquely identifying natural persons, data concerning health, as well as data revealing a person's sex life or orientation. Sprokkereef, when writing about a similar dilemma in the field of novel forms of biometric data, stated that "(...) it is not clear if the algorithms and machine-readable templates that contain the information are always to be considered as sensitive personal data".[47] Taking the earlier described functional approach, based on the need to offer adequate protection to data subjects, suggests that Sensen memories could and most likely *should* be elevated to the sensitive data status. To make another comparison – Art. 29 Working Party's *Opinion 5/2009 on online social networking* aptly stated that it "does not consider images on the Internet to be sensitive data, unless the images are clearly used to reveal sensitive data about individuals."[48] Sensen memories would deserve to be treated in the opposite manner, due to the overwhelming and highly concerning number of art. 9 special data categories, which could materialise in this new medium of information, giving unprecedented and unique degree of insight to parties loading the data subject's memory into their Sensen. While DNA could be seen as a blueprint for one's body (one containing health data or revealing racial or ethnic origin, as the Art. 29 Working Party's *Opinion 3/2012* noted[49]), Sensen memories could be seen as a blueprint for one's soul, thus requiring commensurate protection.

D. Conclusion

47 In the UK trailer for *Remember Me*, Nilin (the game's protagonist) puts forward a quote "the memory of a single man is a fortress, more complex than the vastest of cities."[50] If it ever comes to this, deciding on who should be granted the keys to this fortress, and what kinds of keys, should be a well thought-through exercise, oriented towards finding the

44 Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, at p. 10.

45 *Opinion 8/2014*, supra fn. 47, at p. 17.

46 *Opinion 8/2014*, supra fn. 47, at p. 17.

47 Sprokkereef A and de Hert P, 'Biometrics, Privacy and Agency' (2012) in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer), at p. 92.

48 Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, at p. 8.

49 Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, at p. 15.

50 See <https://www.youtube.com/watch?v=FMyQlnnxXuk> (last accessed on October 12th, 2017).

adequate balance between the socially beneficial uses of the Sensen technology and safeguarding the data (memory) subjects' rights. Recognising the digital memories as sensitive data, regardless of their content, would be a sensible starting point towards finding the said balance in the effort to accommodate the Sensen technology within the European data protection framework.

48 At this very initial analytical point, it seems that the GDPR's definitions of personal and sensitive data are sufficiently technology-neutral to accommodate the concept of digital memories. It seems that the EU legislators' intention to construe the definitions of personal data broadly, as demonstrated by Bygrave,[51] could withstand the challenge brought by Memorize's technology – though not without an analytical struggle, as the discussion of fake memories in section C.I demonstrated. Perhaps, the Regulation's rights and obligations tied to personal and sensitive data would be able to provide an adequate shield against the potential harm to data subjects, while respecting the other stakeholders' interests. For now, this diverse path of inquiry remains to be explored – but given the earlier mentioned scientific developments, the need for further exploration of the GDPR's ability to respond to memory digitisation technologies might become more urgent than we consider it to be.

Acknowledgements

The author would like to express his sincere thanks to Dr David Erdos (University of Cambridge), Jef Ausloos (KU Leuven), Grzegorz Michalak and Paweł Przygucki, for their insightful, helpful and encouraging comments on the draft of this article. Thanks are also owed to the anonymous peer reviewer(s), for the valuable, meaningful and challenging comments, embracing the unconventional research aim(s) of this piece. The article was created within the Human Rights, Big Data and Technology project, supported by the Economic and Social Research Council [grant number ES/M010236/1].

51 Bygrave, supra fn. 4, at p. 127.

Copyright, Doctrine and Evidence-Based Reform

by **Stef van Gompel***

Abstract: Copyright lawmaking is conventionally embedded in a doctrinal tradition that gives much consideration to coherence and formal consistency with legal-theoretical foundations. This contrasts discernibly with the recent trend to base copyright policies and their elaboration into effective legal norms on empirical evidence. Recognizing that both approaches have their relative strengths and weaknesses, this paper explores how evidence-based policy can be reconciled with the traditional doctrinal approach to copyright lawmaking. It suggests that unproven doctrinal constellations that unnecessarily focus the legislative intention unequally on protecting copyright holders should be removed, but that lawmakers at the same time should also not stare blindly on economic evidence if legitimate claims based on fairness rationales are put forward, which also have to be weighed in as evidence.

Keywords: Copyright reform; lawmaking approaches; evidence-based policy; doctrinal underpinnings; economic evidence

Recommended citation: Stef van Gompel, Copyright, Doctrine and Evidence-Based Reform, 8 (2017) JIPITEC 304 para 1.

A. Introduction

1 In an ideal world, copyright law is based on sound, reliable and impartial evidence that thoughtfully and meticulously balances the full breath of often diverging or competing interests of all stakeholders involved.[1] This suggests that any new legislation must be carefully prepared by assessing and taking into account all the different – legal, social and economic – dimensions of the proposed measure, including all relevant empirical facts. Additionally, the legislative process must be clear and open to public scrutiny, so as to ensure the legitimacy and public acceptability of the law. This requires adequate transparency about all the evidence considered, including how much it has weighed into the norm-setting, which information gaps nonetheless existed, and how these gaps have been filled or dealt with. Moreover, it must be clear how different interests of relevant stakeholders are balanced and eventually reflected in the law as adopted.

2 Despite best efforts and good intentions of law and policy makers, such an ideal norm-setting scenario hardly ever materializes in practice.[2] Often, it is

* Dr. S.J. van Gompel is senior researcher at the Institute for Information Law (IViR) of the University of Amsterdam.

The research for this paper was conducted within the framework of the research programme Veni with project number 451-14-033 ("The challenge of evidence-based intellectual property law reform: Legal pragmatism meets doctrinal legal reasoning"), which is partly financed by the Netherlands Organisation for Scientific Research (NWO). An earlier version of this paper was discussed at the ALAI 2017 Congress "Copyright - to be or not to be", which was held in Copenhagen, Denmark on 17-20 May 2017. I thank the participants of that conference for their remarks and suggestions, which helped me to improve the paper. Any errors are my own.

1 E. Derclaye, 'Today's Utopia Is Tomorrow's Reality' [2017] *IIC* 1.

2 See B.H. Mitra-Kahn, 'Copyright, Evidence and Lobbynomics: The World after the UK's Hargreaves Review' (2011) 8 *Review of Economic Research on Copyright Issues* 65, giving a number of reasons why policy makers are struggling to adequately ground copyright policy in evidence. See also I. Hargreaves,

difficult for legislators to draw up a full-framed picture of all relevant data that sheds light on the issue under consideration.[3] Information may be scarce or unavailable and the reliability and validity of sources is not necessarily easy to establish,[4] which renders it hard to make informed and balanced policy decisions.[5] Moreover, even if legislators manage to gather sufficient evidence, they may face difficulties to bring it on a par with the doctrinal underpinnings of the law at issue. Especially in a domain such as copyright, which traditionally rests strongly on doctrinal foundations, it cannot be automatically presumed that evidence brought forward neatly fits the existing legal framework. In the current digital era, in particular, traditional copyright principles have increasingly come under attack due to the changes in the way people produce, disseminate, share and consume works. For legislators, this raises the arduous question of what to do with evidence that does not sit well with, or even contradicts, the legal-theoretical foundations on which copyright law is built.

3 This paper explores ways in which the current evidence-based policy approach can be reconciled with the traditional doctrinal approach to copyright lawmaking. To that end, the paper first juxtaposes the two approaches and examines their relative strengths and weaknesses. Next, it gives a number of concrete recommendations that aim to facilitate the current shift in copyright lawmaking from a classic doctrinal approach towards a more evidence-based approach. By enabling legislators to adopt evidence-based policy without requiring them to abandon doctrinal principles altogether, this paper aims to contribute to improving the quality of lawmaking in the field of copyright.

B. Approaches to copyright lawmaking

I. Doctrinal versus evidence-based approaches to lawmaking

4 In copyright law, there is a growing trend to base new legislation on empirical evidence.[6] To remain a key instrument of innovation, cultural and growth policies, copyright law constantly needs to adapt to societal changes caused by the emergence of new digital technologies. This requires a careful balancing of the interests of creators, rightholders, users, and end-consumers. Policymakers around the world increasingly acknowledge that, for reasons of sound policy and better lawmaking, copyright policies and their elaboration into effective legal norms should be based on empirical evidence that allows measurable economic objectives to be balanced against social goals.[7]

5 To give a few examples, at the international level, the World Intellectual Property Organization (WIPO) has been integrating economic research in its work program to enable evidence-based policymaking by monitoring the effectiveness and managing the accountability of treaty norms.[8] In the EU, law and policy initiatives, including on intellectual property, are preceded by impact assessments that aim to provide transparent, comprehensive and balanced evidence on the nature of the problem to be addressed.[9] National governments typically demand the same. Probably the best example is the UK, where the Intellectual Property Office has adopted rules on good evidence for policy,[10] following recommendations by the Hargreaves report.[11] All this shows a shift towards a more evidence-based lawmaking approach.

Digital Opportunity: A Review of Intellectual Property and Growth (London: IPO 2011), p. 19, giving examples of copyright measures that lawmakers have adopted, notwithstanding the availability of evidence opposing these measures.

3 J. de Beer, 'Evidence-Based Intellectual Property Policy Making: An Integrated Review of Methods and Conclusions' (2016) 19 *The Journal of World Intellectual Property* 150. See also E.R. Gold, J.-F. Morin & E. Shadeed, 'Does intellectual property lead to economic growth? Insights from a novel IP dataset' (2017) *Regulation & Governance*, [online] doi: 10.1111/rego.12165.

4 In the field of copyright in particular, a serious knowledge asymmetry may exist as a result of information not being publicly controlled but privately owned by stakeholders, including copyright industries, collective rights management organisations, internet intermediaries, online platforms, or other entities.

5 See M. Kretschmer & R. Towse (eds), *What Constitutes Evidence for Copyright Policy?* (Digital proceedings of ESRC symposium, CREATe Working Paper, no. 1, January 2013).

6 See P. Samuelson, 'Should Economics Play a Role in Copyright Law and Policy?' (2003-2004) 1 *U. Ottawa L. & Tech. J.* 1, p. 21, already predicting 'that economic analysis will have greater impact on copyright in the future.'

7 See e.g. the recommendation in Hargreaves, *op. cit.*, pp. 8 and 20.

8 WIPO, The Economics of IP, <http://www.wipo.int/econ_stat/en/economics/>.

9 European Commission, Impact assessments, <https://ec.europa.eu/info/law-making-process/planning-and-proposing-law/impact-assessments_en>.

10 UK Intellectual Property Office, *Guide to Evidence for Policy* (Newport: Concept House 2014). For a critical comment on the approach taken by the UK Intellectual Property Office, see T. Dillon, 'Evidence, policy and "evidence for policy"' [2016] *Journal of Intellectual Property Law & Practice* 92.

11 Hargreaves, *op. cit.*, pp. 8 and 20.

6 Today's copyright law, however, is clearly the result of a more doctrinal approach. In continental Europe in particular, the justification of copyright law is traditionally based in a potent mixture of personality-based arguments and private property doctrine.[12] The narrative has been – and still is – to emancipate authors from patrons and publishers by granting them exclusive rights to protect their economic and moral interests. Illustrative of the strength of the property rights rhetoric is the Charter of Fundamental Rights of the EU, which in its section on private property explicitly sets out: "Intellectual property shall be protected".[13] Such a narrative reflects the doctrinal roots of copyright lawmaking that is dominant in continental Europe, but also elsewhere in the world.

II. Relative strengths and weaknesses

7 The shift towards evidence-based lawmaking, although it may certainly complement the current doctrinal approach, does require a change of attitude and a new way of thinking about copyright reform. Under a doctrinal approach, the lawmaker's primary concern in reform initiatives is to maintain normative coherence and formal consistency with legal-theoretical and ideological underpinnings of established rights. A doctrinal approach thus invites systematic legal reasoning aimed at logically sound laws.[14] In its ultimate manifestation, this may result in overly legalistic and formalistic law and might even establish tunnel vision in legislative efforts.[15] A strong advantage of a doctrinal approach is, however, that it creates legal certainty.[16] Generally speaking, reform decisions based on established reasoning and principles tend to be foreseeable and require less explicit balancing of interests, thus making them politically easier to achieve.[17]

8 By contrast, an evidence-based lawmaking approach expects the legal implementation of copyright policies to be based on testable assumptions and instrumental impacts in the future. Rather than focusing chiefly on coherence and formal consistency of norms with legal-theoretical foundations, legislators must apply practical reason to make rational policy-decisions within the confines of the best evidence available.[18] In its ultimate manifestation, an evidence-based lawmaking approach may potentially lead to more ad hoc and unprincipled decision-making and thus to less predictable law.[19] Yet, it also has the advantage of better accommodating the law to a societal context than an approach that largely rests upon untested and essentialist doctrinal assumptions.

C. Reconciling evidence-based lawmaking with copyright's doctrinal foundation

9 The above comparison between doctrinal and evidence-based lawmaking approaches suggests that, in order to create better law in the field of copyright, the two approaches somehow need be reconciled. Ideally, a practice emerges that enables legislators to build on the strengths while curtailing the weaknesses of both approaches. This would require a shift in mindset and practices on different levels. On the one hand, lawmakers need to create adequate room for evidence-based copyright reform by removing any doctrinal constellations that are unnecessary and unproven and by preventing political capture by norms contained in the international copyright framework. On the other hand, they must also accept that certain doctrinal principles based on fairness rationales ought to be considered, which may sometimes even prevail over economic evidence if there is a clear need to protect specific interests of authors. A broader definition of evidence that extends beyond the purely economic would arguably lead to a better and more nuanced understanding of the potential to use evidence in copyright lawmaking. If fairness or personality-based arguments are used to justify particular copyright policies, however, it would be reasonable to demand evidence that those policies

12 M. Buydens, *La propriété intellectuelle: évolution historique et philosophique* (Bruxelles: Bruylant 2012).

13 Art. 17(2) Charter of Fundamental Rights of the EU, *OJ EU* C 364/1, 18 December 2000.

14 See e.g. J. Bengoetxea, 'Legal System as a Regulative Ideal' in H.J. Koch & U. Neumann (eds), *Praktische Vernunft und Rechtsanwendung/ Legal System and Practical Reason* (ARSP-Beiheft 53, 1994), pp. 65-80, at pp. 70 et seq., discussing some of the systematizing features of legal doctrine in creating norm-propositions in law.

15 Compare the criticism voiced against overly-formalistic law by proponents of legal realism in the United States in the early twentieth century. See e.g. M. White, *Social Thought in America: The Revolt Against Formalism* (rev. edn, Boston: Beacon Press 1957), pp. 15-17.

16 This function of the law is also recurrently emphasized by proponents of legal positivism. See e.g. H.L.A. Hart, *The Concept of Law* (2nd edn, Oxford: Clarendon Press 1961), p. 127; S.J. Shapiro, 'On Hart's Way Out' (1998) 4 *Legal Theory* 469, p. 494, speaking about the 'essential guidance function of law'.

17 A. Peczenik, *On Law and Reason* (Dordrecht: Springer Science + Business Media 1989), pp. 177-178.

18 In this manifestation, evidence-based lawmaking bears some resemblance to theories of legal pragmatism that also strongly adhere to empiricism. See T.F. Cotter, 'Legal pragmatism and Intellectual Property Law' in S. Balganesh (ed), *Intellectual Property and the Common Law* (Cambridge: Cambridge University Press 2013), pp. 211-229.

19 Peczenik, *op. cit.*, p. 178.

are effective in achieving them.[20] In the end, the purpose of copyright law is to create an effective and balanced system of protection addressing the interests of creators, rightholders, users, and the general public in a manner that reflects empirical reality, while taking account of specific needs that may exist on the different sides of the copyright spectrum.

I. Remove unnecessary and unproven doctrinal constellations

10 If law and policy makers in the area of copyright want to give evidence-based lawmaking a fair chance, they must first eliminate all doctrinal constellations based on untested or unproven assumptions, which may unwillingly frame their mindsets towards a specific predetermined position. A clear example of such unnecessary and undesirable doctrinal constellations can be found in various EU directives on copyright, including the InfoSoc Directive.[21] Taking, as the starting point, that copyright fosters creativity and innovation, recital 9 proclaims that "[a]ny harmonisation of copyright and related rights must take as a basis a high level of protection, since such rights are crucial to intellectual creation." In the same way, recital 11 assumes that "[a] rigorous, effective system for the protection of copyright and related rights is one of the main ways of ensuring that European cultural creativity and production receive the necessary resources and of safeguarding the independence and dignity of artistic creators and performers."

11 Such direct references to a "high level of protection" and a "rigorous, effective system" of copyright and related rights unmistakably focuses the legislative intention too unevenly on protecting creators and rightholders.[22] This also has effects on the interpretation of the copyright framework by the Court of Justice of the EU (CJEU), which has consistently confirmed that the InfoSoc Directive grants to authors and rightholders a set of broadly defined exclusive rights,[23] from which only the exhaustively listed and strictly defined exceptions or limitations may derogate.[24] Such doctrinal logic does not help to preserve the delicate balance between protecting authors and rightholders and safeguarding the interests of users and it certainly does not aid evidence-based decision-making.

12 Generally speaking, aiming for a high level of copyright protection must never be a goal in itself, as it does not necessarily contribute to enhanced creativity and innovation. In reality, too little protection may have a negative impact on creativity and innovation, but so does an overly strong protection.[25] What the optimal level of protection is, by which sufficient incentives are provided to authors, while innovation and creation by users and subsequent creators is not suppressed, is practically impossible to determine.[26] In effect, rather than striving for a "high level of protection", the starting point of any copyright lawmaking effort should always be the equilibrium that needs to be maintained between the interests of creators, rightholders, users and the public at large,[27] however uncertain and delicate that equilibrium might be, and however difficult it is to situate it.

II. Prevent political capture by international copyright norms

13 In a similar vein, to enable lawmakers to adapt copyright law to new economic, societal and technological challenges, it must be ensured that

20 See e.g. R. Giblin, 'Reimagining copyright's duration', in R. Giblin & K. Weatherall (eds), *What if we could reimagine copyright?* (ANU Press, 2017), pp. 177-211.

21 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, *OJ EU* L 167/10 of 22 June 2001.

22 T. Dreier, 'Thoughts on revising the limitations on copyright under Directive 2001/29' [2016] *Journal of Intellectual Property Law & Practice* 138, p. 139.

23 See e.g. Case C-145/10, *Painer v Standard Verlags* [2011] ECR I-12533, para 96 (on the reproduction right); Case C-610/15, *Stichting Brein v Ziggo* [2017] ECLI:EU:C:2017:456, para 22 (on the right of communication to the public); Case C-516/13, *Dimensione v Knoll* [2015] ECLI:EU:C:2015:315 (on the distribution right).

24 The exhaustive list of exceptions and limitations in art. 5 InfoSoc Directive is strictly observed (Case C-351/12, *OSA v Léčebné lázně Mariánské Lázně* [2014] ECLI:EU:C:2014:110, paras 22-41; Case C-275/15, *ITV v TVCatchup* [2017] ECLI:EU:C:2017:144; Case C-138/16, *AKM v Zürs.net* [2017] ECLI:EU:C:2017:218, paras 31-43). In general, copyright exceptions and limitations must be interpreted strictly (Case C-5/08, *Infopaq v Danske Dagblades Forening* [2009] ECR I-6569), whilst securing their effectiveness and permitting observance of their purpose (Case C-201/13, *Deckmyn v Vandersteen* [2014] ECLI:EU:C:2014:2132; Case C-117/13, *TU Darmstadt v Ulmer* [2014] ECLI:EU:C:2014:2196; Case C-174/15, *VOB v Stichting Leenrecht* [2016] ECLI:EU:C:2016:856).

25 Dreier, *op. cit.*, pp. 139-140.

26 See e.g. N. Elkin-Koren & E.M. Salzberger, *The Law and Economics of Intellectual Property in the Digital Age: The Limits of Analysis* (London & New York: Routledge 2013).

27 Admittedly, in the framework of the EU InfoSoc Directive, recital 31 also asserts that "[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". However, because recitals 9 and 11 put the objectives of creating a high level of protection and a rigorous, effective copyright system first, they provide an imbalance to begin with, as they suggest that ultimately the rights and interests of authors and rightholders must prevail.

they are not needlessly bound by age-old rules that are bedrocked in the international copyright framework. Simply stated, an argument that contends that a copyright rule cannot be changed because it is a norm laid down in international treaties cannot convince and must certainly not serve as an excuse for ignoring evidence. This is not to say that the framework of international copyright law is in need of a complete overhaul, but it certainly is time for a critical and structural rethink of some of the key elements of which it is comprised.[28]

14 The Berne Convention indeed does not consist of unchangeable cast-in-stone copyright norms and was never meant to be understood as such. In the end, just like any other law or treaty, it is a man-made political compromise that ought to be subject to change over time. In fact, the Berne Convention was always meant to be revised as needs arose,[29] on condition that such a revision has the objective of introducing amendments designed to improve the system of the Berne Union.[30] This arguably can be understood in a broad sense,[31] as long as the revised convention keeps protecting "in as effective and uniform a manner as possible, the rights of authors in their literary and artistic works."[32]

15 In reality, however, a revision of the Berne Convention is a next to impossible task, as it requires unanimity of all contracting parties.[33] This virtually gives any of the (presently 174)[34] Berne Union countries the power to veto a change to the convention. Moreover, since the key provisions of the Berne Convention are incorporated by reference into the TRIPS Agreement and the WIPO Copyright Treaty,[35] these treaties would also need to be revised in parallel with each other, in order to be able to effectuate any change of international copyright norms. This in turn renders international copyright reform hard to accomplish.

16 However difficult it may be to change international copyright law, policymakers should not abandon constructive attempts to improve the existing treaties. Any future revision should of course be subject to careful deliberation and supported by sufficient evidence that takes full account of the equilibrium, which copyright law seeks to establish.

III. Include doctrinal principles among the evidence to be considered

17 Other than providing leeway in the doctrinal domain to accommodate evidence-based copyright reform, there is also need to liberate evidence-inspired policymakers from adopting a too narrow economic approach.[36] For one thing, merely relying on economic evidence entails the risk that reform initiatives are rendered futile in cases where such evidence is unavailable or hard to obtain, while giving a strategic advantage to persons and organizations that possess relevant economic data to disclose or conceal such data according to their own interests and needs.[37] As importantly, lawmakers also need to recognize that certain doctrinal principles are simply part of the copyright framework and therefore ought to be taken into consideration in reform decisions.

18 This becomes especially clear when looking at the rationales for copyright protection, which are not merely economic by nature, but are also comprised of personality-based justifications. Indeed, copyright not only aims at encouraging innovation and creativity by providing incentives to create, thus contributing to the dissemination of knowledge and the advancement of culture, or at regulating trade by providing legal instruments to prevent counterfeiting and unfair competition (economic and cultural arguments based on incentive rationales). It also aims to give authors a fair reward for their creative efforts and to protect the personality or individuality of authors by granting them moral rights (social and justice arguments based on fairness rationales).[38]

28 See e.g. D.J. Gervais, *(Re)structuring Copyright: A Comprehensive Path to International Copyright Reform* (Cheltenham, UK & Northampton, USA: Edward Elgar 2017).

29 C. Masouyé, *Guide to the Berne convention for the Protection of Literary and Artistic Works (Paris Act, 1971)* (Geneva: WIPO 1978), p. 121.

30 Art. 27(1) Berne Convention (Paris Act, 1971).

31 See e.g. *Records of the intellectual property conference of Stockholm (June 11 to July 14, 1967)*, vol. 1 (Geneva: WIPO 1971), p. 80, indicating that improvements to the system of the Berne Union "should include not only the enlargement of the protection granted to authors by the creation of new rights or by the extension of rights which are already recognized, but also the general development of copyright by reforms intended to make the rules relating to it easier to apply and to adapt them to the social, technical and economic conditions of contemporary society."

32 Preamble of the Berne Convention (Paris Act, 1971).

33 Art. 27(3) Berne Convention (Paris Act, 1971).

34 See the full list at: <http://www.wipo.int/export/sites/www/treaties/en/documents/pdf/berne.pdf>.

35 Art. 9(1) TRIPS Agreement; art. 1(4) WIPO Copyright Treaty.

36 Dillon, *op cit.*, pp. 96 et seq.

37 See the introduction of this paper and the sources mentioned there.

38 See e.g. F.W. Grosheide, *Auteursrecht op maat: beschouwingen over de grondslagen van het auteursrecht in een rechtspolitieke context* (Deventer: Kluwer 1986), pp. 127-143; J.-L. Piotraut, 'An Author's Rights-Based Copyright Law: The Fairness and Morality of French and American Law Compared' (2006) 24 *Cardozo Arts & Entertainment Law Review* 549; J.C. Fromer, 'Expressive Incentives in Intellectual Property' (2012) 98 *Virginia Law Review* 1745.

19 This suggests that lawmakers must be receptive to including more than just economic evidence in their deliberations when initiatives for copyright reform touch upon social and fairness principles. There may be reason, for example, to give particular attention to moral rights considerations when introducing new copyright limitations, or to recognize the position of the author as a weaker party in contract negotiations with publishers and producers when introducing new rules on authors' contract law. Take the introduction of a right that entitles authors to receive fair compensation in return for a transfer of rights in exploitation contracts. Although, economically speaking, such a right might be regarded as an empty shell, since the fairness of compensation cannot straightforwardly be determined,[39] doctrinally speaking, such a right can nonetheless serve as a necessary stick for authors to defend themselves if they are offered an unfair deal.[40] In such a case, doctrinal observations may ultimately prevail over a well-reasoned economic position.[41]

20 If and to what degree there is need to give social and fairness principles priority in other areas is much more contentious. One example is the value-gap proposal,[42] which builds on the claim that, to ensure a just economic balance in the digital marketplace, it would be fair if authors and performers would get a share of the income that online services make through the sale of advertisements, which accompany the content that users upload on their platforms,[43] a narrative that others claim to be somewhat misleading.[44] Another example is calls for making copyright protection conditional on formalities, for which there may be good economic reasons,[45] but which is often opposed by the argument that it is unfair if authors lose protection due to a failure to complete formalities.[46]

21 How much weight such fairness arguments hold, depends of course on the position that one takes in the debate and, for lawmaking purposes, on the objectives to be achieved. Generally speaking, lawmakers should refrain from prioritizing any type of evidence in advance, but carefully weigh and balance all the evidence available, including economic evidence and doctrinal arguments in favour or against a reform proposal.[47]

22 As a matter of principle, legislators must however be cautious that fairness arguments are not misused, where in fact interests other than those of authors prevail. In practice, it is often not the creators that benefit mostly from copyright protection, but publishers and producers to which copyright exploitation rights have been transferred.[48] This has to be taken into account whenever fairness claims are made in the legislative process. A plain example where the lawmaker failed to recognize this is the EU directive extending the term of protection of related

39 See J.P. Poort, 'Billijke vergoeding in recht en economie' [2015] *AMI* 157; J.P. Poort & J.J.M. Theeuwes, 'Prova d'Orchestra: een economische analyse van het voorontwerp auteurscontractenrecht' [2010] *AMI* 137, pp. 143-144.

40 P.B. Hugenholtz, 'Dirk en Pippi' [2015] *NJB* 1143.

41 J.P. Poort, *Empirical Evidence for Policy in Telecommunication, Copyright & Broadcasting* (dissertation, Vossiuspers UvA – Amsterdam University Press 2015), p. 269: "This leads to a paradoxical observation: an economist would not just have to take a normative position, but a paternalistic one as well, to object to legislation aimed at protecting authors and creators and advocated by a majority of them. Here, an economist should rest his case [...]."

42 European Commission, Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, Brussels, 14 September 2016, COM(2016) 593 final, art. 13.

43 ALAI, Resolution on the European proposals of 14 September 2016 to introduce fairer sharing of the value when works and other protected material are made available by electronic means, Paris, 18 February 2017, available at: <http://www.alai.org/en/assets/files/resolutions/170218-value-gap-en.pdf>.

44 'EU Copyright Reform Proposals Unfit for the Digital Age', Open Letter from European Research Centres to Members of the European Parliament and the European Council, 24 February 2017, available at: <http://www.create.ac.uk/wp-content/uploads/2017/02/OpenLetter_EU_Copyright_Reform_24_02_2017.pdf>, p. 6, arguing that "[t]he idea that the creation of value should lead automatically to transfer or compensation payments has no scientific basis".

45 See e.g. W.M. Landes & R.A. Posner, 'Indefinitely renewable Copyright' (2003) 70 *University of Chicago Law Review* 471; and H. Varian, 'Copying and Copyright' (2005) 19 *Journal of Economic Perspectives* 121, p. 128, arguing that: "Given today's technology, the creation of a 'universal' copyright registry, perhaps in exchange for some incremental benefits to authors, would be highly attractive."

46 See e.g. J.C. Ginsburg, 'The US Experience with Copyright Formalities: A Love-Hate Relationship' (2010) 33 *Columbia Journal of Law and the Arts* 311, p. 342. See also O. Alter, 'Reconceptualizing Copyright Registration' (2016) 98 *Journal of the Patent and Trademark Office Society* 930, supporting this with an analysis in behaviour economics.

47 See Dillon, *op cit.*, arguing that the challenges in accommodating evidence-based policy in lawmaking efforts are not necessarily situated in the types of evidence to be considered, but rather in facilitating due process.

48 See M. Kretschmer & P. Hardwick, *Authors' Earnings from Copyright and Non-Copyright Sources: A Survey of 25,000 British and German Writers* (Poole, UK: Centre for Intellectual Property Policy & Management 2007); Europe Economics, L. Guibault, O. Salamanca & S. van Gompel, *Remuneration of authors and performers for the use of their works and the fixations of their performances* (Brussels: European Commission – DG Connect 2015), available at: <https://www.ivir.nl/publicaties/download/1593.pdf>; Europe Economics, L. Guibault & O. Salamanca, *Remuneration of authors of books and scientific journals, translators, journalists and visual artists for the use of their works* (Brussels: European Commission – DG Connect 2016), available at: <https://www.ivir.nl/publicaties/download/remuneration_of_authors_final_report.pdf>.

rights in sound recordings.[49] Despite the availability of evidence that a term extension would chiefly benefit the recording industry and not the position of performers,[50] the directive was still adopted with the aim of improving the performers' income at the end of their lifetime.[51] There probably is no better example of a lawmaking exercise that disregarded economic evidence without reason.[52]

23 As a final point, if lawmakers on the basis of all evidence considered nevertheless come to decide that doctrinal principles must prevail over economic evidence, then they must be fully transparent about such a decision and the reasons behind it, in order to ensure democratic accountability and to secure the social legitimacy of copyright law.

D. Conclusion

24 In order to create an environment that allows for evidence-based reform, while keeping up with some of the guiding doctrinal underpinnings of copyright law, it is essential that lawmakers adopt a sufficiently open approach that allows them to be receptive of both economic and doctrinal evidence. This requires a change of mentality on the part of the legislator. For one thing, they must abandon certain doctrinal assumptions that guided copyright lawmaking previously, but find no support in empirical evidence, such as the idea that copyright requires a high level of protection. Moreover, the international copyright norms should not be treated as incontestable sacred rights, but subjected to change (however difficult that is) if new circumstances so dictate. At the same time, it must be acknowledged that, in copyright lawmaking, pure economic reasoning may not always be agreeable either, especially where legitimate fairness claims are in question.

25 Transformations in lawmaking practice, as the ones described here, require a stepwise and gradual approach. They do not happen overnight. In the end, any modernisation of copyright must begin with a clear vision on where the law should be heading, including specific objectives to be achieved. These can vary from short to mid-term objectives for national legislators, to long-term objectives for international policymakers. To keep in line with evidence-based policy, it would be desirable if these objectives were inspired by empirical facts and reflected a balanced approach between creators, rightholders, users, and the public at large, without *ex ante* privileging one particular position over another.

49 Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights, *OJ EU* L 265/1 of 11 October 2011.

50 See e.g. N. Helberger, N. Dufft, S.J. van Gompel & P.B. Hugenholtz, 'Never Forever: Why Extending the Term of Protection for Sound Recordings is a Bad Idea' [2008] *EIPR* 174; M. Kretschmer et al., '"Creativity stifled?" A joint academic statement on the proposed copyright term extension for sound recordings' [2008] *EIPR* 341.

51 See recital 5 of Directive 2011/77/EU.

52 Hargreaves, *op. cit.*, p. 19; A. Vetulani-Cęgiel, 'EU Copyright Law, Lobbying and Transparency of Policy-Making: The cases of sound recordings term extension and orphan works provisions' [2015] *JIPITEC* 146.

Non-Commercial Quotation and Freedom of Panorama

Useful and Lawful?

by **Eleonora Rosati***

Abstract: This contribution seeks to assess both the practical implications and lawfulness of national copyright exceptions that – lacking a corresponding provision in Article 5 of Directive 2001/29 (the InfoSoc Directive) – envisage that the only permitted use of a copyright work for the sake of the applicability of a certain exception is a non-commercial one. By referring to different national exceptions allowing quotation and freedom of panorama as case studies, the paper shows some of the shortcomings deriving from different approaches to the same permitted uses of copyright works across the EU, as well as the resulting (negative) impact on the very objective underlying adoption of the InfoSoc Directive: harmonization. This contribution concludes that – in general terms – diverging approaches to copyright exceptions, including limiting the availability of certain exceptions to non-commercial uses, may be both impractical and contrary to the system established by the InfoSoc Directive.

Keywords: Copyright; freedom of panorama; quotation; exceptions and limitations; InfoSoc Directive; non-commercial exceptions and limitations; for-profit; CJEU; Article 5 InfoSoc Directive

Recommended citation: Eleonora Rosati, Non-Commercial Quotation and Freedom of Panorama: Useful and Lawful?, 8 (2017) JIPITEC 311 para 1.

A. The system of the InfoSoc Directive

1 One of the objectives that EU legislature sought to achieve by adopting Directive 2001/29[1] (the InfoSoc Directive) was the harmonization of certain aspects of substantive copyright law. Without intervention at the EU level, diverging national approaches would result in different levels of protection and – from an internal market perspective – restrictions on the free movement of services and products incorporating, or based on, intellectual property.[2] Such risk would also become more acute in light of the challenges facing technological advancement.[3]

2 In parallel with the harmonization of the exclusive rights of reproduction (Article 2), communication and making available to the public (Article 3), and distribution (Article 4), the InfoSoc Directive also

* Associate Professor in Intellectual Property Law (University of Southampton). This study was prepared thanks to a grant of the Wikimedia's Free Knowledge Advocacy Group EU Grant Program. The views and opinions expressed are however only those of the Author, who can be contacted by email at eleonora@e-lawnora.com.

1 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, OJ, L 167, pp 10-19 ('InfoSoc Directive').

2 InfoSoc Directive, Recitals 6 and 7.

3 InfoSoc Directive, Recital 7.

harmonizes related exceptions and limitations (Article 5). With the exclusion of temporary copies (Article 5(1)), exceptions and limitations are optional for EU Member States to implement. All exceptions and limitations are subject to the three-step test contained in Article 5(5): they shall only be applied in certain special cases, which do not conflict with a normal exploitation of the work or other subject-matter, and do not unreasonably prejudice the legitimate interests of the rightholder.

3 The (formal) harmonization of exceptions and limitations may be regarded as limited also because the Directive itself states that their actual degree of harmonization should be based on their impact on the smooth functioning of the internal market, taking into account the different legal traditions in the various Member States.[4] It is essentially for this reason that the Directive includes a 'grandfather clause' in Article 5(3)(o), which allows Member States to retain existing (at the time of the adoption of the InfoSoc Directive) exceptions and limitations allowing uses of copyright works "in certain other cases of minor importance". Such uses shall be allowed insofar as they only concern analogue uses and do not affect the functioning of the internal market, without prejudice to the other exceptions and limitations harmonized by the remaining provisions in Article 5.[5]

B. National implementations: limitation to non-commercial uses

4 Several commentators have criticized the relatively weak harmonizing force of Article 5 of the InfoSoc Directive, with some even labelling the Directive as "a total failure, in terms of harmonization".[6] Since the adoption of the InfoSoc Directive, not only have some exceptions and limitations not been adopted in certain Member States[7], but also – and more seriously – national exceptions and limitations have been designed in such a way as to have diverging scope across the EU. The language employed by national legislatures, in fact, may not correspond to the language in the relevant exception or limitation at the EU level, or even provide for different conditions than the ones established at the EU level. An example in this sense is the restriction – at the national level but not at the EU level – to non-commercial uses of a copyright work in relation to certain exceptions and limitations.

5 It is true that *some* InfoSoc exceptions and limitations are limited to non-commercial uses of copyright works. They are: temporary copies (Article 5(1); the copies made must not have independent economic significance[8]); private copying (Article 5(2)(b)); reproductions by libraries, educational establishments, museums, and archives (Article 5(2)(c)); reproductions of broadcasts by social institutions (Article 5(2)(e), although the provision refers the lack of commerciality not to the use made, but rather the mission pursued by the institution at issue); illustration for teaching or scientific research (Article 5(3)(a)); use for the benefit of people with a disability (Article 5(3)(b); use for advertising the exhibition or sale of works of art (Article 5(3)(j), which prohibits any further commercial use).

6 However, there are national exceptions and limitations that only allow non-commercial uses of a copyright work, despite the lack of a corresponding requirement at the EU level. Instances of this tendency are numerous. This contribution intends to focus, as case studies, on quotation (Article 5(3)(d)) and freedom of panorama (Article 5(3)(h)), these being provisions that – at the level of individual Member States – have been implemented with significant differences, including with regard to the types of works eligible for the application of resulting exceptions and the possibility to only allow non-commercial uses. The experiences of systems belonging to different legal traditions – including common law countries (UK, Ireland), continental French-style systems (France, Italy, Belgium), Germany, and Nordic countries (Denmark,

4 InfoSoc Directive, Recital 31.

5 M van Eechoud *et al*, *Harmonizing European copyright law – The challenges of better lawmaking* (Wolters Kluwer:2009), p. 103. See also the discussion of the grandfather clause and flexibility under Article 5 in C Geiger – F Schönherr, 'Limitations to copyright in the digital age', in A Savin – J Trzaskowski (eds) *Research handbook on EU internet law* (Edward Elgar:2014), pp. 114-115.

6 PB Hugenholtz, 'Why the Copyright Directive is unimportant, and possibly invalid' (2000) 22(11) EIPR 499, p. 501. In the same sense, see MC Janssens 'The issue of exceptions: reshaping the keys to the gates in the territory of literary, musical and artistic creation', in E Derclaye (ed) *Research handbook on the future of EU copyright* (Edward Elgar:2009), p. 332, and bibliography cited in it. For similar criticisms expressed at the proposal stage, see M Hart 'The proposed directive for copyright in the information society: nice rights, shame about the exceptions' (1998) 20(5) EIPR 169, pp. 169–170.

7 For an overview of the various exceptions and limitations adopted by the individual Member States, see <http://copyrightexceptions.eu>.

8 In *Football Association Premier League Ltd and Others v QC Leisure and Others* (C-403/08) and *Karen Murphy v Media Protection Services Ltd* (C-429/08), EU:C:2011:631 ('*Football Association Premiere League*'), paras 174-179, the Court of Justice of the European Union ('CJEU') clarified that the notion of 'economic significance' refers to the fact that the use made of the copyright work by the defendant does not have any economic value other than the one inherent in the reception and viewing of the work. In this sense, see also *Public Relations Consultants Association Limited v The Newspaper Licensing Agency Limited and Others* [2013] UKSC 18, para 18.

Sweden) – will serve to appreciate the interpretative difficulties that arise with regard not just to the text of relevant provisions which limit the possible uses to non-commercial uses only, but also their judicial application.

7 Article 5(3)(d) of the InfoSoc Directive 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".*

8 Article 5(3)(h) allows Member States to permit the "use of works, such as works of architecture or sculpture, made to be located permanently in public places". There is no mention, in either provision, that the corresponding national implementations may be limited to non-commercial quotations or freedom of panorama.

I. Quotation

9 National transpositions of Article 5(3)(d) of the InfoSoc Directive vary substantially. For instance, Italian law (Legge 633/1941)[9] allows quotations insofar as they: are for the purpose of criticism or discussion or for educational purposes (in this sense the Italian approach is similar to its French counterpart which, however, does not exclude for-profit uses);[10] remain within the limits justified for such purposes; and do not conflict with the commercial exploitation of the work. With particular regard to the online dissemination of images and music, Article 70(1bis) of Legge 633/1941 only allows it for educational or scientific purposes, insofar as the dissemination is of low resolution or degraded quality, and only in the case in which such use is for non-profit ('lucro') purposes.

10 This approach differs from the one adopted by UK legislature, which in 2014 introduced into the Copyright, Designs and Patents Act 1988 ('CDPA') a self-standing quotation exception (section 30(1ZA)). Albeit framed within fair dealing (and not tested in court yet), section 30(1ZA) CDPA does not in principle exclude quotations for commercial reasons. The relevant provision requires in fact that: the work has been made available to the public; the use of the quotation is fair dealing with the work; the extent of the quotation is no more than what is required by the specific purpose for which it is used, and the quotation is accompanied by a sufficient acknowledgement (unless this is impossible for reasons of practicality or otherwise). There are no limitations as to the types of works that may be subject to the exception.[11]

11 Even more liberal are the approaches of Ireland, Belgium, Denmark, Sweden, and Germany. Section 52(4) of the Irish Copyright Act[12] states that "copyright in a work which has been lawfully made available to the public is not infringed by the use of quotations or extracts from the work, where such use does not prejudice the interests of the owner of the copyright in that work and such use is accompanied by a sufficient acknowledgement." Article XI.189 of the Belgian Code de Droit Économique, Article 22 of the Danish Copyright Act,[13] and Section 22 of the Swedish Copyright Act[14] allow anyone, in accordance with proper usage and to the extent necessary for the purpose, to quote from works which have been made available to the public. Similarly, Section 51 of the German Copyright Act[15] allows the reproduction, distribution and communication to the public of a published work for the purpose of quotation, so far as such use is justified to that extent by the particular purpose.

12 Quotation has been regarded by some as a 'right' (rather than an 'exception') because the language of Article 10(1) of the Berne Convention[16] appears to require Member States to authorize quotations of

9 Legge 22 April 1941, No. 633 Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (OJ No. 166 of 16 July 1941) – consolidated text as of 6 February 2016 (Legislative Decree 15 January 2016, No. 8).

10 Article L 122-5 No 3 (a) of the Code de la propriété intellectuelle – consolidated text as of 1 August 2017.

11 See A Cameron 'Copyright exceptions for the digital age: new rights of private copying, parody and quotation' (2014) 9(12) JIPLP 1002, pp. 1006-1007; YH Lee, 'United Kingdom copyright decisions and legislative developments 2014' (2015) 46(2) IIC 226, p. 235.

12 Copyright and Related Rights Act, 2000, OJ 28/2000.

13 Consolidated Act on Copyright 2014. An English of the Danish statute is available at <https://kum.dk/fileadmin/KUM/Documents/English%20website/Copyright/Act_on_Copyright_2014_Lovbekendtgoerelse_nr._1144__ophavsretsloven__2014__engelsk.pdf>.

14 Copyright on Literary and Artistic Works Act (1960:729). An English translation of the Swedish statute is available at <http://www.wipo.int/edocs/lexdocs/laws/en/se/se124en.pdf>.

15 Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz, as amended by Law of 4 April 2016). An English translation of the German statute is available at <https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html>.

16 By adopting the InfoSoc Directive, among other things, the EU intended to implement into EU legal order the WIPO Internet Treaties (Recital 15) The WIPO Copyright Treaty requires compliance with Articles 1 to 21 of the Berne Convention.

copyright works.[17] As argued elsewhere,[18] in the EU context it is doubtful whether the Berne Convention may trump the optional nature of the quotation exception in Article 5(3)(d) of the InfoSoc Directive. However, on consideration that quotation is part of the fundamental right to one's own freedom of expression/information as recognized by the European Convention on Human Rights[19] (Article 10) and the Charter of Fundamental Rights of the European Union[20] (Article 11), and freedom of expression/information also includes commercial expressions and information[21], one might wonder whether a Member State that limits its own quotation exception to non-commercial quotations (lacking a corresponding limitation at the EU level), not only might be in breach of its obligations under EU law,[22] but also human rights law. A national law that compressed freedom of expression/information (of which the act of quoting, as also acknowledged by the CJEU, is a manifestation)[23] beyond what is stated at the EU level would compress a fundamental freedom, and do so outside the conditions under which such compression is allowed.[24]

II. Freedom of panorama

13 Turning to freedom of panorama[25], France has recently introduced such exception into its own copyright regime (Article L 122-5 No 11 of the Code de la propriété intellectuelle),[26] but excluded its applicability to commercial uses. The provision, in fact, only allows reproductions and representations of works of architecture and sculpture, permanently located in public places and realized by physical persons, with the exclusion of any use that is directly or indirectly commercial.[27]

14 In this sense, French freedom of panorama differs from the more generous wording of the corresponding exception in UK law (section 62 CDPA). This provision applies to buildings, sculptures, models for buildings and works of artistic craftsmanship, if permanently

17 See J Cohen Jeroham, 'Restrictions on copyright and their abuse' (2005) 27(10) EIPR 359, p. 360; S von Lewinski, *International copyright law and policy* (OUP:2008), §5.163; P Goldstein - B Hugenholtz, *International copyright. Principles, law, and practice*, 3rd edn (OUP:2013), 391, R Xalabarder, 'The remunerated statutory limitation for news aggregation and search engines proposed by the Spanish Government – its compliance with international and EU law' (2014) IN3 Working Paper Series, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2504596&download=yes>, 2. Also speaking of a 'quotation right', see Written questions from the authorities of Belgium, Czech Republic, Finland, Hungary, Ireland and The Netherlands to the Council Legal Service regarding Article 13 and Recital 38 of the Proposal for a Directive on copyright in the Digital Single Market (25 July 2017), available at <http://statewatch.org/news/2017/sep/eu-copyright-directive-ms-questions-council-legal-service-25-7-17.pdf>.

18 E Rosati, 'Neighbouring rights for publishers: are national and (possible) EU initiatives lawful?' (2016) 47(5) IIC 569, pp. 588-589.

19 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended).

20 Charter of Fundamental Rights of the European Union, OJ C 364, pp. 1-22.

21 See however European Court of Human Rights, *Ashby Donald and Others v France*, application No. 36769/08, para 39, clarifying that commercial expression may be subject to further compression than other forms of expressions, e.g. of a political nature. On the interplay between copyright protection and freedom of expression in the jurisprudence of the European Court of Human Rights, see C Geiger – E Izyumenko, 'Copyright on the human rights' trial: redefining the boundaries of exclusivity through freedom of expression', 45(3) IIC 316, pp. 321-322. Highlighting the difficulty of extracting guidelines from relevant case law, see D Voorhoof, 'Freedom of expression and the right to information: implications for copyright' in C Geiger (ed), *Research handbook on human rights and intellectual property* (Edward Elgar:2015), pp. 348-349.

22 See further below sub §4, and E Rosati, 'Copyright in the EU: in search of (in)flexibilities' (2014) 9(7) JIPLP 585, pp. 597-598.

23 In *Eva-Maria Painer v Standard VerlagsGmbH and Others*, C-145/10, EU:C:2011:798 ('*Painer*'), paras 134-135, the CJEU stated that: "134. Article 5(3)(d) of Directive 2001/29 is intended to strike a fair balance between the right to freedom of expression of users of a work or other protected subject-matter and the reproduction right conferred on authors. 135. That fair balance is struck, in this case, by favouring the exercise of the users' right to freedom of expression over the interest of the author in being able to prevent the reproduction of extracts from his work which has already been lawfully made available to the public, whilst ensuring that the author has the right, in principle, to have his name indicated."

24 See also M Husovec, 'Intellectual property rights and integration by conflict: the past, present and future' (2016) 18 CYELS 239, p. 260, suggesting a reading of Article 51(1) of the Charter of Fundamental Rights of the European Union in the sense of imposing a re-adjustment of possible differing levels of protection of fundamental rights at national and EU levels in order to comply with what the Charter, as a primary source of EU law, requires.

25 For an overview of a number of national approaches (both at the EU and non-EU levels) to freedom of panorama, see <https://commons.wikimedia.org/wiki/Commons:Freedom_of_panorama>. See also A Bertoni – ML Montagnani, 'Foodporn: experience-sharing platforms and UGC: how to make copyright fit for the sharing economy' (2017) 39(7) EIPR 396, pp. 400-401.

26 The provision states: "Lorsque l'oeuvre a été divulguée, l›auteur ne peut interdire [...] Les reproductions et représentations d›œuvres architecturales et de sculptures, placées en permanence sur la voie publique, réalisées par des personnes physiques, à l›exclusion de tout usage à caractère commercial."

27 For a critical assessment of the French exception, including in relation to the InfoSoc Directive, see C Manara, 'La nouvelle «exception de panorama». Gros plan sur l'Article L. 122-5 10 du code français de la propriété intellectuelle' (2016) 4049 Revue Lamy Droit de l'Immatériel 40, §2.

situated in a public place or in premises open to the public. It provides that copyright in such works is not infringed by: making a graphic work representing it; taking a photograph or film of it; or making a broadcast of a visual image of it. Nor is the copyright infringed by the issue to the public of copies, or the communication to the public, of anything whose making was not a copyright infringement. The French exception is also narrower than the Belgian provision, i.e. Article XI.190(2/1°) of the Code de Droit Économique. Introduced in 2015, Belgian freedom of panorama, while incorporating the language of the three-step test, does not necessarily exclude commercial uses.

15 With regard to Swedish law, Section 24(1) of the Swedish Copyright Act provides that works of fine art may be reproduced in pictorial form if they are permanently located outdoors on, or at, a public place. The provision does not appear to exclude commercial uses. An even more generous wording can be found in the German Copyright Act, where Article 59 clarifies that freedom of panorama is not limited to certain categories of works. In fact, the provision allows the reproduction, distribution, and making available to the public of works located permanently in public roads and ways or public open spaces. In the case of buildings, this authorization shall only extend to the façade. The wording of the Irish exception allowing freedom of panorama (section 93 of the Irish Copyright Act) is substantially identical to the UK provision. The Danish exception (Article 24(3) of the Danish Copyright Act), although limited to buildings, does not set any particular restrictions to the reproduction (only allowed in pictorial form) of eligible works and their making available to the public.

C. Commercial and non-commercial uses

16 Standing the decision of certain legislatures to limit the availability of exceptions to non-commercial uses of a work, resulting provisions do not clarify what is to be intended as a 'commercial' or 'for-profit' use. As a result, uncertainties might subsist regarding the actual availability of a given exception in some cases. A further complexity, especially in the context of cross-border availability and exploitation of copyright content, may be due to the fact that, while a certain use of a work may be shielded from liability by means of an exception available under a particular EU Member State's copyright law, the same act might be deemed unlawful under the law of another EU Member State. To this one should add that the Court of Justice of the European Union ('CJEU') has shown an increasing uneasiness towards national exceptions whose language and scope depart from what is established in Article 5 of the InfoSoc Directive. In light of recent case law, it is questionable whether national legislatures are actually entitled to limit the availability of national exceptions to non-commercial uses of a work, lacking a corresponding limitation at the EU level.[28]

17 The different conditions of national exceptions and limitations thus raise issues of compatibility with EU law, as well as pratical difficulties when it comes to determining the lawfulness of certain uses of a copyright work. Taking quotation and freedom of panorama as examples, the following case studies highlight the potential shortcomings deriving from this situation, which might become particularly challenging in the online environment. The first case study addresses the lawfulness (in principle) of making and disseminating a GIF/meme derived from a copyright work over the internet, and considers the relevant treatment under the quotation exceptions of the Member States mentioned above. The second case study tackles the lawfulness (in principle) of taking and posting on a publicly accessible website the photograph of a copyright-protected scupture permanently located on public display. While other exceptions and limitations might be potentially available in the latter scenario (including quotation and incidential inclusion of copyright material), consideration is limited to the relevant treatment under the freedom of panorama exceptions envisaged in the laws of the Member States mentioned above.

I. The making of a GIF/meme from a copyright work and its online dissemination

18 A GIF (graphic user interface) is a computer file format for the compression and storage of visual digital information. Usually, GIFs are made from video files thanks to several tools available online (e.g. Wondershare Filmora, GIPHY, Photoscape, etc). Although potentially GIFs can have any length chosen by their maker,[29] they generally last a few seconds. Unlike GIFs, memes do not represent moving images, but rather captioned pictures or videos whose meaning is often distorted for satirical and humorous purposes. Popular examples include 'Condescending Wonka',[30] 'Xzibit Yo Dawg',[31] and the 2017 meme sensation known as 'Distracted

28 See further sub §4.

29 A GIF can potentially take even 1,000 years to play: see <https://nextshark.com/juha-van-ingen-janne-sarkela-longest-gif/>.

30 See <http://knowyourmeme.com/memes/condescending-wonka-creepy-wonka>.

31 See <http://knowyourmeme.com/memes/xzibit-yo-dawg>.

Boyfriend'.[32]

19 With regard to GIFs and memes, the question that arises is whether their creation can fall under the scope of copyright protection or possibly protection by means of a *sui generis* right (as per the possibility expressly left open to Member States by Article 6 of Directive 2006/116, i.e. the Term Directive[33]) and, if so, whether permission from the relevant rights owner may be needed for their use. The question further becomes whether the reproduction at stake in a GIF (a video that lasts a few seconds) or in a meme is such as to fall within the scope of reproduction or reproduction in part under Article 2 of the InfoSoc Directive. The answer is in the affirmative, as long as the work or part thereof thus reproduced is "its author's own intellectual creation",[34] i.e. is sufficiently original, in the sense that it carries its "author's personal touch"[35] and is ultimately the result of "free and creative choices".[36] However, for photographs protected by means of *sui generis* rights pursuant to the freedom left to Member States by Article 6 of the Term Directive, there is not even a requirement that they possess a sufficient degree of originality.[37]

20 There is no particular reason to exclude *ex ante* that a video (or part thereof) or image reproduced in a GIF or meme would not possess the required level of originality and be, as such, excluded from copyright protection. In such case, in fact, the act of reproduction at issue in the GIF or meme would be under the exclusive control of the copyright owner, with the exclusion of situations governed by relevant copyright exceptions and limitations. In this regard, depending on the use made and by whom, as well as whether the reproduction is verbatim or altered, different exceptions and limitations might come into consideration, including parody (if the reproduction is altered and constitutes an expression of humour or mockery)[38] and quotation (especially – although potentially not only[39] – if the reproduction is unaltered). With particular regard to the latter, and without engaging in a discussion of whether a quotation can be self-standing or rather needs to be incorporated into the user's work,[40] what is the relevant treatment of a GIF or meme made by someone other than the copyright owner and shared on, say, one's own blog? The answer may differ depending on the law applicable to the case at issue.

21 If the blog is in fact run for profit, e.g. because it displays advertisements and/or makes available items for sale/download, then it might be argued that the display of a good GIF or meme might contribute to making the overall blog environment more attractive and, as a result, contribute to the overall profit-making intention of its owner. Such a broad interpretation of profit finds support in CJEU case law which, in the context of decisions on the right of communication to the public within Article 3(1) of the InfoSoc Directive, has suggested that the presence of a profit-making intention should be assessed not having regard to the specific act of communication at hand, but rather the broader context in which the act is performed. It follows that the use made of the work might be regarded to be profit-driven and, as a result, commercial.

22 In such an interpretative context, should Italian law apply, it could be difficult to invoke successfully the exception within Article 70(1bis) of Legge 633/1941. The Italian quotation exception requires, for the online dissemination or images and music, that this is: for educational or scientific purposes; of low resolution or degraded quality; and for non-profit purposes. Part of scholarly literature suggests that the notion of 'lucro' (profit) is narrower than

32 For background information regarding this viral meme, see <https://petapixel.com/2017/09/18/story-behind-viral-distracted-boyfriend-meme-photo/>.

33 Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights (codified version), OJ L 372, pp. 12-18.

34 *Infopaq International A/S v Danske Dagblades Forening*, C-5/08, EU:C:2009:465, paras 33-39.

35 *Painer*, cit, para 92.

36 *Ibid*, para 89, referring to *Football Association Premier League*, cit, para 98.

37 For instance, Articles 87-92 of Legge 633/1941 set the scope of protection for 'simple' photographs ("other photographs" to use the language of the directive), which lasts for twenty years from the production of the photograph.

38 In its decision in *Johan Deckmyn and Vrijheidsfonds VZW v Helena Vandersteen and Others*, C-201/13, EU:C:2014:2132, para 33, the CJEU clarified that "the essential characteristics of parody, are, first, to evoke an existing work, while being noticeably different from it, and secondly, to constitute an expression of humour or mockery."

39 In mid-2017 Germany's Federal Court of Justice (Bundesgerichtshof - BGH) made a reference to the CJEU asking, among other things, whether the exception within Article 5(3)(h) of the InfoSoc Directive requires a quotation to be an unaltered reproduction of part of the original, or also allows the reproduction not to be identical. The case referred is: Beschluss des I. Zivilsenats vom 27.7.2017 – I ZR 228/15 (see <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2017&Sort=3&nr=79067&pos=0&anz=124>).

40 In *Painer, cit*, paras 130 and 137, the CJEU held that a quotation within Article 5(3)(d) of the InfoSoc Directive does not require that the material which quotes a work or other protected subject-matter is not a literary work protected by copyright. However, quotation exceptions like the French one (Article L-122-5(3)(a) of the Code de la propriété intellectuelle) allow quotations insofar as they clearly indicate the name of the author and the source, and are justified for by the critical, polemic, educational, scientific or information of the work in which they are incorporated. For further discussion, see P Jougleux & TE Synodinou, 'Holograms and intellectual property law: a multidimensional issue' (2016) 38(8) EIPR 492, pp. 494-495.

that of commercial exploitation (to be intended under Italian copyright law as use of a work that competes with the one of the original work) and, therefore, that the applicability Article 70(1bis) is not necessarily excluded in a commercial context.[41] However, the degradation requirement – together with the restriction to certain, specified uses (this would be the case also under French law) – makes the exception applicable to a limited number of cases, and arguably not in a situation like the one considered in this section. This conclusion is further supported by CJEU case law, which intends the notion of 'lucro' (profit) broadly and, as a result, may make the exception unavailable in several instances, including the one at hand.

23 In the UK context, lacking a judicial interpretation of section 30(1ZA) CDPA, the case at issue would be assessed under the lens of fair dealing, also considering that the statute does not require the quotation to be for any particular purpose ("whether for criticism or review or otherwise"). The CDPA does not define the concept 'fair dealing', nor does it stipulate what factors are to be considered when assessing whether a certain dealing with a work is to be considered fair. The notion of 'fair dealing' has been thus developed though case law from the perspective of a "fair-minded and honest person",[42] and has been traditionally considered a matter of degree and impression.[43] A number of considerations may inform the decision whether a certain use of a work is fair, although the relative importance of each of them will vary according to the case in hand and the dealing at issue.[44] One of the most relevant considerations is not whether the use of the work at issue is motivated by profit, but rather whether "the alleged fair dealing is in fact commercially competing with the proprietor's exploitation of the copyright work, a substitute for the probable purchase of authorised copies, and the like".[45] In the example discussed in this section, it may be doubtful whether a GIF or meme could be regarded as competing with the original video/film and whether a captioned meme is a potential substitute for the probable purchase of authorized copies of the original video or photograph.

41 See C Sappa, 'Articolo 70 L. 22 aprile 1941, n. 633 (legge autore)', in LC Ubertazzi (ed), *Commentario breve alle leggi su proprietà intellettuale e concorrenza*, 6th edn (CEDAM:2016), pp. 1730-1732.

42 *Hyde Park Residence Ltd v Yelland and Others* [2001] Ch 143.

43 *Hubbard v Vosper* [1972] 2 QB 84.

44 See L Bently & B Sherman, *Intellectual property law*, 4th edn (OUP:2014), p. 224. See also R Arnold & E Rosati, 'Are national courts the addressees of the InfoSoc three-step test?' (2015) 10(10) JIPLP 741, p. 748; S Jacques, 'Are the new 'fair dealing' provisions an improvement on the previous UK law, and why? (2015) 10(9) 699, p. 703.

45 *The Right Honourable Paddy Ashdown, MP PC v Telegraph Group Ltd* [2001] EWCA Civ 1142, para 70.

24 The assessment under Irish, Belgian, Danish, Swedish, and German laws might be more straightforward, in the sense that these Member States' exceptions are substantially in line with what is required at the EU level, and the relevant analysis would be one that takes into account the boundaries of the three-step test, rather than the purpose of the quotation, whether this is for commercial or for-profit reasons, or fair dealing with the original work.

25 From the discussion above it becomes apparent that determination of the law applicable to a case like the one described might become key, in that the same use of a given work might be regarded as infringing in one Member State but not in another.

II. The taking and posting on a publicly accessible website of the photograph of a copyright-protected sculpture permanently located on public display

26 Difficulties similar to those highlighted above would also subsist in relation to the different scope of national exceptions allowing freedom of panorama. In the event of a reproduction made of a publicly located sculpture, for instance, the Danish exception allowing freedom of panorama would be inapplicable at the outset due to the fact that the provision is limited to buildings.

27 Unlike – for instance – the UK exception within section 62 CDPA, the recently introduced French exception on freedom of panorama does not cover reproductions made by subjects other than physical persons and for reasons other than non-commercial ones. If one again interprets the concept of 'profit' broadly (as the CJEU appears to have done and the wording of the French provision confirms, by excluding uses that are directly or also merely indirectly commercial), then the applicability of the exception (not yet tested in court) would be likely excluded in relation to any reproductions done in a profit-making or commercial context, e.g. even a blog or online project that displays advertisements.

28 The wording of the UK freedom of panorama exception (section 62 CDPA) is such as to set a broader scope than the French provision, although this is potentially narrower than its InfoSoc counterpart. In fact, while the latter uses the phrase "*such as* works of architecture or sculpture" (emphasis added), similarly to the French, Belgian and Swedish provisions and unlike the case of the German provision, section 62 CDPA is limited to

specified categories of works.[46] However, unlike the InfoSoc provision, the UK exception applies to buildings irrespective of their location.[47] This said, it is worth highlighting that the UK provision is not even framed within fair dealing. Notwithstanding potential uncertainties regarding the definition of the concepts used by UK legislature (and also the fact that there has been no real judicial application of the provision to date), there is no reason to exclude that the defence would not also be available to reproductions done for commercial reasons, as has been the case under UK law since the 1911 Copyright Act.[48] In any case, however, the application of section 62 CDPA (and the Irish exception) could be subject to additional considerations, including the three-step test in Article 5(5) of the InfoSoc Directive. This would be the case should one conclude that Article 5(5) is not just aimed at national legislatures when transposing the InfoSoc Directive into their own copyright systems, but also national courts when applying the resulting national exceptions and limitations.[49] Unlike other Member States, the UK has not transposed the language of the three-step test within Article 5(5) of the InfoSoc Directive into its own copyright law. The reason is that, at the time of implementing the InfoSoc Directive into its own legal system, the UK Government took the view that relevant copyright exceptions already complied with Article 5(5)[50] and the notion of 'fair dealing' would be substantially the same as what is required under the three-step test.[51] It is possibly due to this consideration that in UK case law the InfoSoc three-step test has received limited consideration over time.[52]

29 A direct application of the three-step test in relation to freedom of panorama may be found in a recent (2016) decision of the Swedish Supreme Court.[53] In a dispute involving a Swedish collecting society and the operator of an online publicly accessible free database over the reproduction and making available, by the latter, of copyright works to which the former administers the relevant rights, the Supreme Court ruled that section 24(1) of the Swedish Copyright Act does not go as far as granting an online publicly accessible database the right to make photographs of artworks located permanently outdoors or in public spaces available to the public. According to the court, the value of exploiting works through the internet should be reserved – arguably in any situation – to copyright owners: an unauthorized communication to the public, e.g. by means of a publicly accessible database, would unreasonably compress the authors' legitimate interests.[54] As such, allowing such use of a copyright work without providing, at least, for any compensation to the copyright owner, would go against the three-step test in the InfoSoc Directive. The decision of the Supreme Court was applied by the referring court in 2017.[55]

D. Assessment of national exceptions limited to non-commercial uses

30 The assessment of national exceptions that – lacking a requirement in this sense in the InfoSoc Directive – only allow non-commercial uses of copyright content should be undertaken from both the point of view of their practical effects and their lawfulness under EU law.

46 R Burrell – A Coleman, *Copyright exceptions: the digital impact* (CUP:2005), pp. 233-234. See also, M Iljadica, 'Copyright and the right to the city' (2017) 68(1) NILQ 59, p. 74.

47 On the scope of section 62 CDPA, see further G Davies *et al*, *Copinger and Skone James on copyright*, 17th edn (Sweet&Maxwell:2016), Vol I, §§9.266-9.268.

48 As explained by M Iljadica, 'Copyright and the right to the city' (2017), *cit*, pp. 70-71, despite concerns that arose during the Parliamentary debate regarding third-party commercial exploitation of artworks placed in public, the UK legislature eventually opted for a broad public placement exception.

49 See Arnold & Rosati, 'Are national courts the addressees of the InfoSoc three-step test?', *op. cit.* See also, arguing that the question of the addressees of the InfoSoc three-step test remains open, J Griffiths, 'The "three-step test" in European copyright law – problems and solutions' (2009) 2009/4 IPQ 428, p. 431.

50 Arnold & Rosati, 'Are national courts the addressees of the InfoSoc three-step test?', *op. cit.*, p. 743.

51 *England and Wales Cricket Board Limited and Others v Tixdaq Limited and Another* [2016] EWHC 575 (Ch), para 89. Wondering whether this decision signals beginning of more frequent references to the three-step test in UK case law, see I Fhima, 'Fairness in copyright law: an Anglo-American comparison' (2017) 34 Santa Clara High Tech LJ 44, p. 51.

52 See E Rosati, 'To what extent do current exclusions and limitations to copyright strike a fair balance between the rights of owners and fair use by private individuals and others? - UK Report, in *LIDC contributions on antitrust law, intellectual property and unfair competition* (forthcoming: Springer), available at <http://www.ligue.org/uploads/documents/Cycle%202017/rapports%20B%20Rio/UKB.pdf>, §3.

53 Swedish Supreme Court, Case No. Ö 849-15, 4 April 2016. An English translation of the decision is available at <https://upload.wikimedia.org/wikipedia/foundation/e/ec/TheSwedishSupremeCourtsDecisionBUSvWikimediaFINAL-English_Translation.pdf>.

54 However, according to a survey conducted by Wikimedia in 2017 among over 600 Italian-based architects (as a EU Member State, Italy has not expressly implemented Article 5(3)(h) of the InfoSoc Directive, but see G Cavagna di Gualdana, 'Freedom of panorama in Italy: does it exist?' (14 July 2017), The IPKat, available at <http://ipkitten.blogspot.com/2017/07/freedom-of-panorama-in-italy-does-it.html>), over 70% of respondents considered freedom of panorama in positive terms. A preliminary discussion of the survey results is available at <https://meta.wikimedia.org/wiki/Research:Freedom_of_panorama_survey_among_architects_of_Italy>.

55 Stockholms Tingsrätt Patent- och marknadsdomstolen, Case No. PMT 8448-14, 6 July 2017.

31 In relation to the former, it is necessary to understand how and where the line between commercial or for-profit uses and non-commercial uses of a copyright work should be drawn. In this sense, also CJEU case law stands as a demonstration of the complexities underlying such an evaluation. When determining whether the act of communication at issue falls within the scope of Article 3(1) of the InfoSoc Directive, the CJEU has placed increasing relevance on a number of considerations other than the two primary requirements of having 'an act of communication' directed to a 'public'. Such considerations include, among other things, whether the defendant has a profit-making intention. The CJEU has not yet examined the question whether and to what extent the concepts of 'for-profit intention' (in relation to exclusive rights) and commercial use (in relation to InfoSoc exceptions and limitations) overlap. However, relevant case law on the former shows – on the one hand – the difficulties of making such a determination and – on the other hand – that the notion of for-profit intention is broad.

32 In its relatively recent Grand Chamber judgment in *Reha Training v GEMA* (C-117/15), the CJEU considered the profit-making intention of the defendant somewhat reductively, stating that such criterion role is relevant, yet not decisive.[56] However, more recent decisions – notably *GS Media v Sanoma* (C-160/15)[57], *Stichting Brein v Filmspeler* (C-527/15)[58], and *Stichting Brein v Ziggo and XS4All Internet* (C-610/15)[59] – suggest that consideration of the profit-making intention of the defendant is central to the assessment of *prima facie* liability.[60] The Court has not yet clarified – in express terms – whether the profit-making intention of the defendant should be assessed having regard to the unauthorized restricted act put in place or, rather, the surrounding context in which the act is performed. Nonetheless it appears that the latter interpretation may be the one more in line with existing case law. In *SGAE v Rafael Hoteles* (C-306/05)[61], *Football Association Premier League Ltd and Others v QC Leisure and Others* (C-403/08) and *Karen Murphy v Media Protection Services Ltd* (C-429/08)[62], and *Reha Training v GEMA* (C-117/15)[63] the CJEU, in fact, considered that the profit-making nature of the communication at issue could be determined by considering that the defendants transmitted the relevant works in their own establishment (hotels, a public house, and a rehabilitation centre, respectively) in order to benefit therefrom and attract customers to whom the works transmitted would be of interest. The same approach has been maintained in more recent decisions. In *GS Media v Sanoma* (C-160/15), the Court granted the profit-making intention of the defendant a central role. Although it failed to elaborate further on how this should be assessed, from the first national applications of that judgment it appears that the context in which the act is performed is key to the determination of the profit-making intention of the defendant.[64] This finds further support in the recent decisions in *Stichting Brein v Filmspeler* (C-527/15) and *Stichting Brein v Ziggo and XS4All Internet* (C-610/15). In the former, the CJEU identified the profit-making intention of the defendant in the circumstance that the relevant multimedia player "is supplied with a view to making a profit, the price for the multimedia player being paid in particular to obtain direct access to protected works available on streaming websites without the consent of the copyright holders."[65] The more recent decision in *Stichting Brein v Ziggo and XS4All Internet* (C-610/15) substantially consolidates the CJEU position regarding the broad construction and centrality of the profit-making intention of the user/defendant.[66]

33 All this suggests that determining when a use is 'commercial' or 'for-profit' might prove particularly challenging, especially in situations in which the for-profit or commercial aspect is merely indirect or ancillary to the contested use. Removing at the outset any possibility of a commercial or for-profit use of a certain work may thus contribute to the overall complexity and uncertainty of the system.[67]

56 *Reha Training Gesellschaft für Sport- und Unfallrehabilitation mbH v Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte eV (GEMA)*, C-117/15, EU:C:2016:379 ('*Reha Training*'), para 49, recalling *Football Association Premier League*, para 204.

57 *GS Media BV v Sanoma Media Netherlands BV and Others*, C-160/15, EU:C:2016:644.

58 *Stichting Brein v Jack Frederik Wullems*, C-527/15, EU:C:2017:300 ('*Filmspeler*').

59 *Stichting Brein v Ziggo BV and XS4All Internet BV*, C-610/15, EU:C:2017:456.

60 See further E Rosati, 'The CJEU *Pirate Bay* judgment and its impact on the liability of online platforms' (2017) 39(12) EIPR 737, pp. 739-740.

61 *Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA*, C-306/05, EU:C:2006:479, para 44.

62 *Football Association Premier League*, *cit*, paras 205-206.

63 *Reha Training*, *cit*, paras 63-64.

64 *Rebecka Jonsson v Les Éditions de l'Avenir SA*, FT 11052-15 (Sweden); LG Hamburg, 310 O 402/16 (Germany). See further E Rosati, '*GS Media* and its implications for the construction of the right of communication to the public within EU copyright architecture' (2017) 54(4) CMLRev 1221, pp. 1237-1238.

65 *Filmspeler*, *cit*, para 51.

66 See further Rosati, 'The CJEU *Pirate Bay* judgment and its impact on the liability of online platforms', *cit*, pp. 739-740. See also the discussion in P Savola, 'EU copyright liability for internet linking' (2017) 8(2) JIPITEC 139, pp. 145-146.

67 This is in line with the European Commission's position regarding the proposal for a text and data mining exception: see further below.

34 Turning to consideration of the system of the InfoSoc Directive, two points arise. The first is whether the legislative restriction of the applicability of a certain exception to non-commercial uses of a work presents any particular advantages over the kind of assessment that, in any case, is required under the three-step test (especially if one deems it directed at Member States' courts) and national concepts of fairness and reasonableness. The second is whether, in light of the rationale underlying the adoption of the InfoSoc Directive as also interpreted by the CJEU, EU law actually allows Member States the freedom to introduce conditions in national copyright exceptions other than those envisaged at the EU level.

35 In relation to the first point (limitation to non-commercial uses only), uncertainties surrounding determination of what is to be regarded as commercial or for-profit use may exclude the availability of a certain exception at the outset. This issue has arisen not just at the national level, but also at the EU level. Under the umbrella of its Digital Single Market Strategy[68], the European Commission is engaged in the reform of the copyright *acquis*. Among other things, its proposal for a Directive on Copyright in the Digital Single Market[69] contains provisions that, if adopted, would introduce new (mandatory) exceptions at the EU level, including a new exception allowing text and data mining (Article 3). In the Impact Assessment accompanying the proposal, the Commission concluded that the option of allowing both commercial and non-commercial text and data mining for scientific research would be preferable.[70] This is because an exception for commercial and non-commercial uses (although for a limited group of beneficiaries) alike would provide greater legal certainty and result in a reduction of transaction costs for researchers than what a non-commercial only option would do.[71] In particular, the option chosen by the Commission "would remove the legal uncertainty and the grey area as regards the research projects carried out by public organisations with a possible commercial outcome, including in cooperation of these organisations with private partners".[72]

36 In addition, the scrutiny undertaken under lenses such as fairness, reasonableness, and the three-step test (whose language some Member States have directly transposed into their own national laws),[73] would allow courts to determine whether the commercial exploitation at issue should be reserved for copyright owners. In this sense, an *ex ante* limitation to non-commercial uses might have limited sense.

37 Although the present analysis has focused on quotation and freedom of panorama, it appears possible to conclude more generally that, lacking a corresponding limitation at the EU level, it is doubtful whether Member States are actually entitled to have corresponding national exceptions only allowing non-commercial uses. As explained more at length elsewhere,[74] over time the CJEU has become particularly reluctant to consider national exceptions whose language and scope depart from the corresponding exceptions and limitations in the InfoSoc Directive compatible with EU law. By relying also on the (increasing) need to consider relevant concepts in exceptions and limitations as autonomous concepts of EU law, as well as prompted by internal market concerns, the CJEU has contested the lawfulness of a number of national exceptions and limitations whose scope differ from the one provided for in the InfoSoc Directive.[75] The approach of the Court is correct and in line with what is established at Recital 32 in the preamble to the InfoSoc Directive, i.e. that Member States should arrive at a coherent application of Article 5 exceptions and limitations. Except where so expressly provided by the Directive (e.g. Article 5(2)(c), which refers to 'specific acts of reproduction' to be defined at the national level), the InfoSoc Directive does not arguably allow Member States to alter the scope of the exceptions

68 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final.

69 Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market, {COM(2016)593}.

70 European Commission, Commission staff working document – Impact assessment on the modernization of EU copyright rules accompanying a Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market and Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, {COM(2016) 593} {COM(2016) 594} {SWD(2016) 302}, §4.3.2.

71 *Ibid*, §4.3.4.

72 *Ibid*.

73 Examples include France, Czech Republic, Greece, Hungary, Italy, Luxembourg, Malta, Poland, Portugal, and Slovakia: see L Guibault – G Westkamp – T RieberMohn, *Study on the implementation and effect in Member States' laws of Directive 2001/297EC on the harmonisation of certain aspects of copyright and related rights in the Information Society* (2012), Amsterdam Law School Research Paper No 2012-28, p. 57.

74 Rosati, 'Copyright in the EU: in search of (in)flexibilities', *cit*.

75 See, eg, *DR and TV2 Danmark A/S v NCB – Nordisk Copyright Bureau*, C-510/10, EU:C:2012:244 (Danish exception for ephemeral recordings made by broadcasters); *ACI Adam BV and Others v Stichting de Thuiskopie and Stichting Onderhandelingen Thuiskopie vergoeding*, C-435/12, EU:C:2014:254 ('*ACI Adam*', Dutch private copying exception); *Hewlett-Packard Belgium SPRL v Reprobel SCRL*, C-572/13, EU:C:2015:750 (Belgian private copying exception).

and limitations they have decided to import into national copyright regimes. An incoherent national drafting of exceptions and limitations frustrates the objectives that the EU intended to achieve by adopting the InfoSoc Directive, notably establishing a level playing field for copyright. It may also amount to a breach of Member States' obligations under EU law, including the doctrine of pre-emption.[76]

E. Conclusion

38 While some exceptions and limitations only allow non-commercial uses of a copyright work, a number of copyright exceptions and limitations within the InfoSoc Directive does not exclude in principle that a commercial use of a work rules out the availability of a certain exception. With particular regard to this group of exceptions and limitations, some national implementations have nonetheless resulted in the addition of a requirement that the use of the copyright work at issue must be a non-commercial or not-for-profit one. The present contribution has focused, as case studies, on quotation and freedom of panorama, and highlighted the shortcomings of such an approach, which appears overall questionable for a number of reasons.

39 First, diverging national implementations of InfoSoc provisions defeat the very goal underlying intervention at the EU level, i.e. harmonization of substantive copyright law. The InfoSoc Directive, as also interpreted by the CJEU, requires a greater degree of compliance with the scope of its provisions than what has been so far the case in practice. Over the past few years, the CJEU has highlighted that the incorrect transposition of relevant InfoSoc provisions frustrates internal market goals. A national exception or limitation limited to non-commercial uses of a copyright work could be regarded as equally inconsistent with the InfoSoc Directive, lacking such a limitation in the corresponding Article 5 provision thereof.

40 Secondly, as the discussion around an EU text and data mining exception also highlights, an *ex ante* exclusion of any commercial use of, may defeat important policy objectives, including legal clarity and reduction of transaction costs.

41 Thirdly, from a practical standpoint, determination of what amounts to a commercial or for-profit (and, as such, forbidden) use of a work may prove uncertain. Relevant CJEU case law on Article 3(1) of the InfoSoc Directive highlights the difficulty of determining a profit-making intention on the side of the defendant.

42 Finally, also in light of the three-step test, it does not appear correct to think that a commercial use of a work should always require the authorization of the relevant rightholder. Rather, the assessment should be more sophisticated, in the sense of entailing consideration, not of whether the use is driven by a particular intention or is for a particular reason *per se*, but rather what the effects on the market for the original work could be. In this sense, a use should be regarded as unlawful not because it is inherently commercial or driven by a 'profit-making intention', but rather because it is such as to result in the unreasonable diminution of lawful transactions relating to a protected work[77] and, therefore, in a violation of the three-step test.

76 On the rather embryonic doctrine of EU pre-emption, see R Schütze, *European constitutional law* (CUP:2012), p. 364, and P Craig – G de Búrca, (2015), *EU law – Text, cases and materials*, 6th edn (OUP:2015), pp. 84-85.

77 *Filmspeler*, *cit*, para 70, referring to *ACI Adam*, *cit*, para 39.

Where is the Harm in a Privacy Violation?

Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights

by **Bart van der Sloot***

Abstract: It has always been difficult to pinpoint what harm follows a privacy violation. What harm is done by someone entering your home without permission, or by the state eavesdropping on a telephone conversation when no property is stolen or information disclosed to third parties? The question is becoming ever more difficult to answer now that data gathering and processing initiatives have grown and are no longer focused on specific individuals, but on large groups or society as a whole. What specific harm is done by the NSA and other intelligence services gathering data on almost everyone or by the thousands of CCTV cameras registering the daily life of citizens on the corner of almost every street? There has been a longstanding debate within the literature regarding whether 'dignitary' or 'immaterial' harm should be protected under the right to privacy. Or should only harm that can be measured and quantified in monetary terms (economic harm) be taken into account? This article takes a descriptive and statistical approach to provide an insight into what types of damages are awarded, how they are calculated, and how the damages relate to the type of harm that is inflicted. It does so by analysing the damages awarded by the European Court of Human Rights with respect to privacy violations.

Keywords: Privacy; harm; damage; financial compensation; statistical analysis

Recommended citation: Bart van der Sloot, Where is the Harm in a Privacy Violation? Calculating the Damages Afforded in Privacy Cases by the European Court of Human Rights, 8 (2017) JIPITEC 322 para 1.

A. Introduction

1 In the field of privacy, the notion of harm has always been problematic as it is often difficult to substantiate the harm a particular violation has caused, e.g. what harm follows from entering a home or eavesdropping on a telephone conversation as such when neither objects are stolen nor private information disclosed to third parties? Even so, the traditional privacy violations (house searches, telephone taps, etc.) were often clearly demarcated in time, place, and person, and the effects are therefore relatively easy to define. In the current technological environment with developments such as Big Data, however, the notion of harm is becoming increasingly problematic.[1] Often, an individual is simply unaware that his personal data are gathered by either his fellow citizens (e.g. through the use of smartphones), by companies (e.g. by tracking cookies), or by governments (e.g. through covert surveillance). And if an individual does go to court to defend his rights, he has to demonstrate a personal interest, i.e. personal harm, which is a particularly problematic notion in Big Data processes, e.g. what concrete harm has the data gathering by the National Security Agency (NSA) done to an ordinary American or European citizen?[2]

* Senior Researcher at the Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Netherlands.

1 The standard work on harm: J. Feinberg, 'Harm to Others', Oxford University Press, Oxford, 1984. J. Feinberg, 'Offense to Others', Oxford University Press, Oxford, 1985. J. Feinberg, 'Harm to self', Oxford University Press, Oxford, 1986. J. Feinberg, 'Harmless Wrongdoing', Oxford University Press, Oxford, 1988.

2 B. van der Sloot, 'Privacy as virtue', Intersentia, Alphen aan de Rijn, 2017.

2 This example shows the fundamental tension between the traditional legal and philosophical discourse and the new technological reality – while the traditional discourse is focused on individual rights and individual interests, data processing often affects a structural and societal interest and in many ways transcends the individual. This article will analyse how the European Court of Human Rights (ECtHR) determines harm and compensation for harm with respect to infringements on the right to privacy as entailed in the European Convention on Human Rights (ECHR), Article 8: '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[3]

3 In order to gain such insights, a number of factors have been distinguished.[4] First, it is important that under the ECHR, the European Court of Human Rights (ECtHR) may grant three types of damages. First, compensation may be granted for the costs of the legal procedure itself – lawyers, travel costs, gathering documents, etc. Second, the Court may award damages for direct, material harm. For example, due to a privacy violation, a person has lost his job; or, when the police raids the home of a person without a warrant, they destroy a number of items in that home or damage the property. In such cases, financial compensation may be awarded to the victim in the form of pecuniary damages. Third, the ECtHR may award non-pecuniary damages, for what could be qualified as dignitary harm. Examples may be the very fact that the state or governmental official obtained certain personal information, even though that information has not been used or abused; or, the bodily or psychological integrity of a person is violated.

4 This article shows four things in particular. First, that the privacy approach under the European Convention on Human Rights stands in contrast with other jurisdictions, such as the American example, where privacy is mainly protected through tort law and applied primarily in horizontal relations.[5] Although tort law can in principle be used to award damages for dignitary harm, mostly, there has been a tendency in the United States to focus on material damages.[6] Under the European Convention on Human Rights, privacy is not approached as a concept that plays a role in horizontal relationships (for example between a consumer and a company), but in vertical relationships (between a citizen and a state). Privacy is approached as a human right, which the Court stresses is a concept that protects the autonomy, dignity, and personality of citizens.[7] Consequently, an analysis of the case law of the European Court of Human Rights shows how immaterial damages are calculated and in which types of cases they are granted.

5 Second, under Article 8 ECHR, different types of privacy are provided protection. The provision contains four concepts, namely private life, family life, home, and correspondence. Correspondence relates, for example, to the secrecy of letters and the freedom from eavesdropping on telephone conversations.[8] The protection of the home, protects citizens from states and governmental officials entering their home without a warrant.[9] Family life refers to the sanctity of the relationship between children and parents in particular, but may have a larger scope depending on the context. This concept protects, inter alia, against children being placed out of home, when that is not absolutely necessary. It also entails that parents should always be allowed to see their children, even, for example, when they are in prison.[10] The notion of private life is the broadest of all – which will be explained in more detail below – and refers to concepts such as bodily integrity, the protection of one's personality and one's reputation.[11] Finally, a new type of privacy has been developed by the ECtHR, which is economical privacy. This concept plays a role when material harm is inflicted, such as when the home is destroyed by an army, when property is confiscated, or when someone is fired from work.

3 <http://www.echr.coe.int/Documents/Convention_ENG.pdf>.

4 This article is the first output which will result in a book; the explicit goal is to gather comments and suggestions on the approach, methodology and results that are produced. The database is still preliminary and may contain marginal errors, which will nevertheless unlikely have a substantial impact on the figures featured.

5 J. Q. Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 The Yale Law Journal.

6 P. M. Schwartz & D. Solove, 'Reconciling Personal Information in the United States and European Union', California Law Review, 102, 2013.

7 B. van der Sloot, 'Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?', JIPITEC, 2014-3, p. 230-244.

8 <http://www.echr.coe.int/Documents/FS_Data_ENG.pdf>.

9 <http://www.echr.coe.int/Documents/Admissibility_guide_ENG.pdf>.

10 <http://www.echr.coe.int/Documents/Admissibility_guide_ENG.pdf>.

11 B. van der Sloot, 'Privacy as personality right: why the ECtHR's focus on ulterior interests might prove indispensable in the age of Big Data', Utrecht Journal of International and European Law, 2015-80, p. 25-50.

6 This article will show how damages are awarded in cases in which the different types of privacy are at stake. Are higher damages awarded in cases that revolve around the protection of the home than those regarding family life? Are more damages awarded in matters concerning the protection of private life than when the secrecy of communication is at stake? This analysis will yield that the infringement of certain aspects of privacy lead to higher sums of compensation than others. This means that, in general, the European Court of Human Rights interprets these infringements, for example of one's bodily integrity, as more harmful than the infringements on the sanctity of, for example, one's home. Because those damages are often awarded for immaterial damages, for dignitary harm, the question that can be drawn from this analysis is whether the Court feels a violation of one's bodily integrity is more harmful to one's dignity/personhood than a violation of, for example, one's home. Does the ECtHR prioritize between different types of privacy when it comes to awarding damages and if so, what are the implications?

7 Third, there are different grounds on which a violation of privacy may be found. If there is an infringement on the privacy of citizens – for example when the police enter the home of an individual – the European Court of Human Rights will apply a three-step test in order to assess whether the infringement has to be considered legitimate. First, the infringement has to be based on a legal provision and has to abide by the conditions laid down in that legal provision. The police cannot enter the home of a citizen without a legal basis – if it does so nevertheless, there will be a violation of the right to privacy under the European Convention on Human Rights.[12] Second, the infringement should serve a legitimate aim. The aims are enlisted in the second paragraph of Article 8 ECHR and include national security, public health, and the protection of the rights of other citizens. The police can, consequently, not enter the home of a citizen out of curiosity, even if it has a warrant and acts on a legal basis.[13] The third is that the infringement must be necessary in a democratic society – the police cannot enter the home of a citizen when that is not strictly necessary. One of the core questions in this respect is whether the infringement is proportionate to the goal pursued, and whether there are less intrusive means to reach the same goal – the so called subsidiarity principle.[14]

8 If either of these three conditions is not met, the infringement will qualify as a 'violation' of the European Convention on Human Rights, which means that the victim may ask for damages. This article will show whether higher sums of damages are awarded when, for example, the legal basis is lacking when the infringement does not serve a legitimate interest. This is of interest, because the different steps protect different values. The requirement of having a legal basis is rooted in the respect for the rule of law and the separation of powers – the executive branch can only use its power to infringe on the privacy of citizens when it has been authorized to do so by the legislative branch.[15] The requirement of the infringement being necessary in a democratic society, on the other hand, refers to the need to curtail the use of power by the state to the absolute minimum extent necessary – it essentially ensures that even if the executive branch has a legal mandate, it still has to abide by a set of minimum requirements.[16] This article will show how and when the ECtHR differentiates between awarding damages for a violation of privacy on the basis of each of these three requirements.

9 Fourth and finally, there are a number of factors taken into account which may tell more about when and why the European Court of Human Rights awards damages.

- The number of applicants. A claim may be lodged by one specific individual, a small group (such as a family) having suffered from the same privacy violation or by a larger group of people, for example when a substantial number of people have been affected by a certain governmental policy.

- The country against which the claim was lodged. There are currently 47 countries subjected to the European Convention on Human rights, all with their own background and, so to say, story. Different countries have a different approach to the right to privacy, and human rights in general.

- The type of applicant that has lodged the complaint. In general, the ECHR allows both natural persons, legal persons and groups to file an application for the violation of a human right. It will be analysed whether the type of applicant has an impact on the damages awarded.

12 Especially applied in mass surveillance cases: <http://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf>.

13 B. van der Sloot, 'How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one', Information & Communication Technology Law, 2015-1, p. 74-103.

14 J. Christoffersen, 'Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights', Human Rights and Humanitarian Law E-Books Online, Collection 2009.

15 G. Lautenbach, 'The rule of law concept in the case law of the European Court of human rights', Universiteit van Amsterdam, 2012.

16 See in comparison: <http://ysu.am/files/Davit_Melkonyan-1415702096-.pdf>.

- The chamber of the Court that deals with the complaint. The European Court of Human Rights is subdivided in number of chambers and compositions, which may have an impact on the damages awarded.

10 This article shows how these different factors and aspects influence the type of damage that is awarded for a privacy violation and the amount of damages attributed to victims. Is it by definition so that the higher the number of complainants, the higher the amount of damages awarded (per claimant)? Are certain countries required to pay more damages than others and does that mean that the violations inflicted on the citizens of these countries are more 'severe' than those inflicted on the citizens of other countries? Are natural persons awarded different types of damages than legal persons and if so, why? These are a few of the questions that will be addressed by this paper.

11 This study has analysed the cases about a potential violation of Article 8 ECHR, with which the ECtHR has dealt with in substance, after cases have been declared admissible (explained in section B. below). It is built on a database and SPSS analysis, providing statistical correlations. It focusses only on the damage awarded in cases in which a violation of Article 8 ECHR is established. Doing so, an indication is given on the potential harms the ECtHR acknowledges. The article takes a mainly neutral and 'data-driven' approach, although personal choices and subjective interpretation can of course never be avoided in full. The goal is to identify factors that may help in determining the amount of damage that is afforded per case, which may say something about the harm that is being acknowledged by the ECtHR.

12 Eight factors have been selected in order to evaluate the amount of damages awarded per case. These are: (1) the year in which the judgement was delivered by the Court (third section); (2) the country against which the complaint was lodged (fourth section); (4) the setting of the Court which delivered the judgement (fifth section); (5) the type and (6) the number of applicants (sixth section); the type of damage that is compensated (explained in the seventh section of this article); (7) the type of privacy at stake (eighth section); (8) and the grounds on which a violation was established (ninth section). Each section will be divided in three sub-sections. The first subsection will provide background information about the factor analysed and the methodological approach taken. The second subsection will provide the reader with the basic statistical information gathered from the database. The third subsection will provide a brief analysis and suggest some questions and issues for further research. The article will conclude with a summary of the most important findings (tenth section). The article will begin, in the next section, by providing the reader with some background information about the European Convention on Human Rights.

B. Background of the ECHR

13 The idea behind the ECHR was to adopt a legal instrument that could be invoked by citizens, legal persons, groups and other states alike; the European Court of Human Rights was installed to assess cases that were brought under the Convention. The Convention contains two modes of complaint: individual applications and inter-state complaints. The first mode of application is open to natural persons, legal persons (not being governmental institutions), and groups of natural persons.[17] The second mode is open to member states to the Convention.[18]

14 Under the Convention, a two-tier system exists. Originally, the system was as follows. First, the European Commission on Human Rights (ECmHR) would decide on the admissibility of cases and functioned as a mere filtering system.[19] It would not provide a substantial review of cases, but would reject those cases that were clearly unfounded, submitted out of time, fell outside the competence of the Court, etc. Second, if a case was declared admissible, the European Court of Human Rights could assess the content of the case and determine whether a state had violated one or more of the provisions contained in the Convention. Currently, the system has been changed somewhat; but although the Commission has ceased to exist, its tasks have been transferred to a separate division of the ECtHR.

15 Consequently, the two-tier model still exists, but is operated by two different sectors of the Court. It should be noted that this study has only analysed the substantive judgements of the ECtHR (the second-tier) and not the decisions on the admissibility of cases (the first-tier). Until now, over 1800 cases regarding the right to privacy under the ECHR have been dealt with in substance by the ECtHR;[20] by contrast, there have been over 4000 decisions on the admissibility of cases in which the right to privacy was invoked.[21] Of the over 1800 cases, those cases that have been delivered until 2010 have been

17 Article 33 ECHR.

18 Article 34 ECHR.

19 See for the original Convention <http://www.echr.coe.int/Documents/Collection_Convention_1950_ENG.pdf>.

20 <http://hudoc.echr.coe.int/eng#{"languageisocode":["ENG"],"article":["8"],"documentcollectionid2":["JUDGMENTS"]}>.

21 <http://hudoc.echr.coe.int/eng#{"languageisocode":["ENG"],"article":["8"],"documentcollectionid2":["DECISIONS"]}>.

analysed for this study, which make up about 1000.[22] The cases from 2010 onwards are not included yet – this article provides preliminary results. The cases are manually coded in the database, with the methodology explained according to each section.

C. Number of cases and violations

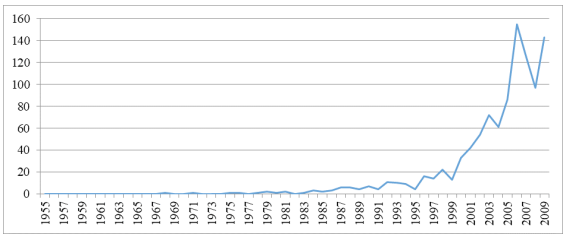
I. Introduction

16 The number of cases before the Court has been a matter of concern. The European Convention on Human Rights was initially drafted as a supra-national document providing relief to victims in ultimum remedium. The types of harms that were on the mind of the authors of the Convention related to the atrocities that took place during the Second World War and thereafter in fascist and communist regimes. Consequently, the idea was that only a handful of very serious cases would be submitted to the ECtHR. As will be discussed later on, the inspiration of the European Court of Human Rights was found in the International Court of Justice (ICJ), which still exists and only has a handful of cases per year. Over the years, however, the case load before the ECtHR has grown to a point that has become unbearable. Some changes to the rules of procedure and dealing before the Court have been made.[23] Although these changes to the Convention have not put a halt to the high numbers of cases, the exponential rise of cases has been stopped.

II. Results

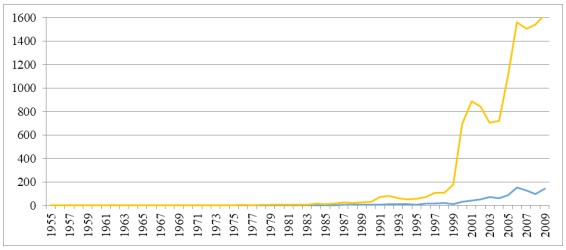
17 The importance of the right to privacy as protected under Article 8 ECHR and the European Convention on Human Rights in general, has increased over time. Likewise, the case load for the ECtHR has grown exponentially. In the 50 years from the moment the Convention was adopted in 1950 until 2000, the Court assessed 145 cases in substance on a potential violation of the right to privacy. In the year 2009 alone, 143 cases were assessed by the ECtHR with regard to a possible violation of Article 8 ECHR, as is shown in Figure 1.

18 **Figure 1: Number of cases in total on Article 8 ECHR:**



19 There are a number of potential reasons for this stark increase, such as: (1) there is a general societal tendency to use legal means to resolve disputes; (2) there is greater awareness among claimants and lawyers of the existence of, and possibilities under, the ECHR; (3) the Court has broadened the scope of the provisions under the Convention in its case law, so that more and more cases fall under the Convention's material scope (see also section H.); and (4) more countries have signed onto the Convention (section D.). Consequently, the increase in cases before the ECtHR is a general tendency, not particular to Article 8 ECHR, as is shown in Figure 2.

20 **Figure 2: Total number of cases compared to the cases on Article 8 ECHR:**

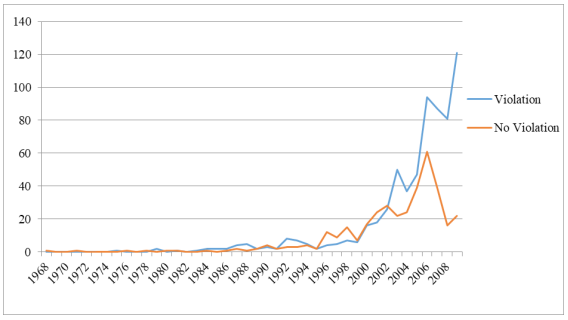


21 What is interesting to see here, is that the Court finds a violation of the right to privacy in a higher percentage of the cases before it over the years. Although until 2000, it held a violation of the right to privacy in about half of the cases under Article 8 ECHR, from the beginning of the new millennium, this has changed significantly, as evidenced by Figure 3 shown below.

22 <http://hudoc.echr.coe.int/eng#{"languageisocode":["ENG"],"article":["8"],"documentcollectionid2":["JUDGMENTS"],"kpdate":["","2010-01-01T00:00:00.0Z"]}>.

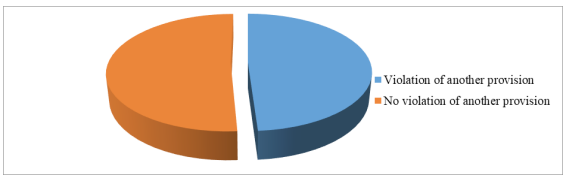
23 <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/140>; <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/155>; <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/204>; <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/194>; <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/213>; <http://www.coe.int/en/web/conventions/search-on-treaties/-/conventions/treaty/214>.

22 **Figure 3: The judgement of the ECtHR on the point: of a violation of Article 8 ECHR**



23 Importantly, most cases under the ECHR are combined complaints, either by multiple claimants and/or claims in which multiple provisions under the European Convention on Human Rights are invoked. For example, a claim might be that the government has violated the right to privacy (Article 8 ECHR) and has denied the right to a fair trial (Article 6 ECHR) of Mr. Black. Or, the government has violated the right to privacy of Mr. Black and has denied a right to a fair trial of Mr. Black, his son and his wife, who tried to defend their shared interests in court. Or, the toxic gasses emitted by a power plant violated the right to life (Article 2 ECHR) and the right to private life (Article 8 ECHR) of Mr. Jones, Mrs. Black, Mr. Smith, and 20 others living in the neighbourhood. Consequently, even in cases in which no violation of Article 8 ECHR was found, the Court will often establish a violation of another provision contained in the Convention. In about half of the cases in which Article 8 ECHR was invoked, but not violated, the ECtHR still found a violation of another provision of the European Convention on Human Rights.

24 **Figure 4: Percentage of the cases in which another article was violated or not, when Article 8 was assessed on the second tier, but no violation established:**



25 Importantly, one of the reasons that no violation in a case is found (when in second-tier), is because the case has been struck from the role. Article 37 ECHR specifies with this respect: '1. The Court may at any stage of the proceedings decide to strike an application out of its list of cases where the circumstances lead to the conclusion that (a) the applicant does not intend to pursue his application; or (b) the matter has been resolved; or (c) for any other reason established by the Court, it is no longer justified to continue the examination of the application. However, the Court shall continue the examination of the application if respect for human rights as defined in the Convention and the Protocols thereto so requires. 2. The Court may decide to restore an application to its list of cases if it considers that the circumstances justify such a course.'[24]

26 A case is generally taken from the role if the parties have come to an agreement, particularly when a Member State admits to having violated the Convention and possibly, to award damages. Article 39 ECHR specifies: '1. At any stage of the proceedings, the Court may place itself at the disposal of the parties concerned with a view to securing a friendly settlement of the matter on the basis of respect for human rights as defined in the Convention and the Protocols thereto. 2. Proceedings conducted under paragraph 1 shall be confidential. 3. If a friendly settlement is effected, the Court shall strike the case out of its list by means of a decision which shall be confined to a brief statement of the facts and of the solution reached. 4. This decision shall be transmitted to the Committee of Ministers, which shall supervise the execution of the terms of the friendly settlement as set out in the decision.'[25]

27 Of the 187 cases in which Article 8 ECHR was invoked and no violation of any provision under the Convention was established (not of the right to privacy, nor of any of the other rights under the Convention), 67 were not assessed in substance (even though they were in the second-tier), but struck from the role. Consequently, only in about 10% of the cases submitted to the ECtHR on a potential violation of Article 8 ECHR, the applicants leave empty-handed.[26] This is important because originally, it was thought that the ECmHR (its role was transferred to a chamber of the ECtHR by the 11th Protocol to the Convention) in the admissibility procedure (the first-tier) would filter cases on mainly procedural aspects and the ECtHR would judge in substance (the second-tier) whether a violation of the Convention has occurred. Currently, however, it seems that if a case passes the first-tier, there is a very high chance that a violation of the Convention will be established by the ECtHR. Thus, the real hurdle seems to be the first-tier, not the substantive evaluation of the second-tier.

28 Given the fact that the total number of cases has increased exponentially over the years and added to that, that from 2000 onwards, the ECtHR has held a violation of Article 8 ECHR in a significantly higher percentage of the cases before it, it should not come as a surprise that the majority of the damage

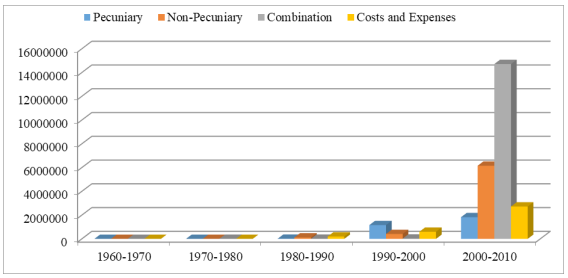
24 Article 37 ECHR.

25 On friendly settlements, see Article 39 ECHR.

26 Even with regard to these cases, some of them have been submitted to the Grand Chamber and repealed.

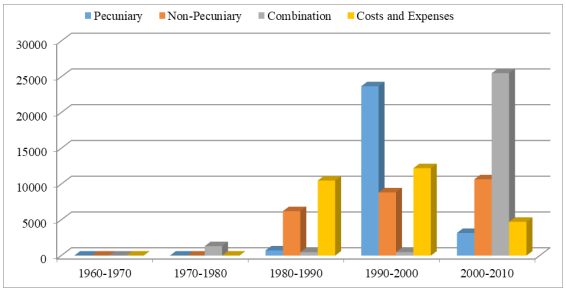
that has been awarded by the Court was granted in the last decennium. Especially the 'Combination' and the 'Non-Pecuniary' damages are high, as is evidenced by Figure 5 below. As will be explained in section G. in more detail, it is possible for the ECtHR to award pecuniary damages (for material harm), non-pecuniary damages (for immaterial harm), and it can award costs and expenses (for example travel costs or the costs for hiring a lawyer). Sometimes, it combines 2 or more types of damages into one amount (the combination category).

29 **Figure 5: Damages awarded in absolute numbers per decennium:**



30 What is interesting to see, however, is that the amount of damages awarded per case in which a violation was found is relatively stable, as can been seen in Figure 6. The non-pecuniary damage awarded per case has steadily but slowly increased over time. Perhaps more remarkable is that the costs and expenses awarded by the Court on average per case has dropped in the last decennium. Why this is remains unclear. From the comparison between the last two decennia it appears that the categories 'pecuniary damage' and 'combination of damages' are communicating vessels. When the pecuniary damages are high, the combination category is relatively low and vice versa. This should not come as a surprise, because both categories are particularly used in the same types of cases; for example, in a country where the homes of the applicants have been destroyed or been made inaccessible or villages have been evacuated by military means, thereby preventing the inhabitants from returning for years. Relatively large sums of money are granted by the ECtHR in these types of cases. Consequently, the larger part of the 'combination' category is presumably made up of pecuniary damage.

31 **Figure 6: Damages awarded relative to the amount of cases in which a violation was found per decennium:**



III. Analysis

32 The first point of interest is that the number of cases has increased over time. There are a number of obvious and unavoidable reasons for this. The number of states that have joined the Convention has grown substantially, and in general, the population of those countries has grown. In addition, there are certain societal tendencies, such as the increased juridification of society,[27] and the increased awareness of citizens of their rights in general, and of their rights under the European Convention in particular. These have all influenced the case load of the court. What is perhaps more important is that material scope of the rights under the Convention in general and of the right to privacy has grown substantially (see section H.) – this means that more cases will be declared admissible with respect to a claim regarding Article 8 ECHR. Although the Convention was originally drafted for claims relating to severe human rights infringements, there has been a tendency to increasingly allow claims about infringements of quite ordinary legal doctrines, such as, for example, the portrait right of individuals.[28] This means that the Human Rights Court is increasingly acting as a normal legal court on a European level, and acts increasingly as a court of fourth-instance (complementing the three instances normally provided on a national level).

33 In addition, as pointed out in the results section, the percentage of cases in which a violation is found by the European Court of Human Rights is quite high. The original idea behind the two-tiered system was that in first instance, the ECmHR or after the 11th Protocol entered into force, a separate chamber of the ECtHR, would filter cases on their admissibility. Has the case been submitted out of time? Have all domestic remedies been exhausted?

27 J. Habermas, 'Theorie des kommunikativen Handelns', Frankfurt am Main, Suhrkamp Verlag, 1981.

28 ECtHR, Bogomolova v. Russia, application no. 13812/09, 20 June 2017.

Does the claimant have standing? Has the case already been judged by the ECtHR? These are all mainly procedural aspects, leaving the substantive analysis of the case to the European Court of Human Rights in the second-tier. There is one criterion in the first-tier that touches on the content – cases can be declared inadmissible if the claim is 'manifestly ill-founded'.[29] Originally, this ground would rarely lead to the inadmissibility of cases. Now, however, it is used more and more by the Court in the first-tier to already do a substantive analysis of the matter before it and reject cases when they do not yield a violation of Article 8 ECHR.[30]

34 Finally, with respect to the damages awarded, three things are clear:

- Over time, more damage for non-pecuniary harm is awarded to victims. This can in part be explained as a correction for inflation, but not in its entirety. Because the increased number of cases before the Court can in part be explained by the fact that it has opened itself up for claims revolving around more ordinary legal conflicts, the increase of damages can presumably not be explained by the fact that the type of harm inflicted on victims has become more severe over time. The most appealing hypothesis seems that the European Court of Human Rights has shifted its approach, from offering mostly symbolic damages for non-pecuniary harm (as is a tradition in many European countries), towards a more substantial form of compensation.

- Second, the category of material harm and the 'combination' category are communicating vessels. Consequently, it seems logical to presume that most of the damages offered in the combination category actually consist of pecuniary damage.

- Third and finally, the costs and expenses awarded to victims has dropped in the last decennium analysed for this study. The reason for this is unclear. Have costs dwindled because access to justice is facilitated in the various countries? Has the digitisation of legal procedures had a positive effect on the costs of legal procedures? This could be a topic for further research.

29 Article 35(3)(a) ECHR.

30 See for example: ECtHR, Pihl v. Sweden, application no. 7472/14, 07 February 2017.

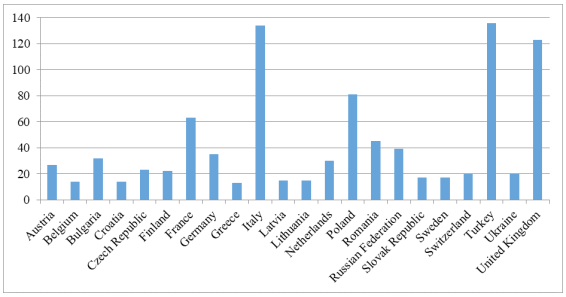
D. Countries

I. Introduction

35 The European Convention on Human Rights was adopted in 1950 by a small number of countries. Subsequently, it was ratified in the 1950's by thirteen states. It was only in the 1970s that a number of bigger European countries, in particular from the south, joined. In the 1990s the ECHR became the standard across Europe, especially because a number of Eastern-European countries joined. There are currently only a handful of European countries that have not ratified the Convention, such as Vatican City, Belarus, and Kazakhstan. It is important to stress, however, that even though countries have ratified the Convention, it is possible for them to make reservations, inter alia, with respect to the authority of the ECtHR. For example, although Turkey signed the Convention in 1954, it was only in 1995 that the ECtHR first assessed a case against Turkey (second-tier).

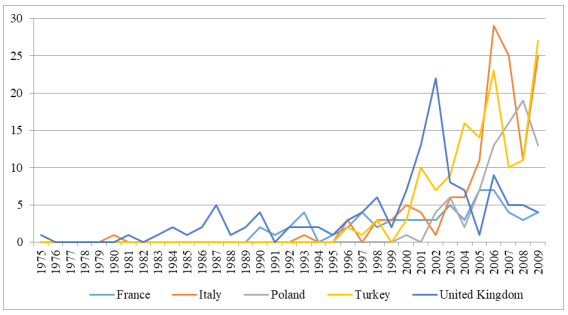
II. Results

36 Figure 7: Countries with 10 cases or more on a potential violation of Article 8 ECHR until 2010:



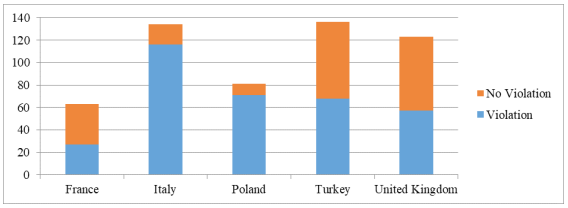
37 What is remarkable is that the majority of the Member States that have signed the Convention have been involved with no, or only a very limited number of cases regarding a potential violation of Article 8 ECHR. The ECtHR has assessed 10 complaints or more about a violation of Article 8 (second-tier) only with respect to 22 of the 47 countries that have ratified the Convention. The other 25 countries have been involved with no, or only a very limited amount of complaints against them regarding a potential violation of the right to privacy. And of these 22 countries, only 10 were involved in more than 30 cases. In fact, it is clear from Figure 7 that a handful of countries are responsible for most cases, namely Italy, Turkey and the United Kingdom, and to a lesser extent Poland and France.

38 **Figure 8: Number of cases regarding Article 8 ECHR per country per year:**



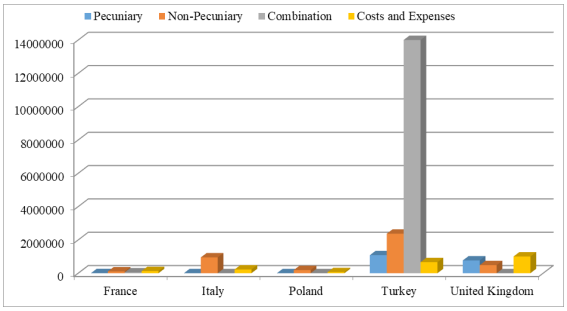
39 Figure 8 shows the number of cases per year with respect to France, Italy, Poland, Turkey, and the United Kingdom. It appears that France has quite a small but steady number of complaints per year, the United Kingdom seems to have peaked, in particular in 2001 and 2002, and that Italy, Poland and Turkey have been involved with cases regarding a potential violation of the right to privacy in particular in the new millennium; the first case ever assessed (second-tier) against Italy being in 1980, against Poland in 2000, and against Turkey in 1996. It is important to emphasize that there is an important difference between these five countries, as is evidenced by Figure 9. While France has not been convicted for a violation of the right to privacy in the majority of the cases lodged against it under Article 8 ECHR, Turkey and the United Kingdom are held in violation for about 50% of cases, and Italy and Poland are held in violation of the Convention in the majority of the cases.

40 **Figure 9: Number of cases in which the ECtHR has or has not established a violation of Article 8:**



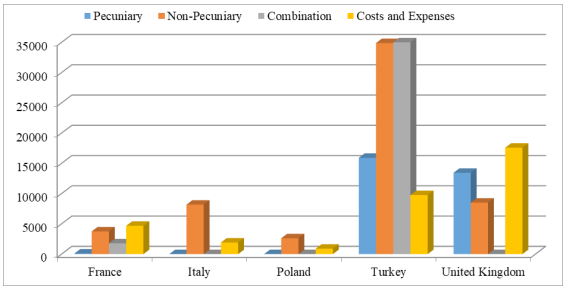
41 There are a number of other countries with a poor track record. Of the 27 cases (second-tier) regarding a potential violation of Article 8 ECHR against Austria, the ECtHR established a violation in 23 of those cases. For Bulgaria, this was 24 of the 32 cases, for Finland 14 of the 22 cases, for Germany 20 of the 35 cases, for Latvia, 12 out of 15, for Lithuania,14 out of 15, for Romania 31 of the 45 cases, for Russia 30 out of 39, and both Switzerland and the Ukraine were held in violation of Article 8 ECHR in 14 of the 20 cases lodged against them under this provision. In fact, 467 of the 647 cases in which the Court has found a violation of Article 8 ECHR (almost 75%), involved either one of these 10 countries: Austria, Bulgaria, France, Germany, Italy, Poland, Romania, Russia, Turkey, and United Kingdom. The remaining 37 countries are responsible for the other 25 % of the violations of Article 8 ECHR.

42 **Figure 10: Total amount of damages awarded per category per country:**



43 If the 5 countries are analysed against which the most cases under Article 8 ECHR were assessed by the European Court of Human Rights, it appears that there exists a significant difference between them. While Poland is the country, which is held in violation of Article 8 ECHR most often after Italy, it is required to pay only minimal damages. Italy is primarily required to compensate non-pecuniary damages, while the United Kingdom has to pay quite significant amounts for both material and immaterial damages, and for the costs and expenses. Turkey is the champion on the point of both material and immaterial costs, and in particular the 'Combination' category, the reason for which was already explained above. Figure 10 shows the total amount of damages the countries had to pay in cases in which a violation of Article 8 ECHR was found. Figure 11 shows the total amount of damages per country divided by the number of cases in which a particular country was held in violation of Article 8 ECHR. The category 'Combination' in the case of Turkey was € 208.721 on average per case in which the Court considered that it had violated the right to privacy of its citizens (not included in full in figure 11 for reasons of legibility).

44 **Figure 11: Total damages awarded divided by amount of cases a country was held in violation of Article 8 ECHR:**



III. Analysis

45 From the previous results, three important conclusions may be drawn. First, a number of countries are responsible for by far the most cases before the European Court of Human Rights (second-tier) regarding a potential violation of the right to privacy (Article 8 ECHR). This picture is to a large extent a representation of all cases before the Court, but there are important differences. Turkey is the champion in terms of the number of cases brought against it under the European Convention on Human Rights (with 2296 cases until 2010), followed closely by Italy (2023 cases), and then Russia (863 cases), France (774 cases), Poland (767 cases), Romania (648 cases), Ukraine (608 cases), Greece (558 cases), and the United Kingdom (422 cases). Consequently, the most remarkable feature seems that a relatively large part of the cases against the UK regard a potential violation of privacy (122 of the 422 cases). With Turkey, this is only 128 of the 2296 cases, and for Italy 135 of the 2023 cases, which can be seen as relatively low numbers. Consequently, some countries are involved with a significantly higher percentage of cases on privacy than others. One of the reasons that the United Kingdom may stand out in this respect may be that until late in the previous century, it had quite Victorian policies towards sexual minorities, such as homosexuality and transgender people, and towards non-biological forms of reproduction, such as artificial insemination and surrogate parenthood. Many of the cases against the UK revolve around matters such as homosexuality in the army, BDSM practices, assisted suicide, the protection of transgender people, and the possibility for prisoners to create life through artificial insemination.

46 Second, it appears that some countries are held in violation of the right to privacy in a significantly higher percentage of cases than others. With respect to France, Turkey, and the United Kingdom, cases are declared admissible (first-tier), but no violation is found by the ECtHR (second-tier) in about half of the cases. This means that the questions concerning the matter of the case are considered serious and/or important enough to require a substantial analysis of the Court, allowing it to provide legal guidance to countries, without there necessarily being a violation. An example may be cases revolving around the issue of euthanasia. In Pretty v. the United Kingdom, the case was declared admissible, but no violation was found by the Court. Still, the fact that the case was declared admissible allowed the Court to lay down a legal framework for questions concerning assisted suicide.[31]

47 Finally, it is clear that one country in particular – namely Turkey – is responsible for the majority of damages being awarded in privacy cases before the European Court of Human Rights. This is especially true with respect to the material damages (also part of the 'combination' category). Regarding the United Kingdom, most damages are afforded with respect to the costs and expenses – apparently, legal procedures in that country are costly. In the cases of Poland and Italy, on the other hand, the awards for costs and expenses are negligible and most damages are offered with respect to non-pecuniary damages. Apparently, these countries violate the dignitary aspect of privacy more than other countries do.

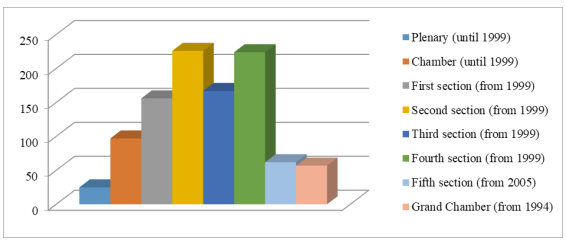
E. Courts

I. Introduction

48 Originally, the Court could convene either in a plenary setting or in a chamber. From 1999 onwards, the second-tier has been dominated by different sections (or chambers) of the Court, namely the first, the second, the third, and the fourth section. In fact, the possibility to judge cases in a plenary setting is now provided for by the possibility of a section to relinquish jurisdiction to the Grand Chamber when a case pending before it raises a serious question affecting the interpretation of the Convention, or where the resolution of a question before the Chamber might have a result inconsistent with a judgment previously delivered by the Court.[32] In 2005, a fifth section has been added. Although there should be no significant difference in how the different sections treat cases revolving around potential privacy violations, there are important variations nevertheless.

II. Results

49 **Figure 12: Amount of cases per setting of the court:**

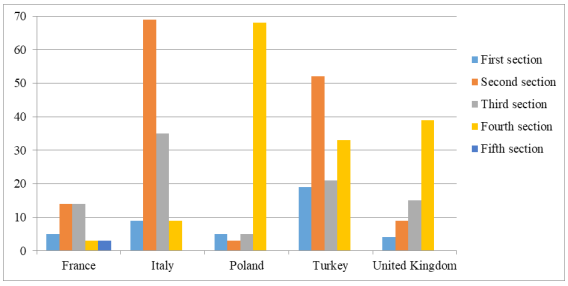


31 ECtHR, Pretty v. the United Kingdom, application no. 2346/02, 29 April 2002.

32 Article 30 ECHR.

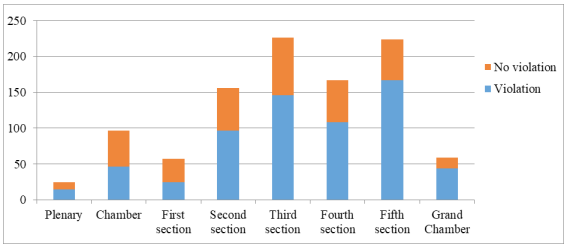
50 Officially, there is no separation of tasks between the different sections. Still, it is remarkable that the second and fourth section seem to deliver significantly more judgements on the question of a violation of Article 8 ECHR than the first and the third section. Maybe this is because there is, in fact, a separation of tasks between the sections. For example, the second chamber has delivered significantly more judgements on the point of family and relational privacy than the other sections. Likewise, the fourth section has delivered 76 out of the 187 cases on informational privacy. Another possibility is that certain sections deliver more judgements on particular countries than others. For example, of the 27 cases against Austria, 16 have been dealt with by the first section. Of the 32 cases against Bulgaria, 28 where dealt with by the fifth section. In a similar fashion, 13 of the 14 cases against Croatia have been dealt with by the first section, etc. It is unclear why this is, but it might have to do with the requirement that one of the judges sitting in the chamber dealing with the cases is of the nationality of the state against which the complaint is lodged.[33] It is remarkable that 22 of the 57 before the Grand Chamber involve a complaint against the United Kingdom.

51 **Figure 13: Number of cases a court has assessed a complaint in substance on Article 8 ECHR per country:**

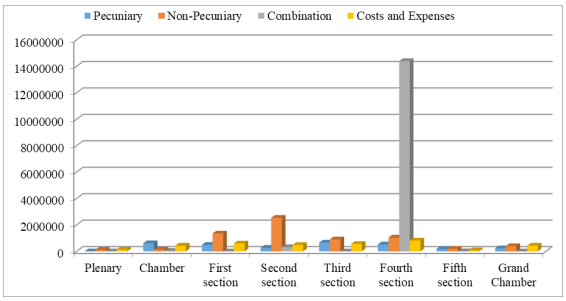


52 The last point that may be interesting in this respect is the percentage of cases in which the different chambers, sections, and courts established a violation. From the early period, it becomes clear that when the court convened in plenary setting, which would typically be in more weighty cases, a far higher percentage of the cases resulted in a violation than when the ECtHR convened in a chamber setting. This is mirrored with respect to the different sections and the Grand Chamber in the later period. In addition, it is also remarkable that especially the first section will find a violation of Article 8 ECHR in a significantly lower percentage of the cases than the other sections. The reason for this remains unclear.

53 **Figure 14: Number of cases in which a court a violation was found of the right to privacy:**

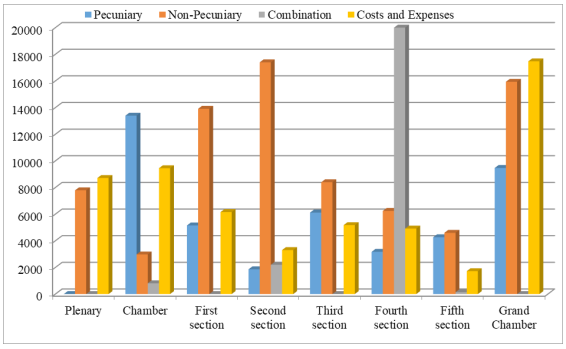


54 **Figure 15: Total amount of damages awarded per court:**



55 Figure 15 shows the total amount of damages awarded per court. It appears that the fourth section has used the 'Combination' category in particular; why this is remains unclear. Apart from that, it is clear that especially the first and the second section, and the Grand Chamber attribute higher sums for immaterial damage than the other chambers. From Figure 16, it also appears that the third and fifth section and the Grand Chamber, as opposed to some other sections, have a quite even spread across the pecuniary, non-pecuniary and costs and expenses categories. The average of the 'Combination' category per case in which a violation was found by the fourth section is € 86.186,- This graph only goes to € 20.000,- for reasons of legibility.

56 **Figure 16: Total amount of damages divided by the number of cases in which a court found a violation:**



33 Rule 26 of the Rules of the Court.

III. Analysis

57 It is mostly unclear why these differences between the different chambers and sections of the Court appear. These sections are supposed to be primarily administrative entities. The website of the Court specifies with this respect: 'A Section is an administrative entity and a Chamber is a judicial formation of the Court within a given Section. The Court has 5 Sections in which Chambers are formed. Each section has a President, a Vice-President and a number of other judges.'[34] Still, the differences that appear from the statistical analysis provided in section E.II. cannot be explained by coincidence, or treated as mere insignificant statistical correlations. Consequently, there must be an explanation for the differences in terms of the type of cases that are dealt with by the different sections, the damages awarded, and the country against which the case was brought. This point needs to be investigated in greater detail in future research.

F. Types and number of applicants

I. Introduction

58 Although, the Convention contains the right of a natural person to petition, this represents but a segment of the European supervisory system as a whole. In this respect, it should be noted that an inter-state complaint is not so much concerned with personal harm suffered by one or more natural persons, but focusses rather on general governmental policies, or systematic abuse of state powers. For example, if a government invokes the state of emergency and derogates from the rights and freedoms under the Convention, other states may question the legitimacy or necessity of these actions before the Court.[35] Second, the right to individual petition is open to three types of complainants: individuals, non-governmental organizations (e.g. a municipality or province) and groups of individuals. Consequently, not only can a natural person complain about a violation, a legal body may also claim to be the victim of an interference of its rights. Such an infringement does not revolve around personal harm – rather a church's freedom of religion may be infringed upon when it is prevented from ringing the church bells in the morning.

59 Moreover, although earlier drafts of the Convention only referred to the right of natural and legal persons to petition, a third category was added, namely any 'group of individuals'. The right to petition of a group of individuals was inserted to broaden the width of the right to petition and to ensure that no one was excluded from access to the Commission.[36] The term 'group of individuals' referred specifically to minority groups, which must be interpreted against the background of the Second World War, in which such groups were stigmatized, discriminated or worse.[37] In such a claim, a group of natural persons does not claim that these persons have suffered themselves specifically and individually from a certain governmental practice – this is already covered by the right of individual petition by natural persons. Rather, a group of individuals has the opportunity to represent the common interests of the minority group as such.

60 Over time, however, the Convention has been revised on a number of points, so that, inter alia, individual complainants (individuals, groups, and legal persons) have direct access to the Court (second-tier) to complain about a violation of their privacy when their case is declared admissible.[38] Moreover, over time, the Court has placed a very large emphasis on individual interests and personal harm if it assesses a case regarding a potential violation of Article 8 ECHR.[39]

61 This focus on individual harm and individual interests brings with it that complaints are declared inadmissible by the European Court of Human Rights if the claimant cannot show that he has suffered from significant harm due to the infringement of his right complained of. By and large, only natural persons are successful in their claims before the Court with respect to their right to privacy, if they have suffered from significant, personal harm. That is why two factors have been analysed for this study. First, the type of applicant and second, the number of applicants.

62 With respect to the types of applicants, a differentiation is made for this study between natural persons and legal persons (individual complaints) and states (inter-state complaints). With respect to the category 'legal persons', a somewhat broader take has been adopted, not only listing organizations themselves that have submitted a complaint, but also incorporating those complaints that have been lodged by natural persons when their interests are

34 <http://echr.coe.int/Pages/home.aspx?p=court/judges&c=#newComponent_1346152041442_pointer>.

35 Article 15 ECHR.

36 Robertson, vol. 2, p. 270.

37 Robertson, vol. 1, p. 160-162

38 Protocol No. 9 to the Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 6.XI.1990. Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby. Strasbourg, 11.V.1994.

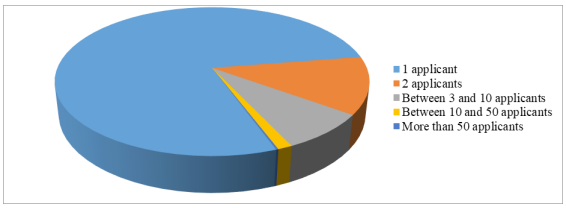
39 See already: B. van der Sloot, 'Privacy in the Post-NSA Era: Time for a Fundamental Revision?', JIPITEC, 2014, 3.

part of or connected to those of a legal person; for example, their private, one-man firm operated from their home. With respect to natural persons, the category has been further sub-divided between ordinary natural persons and natural persons being prisoners or immigrants. This is because prisoners, by the very nature of their imprisonment, are limited in their rights and freedoms, including their privacy. With respect to immigrants, it is interesting to see whether, and if so, how far these cases differ from other cases, because the idea of human rights is precisely that everyone has them by virtue of being human, independent of nationality. If both a natural and a legal person, an immigrant or a prisoner, submitted a complaint, it was listed under 'legal person', 'immigrant', or 'prisoner'.

63 With respect to the number of applicants, although the Court does not allow complaints of groups as groups, it does allow individuals to bundle their individual complaints. Thus, if a group of 50 applicants are all suffering from the same violation, for example, a factory nearby a neighbourhood polluting the area, the ECtHR is willing to accept and bundle their complaints in one case if they can demonstrate that they have all been harmed individually and significantly by the same violation. Five categories have been distinguished for this study; namely, cases in which there was 1 applicant, cases in which there were 2 applicants, cases in which there were between 3 and 10 people involved, cases in which there were between 11 and 50 people involved, and cases in which there were more than 50 applicants. It should be noted that it is often difficult to assess the exact number of applicants. For example, 50 people may lodge a complaint, thereof, 40 people may be declared admissible for their complaint under Article 6 ECHR and 35 under Article 8 ECHR; the Court (second-tier) may then decide that in fact, after a further and more careful assessment, 10 of the applicants complaining about a violation of their right to privacy are actually to be determined under their right to marry and found a family (Article 12 ECHR) and subsequently hold that 15 of the 25 remaining applicants with respect to a potential violation of Article 8 ECHR have indeed suffered from an illegitimate infringement on their right to privacy. Moreover, of those 15 applicants in relation to whom a violation of Article 8 ECHR has been established, 5 of them may be compensated only for the Costs and Expenses, 5 of them for pecuniary or non-pecuniary damages and 5 of them may not been awarded any type of relief. Consequently, there is a margin of error with respect to the numbers and categories below and the results must be taken primarily as indicative.

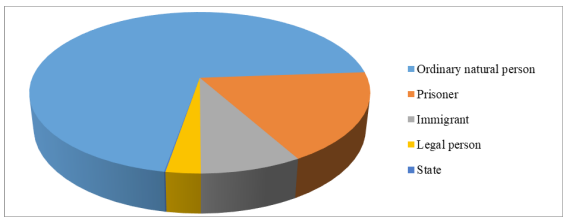
II. Results

64 **Figure 17: Total number of cases in which a certain number of applicants was involved:**



65 Figure 17 shows that in fact, by far most cases are brought forward by one person. In cases in which 2-5 applicants are involved, this mostly concerns a family unit, for example when a political refugee is extradited to Iraq and he argues that this would lead to a violation of his right not to be tortured or subjected to degrading treatment (Article 3 ECHR), and his wife and three children claim that his extradition would violate their right to family life (Article 8 ECHR). There seems no significant correlation between the year in which the case was submitted and the number of applicants, for example a sharp rise or fall of the number of applicants over the years – rather, the cases in which more than 10 applicants were involved seem to be spread quite evenly over the years. Figure 18 shows which types of applicants where involved with the cases judged in the second-tier with respect to a potential violation of the right to privacy. It confirms what has been suggested in paragraph G.I., namely that by far most cases are brought by natural persons, only a small percentage of cases is brought by a company or organisation (note that a governmental organisation cannot submit a claim before the ECtHR – the city of Paris or the province of Andalusia cannot submit an application) and a negligible amount of cases concerns an inter-state complaint.

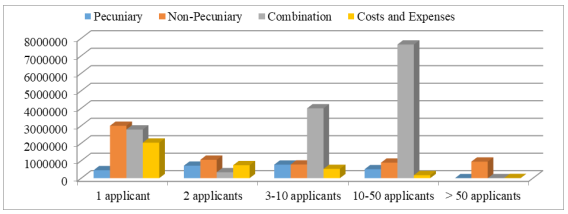
66 **Figure 18: Total number of cases in which a certain type of applicant was involved:**



67 Figure 19 shows the total amount of damages that have been awarded by the ECtHR in cases in which a violation was found of Article 8 ECHR until 2010, per category of applicants. Given the very high number of cases in which there was but one applicant, it should not come as a surprise that in this category the most damages have been awarded. What is apparent from the figure too is that the cases against

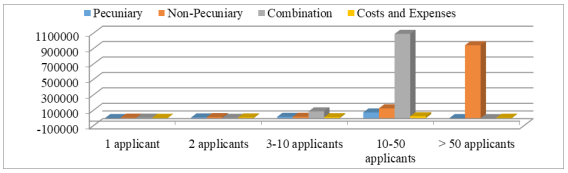
Turkey in which high sums of money were awarded to the applicants have been matters in which larger groups have been involved.

68 Figure 19: Total amount of damages awarded per number of applicants:



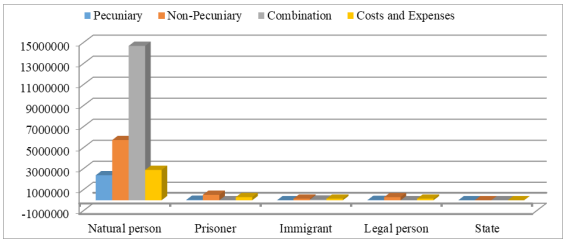
69 Figure 20 shows the average amount of money awarded to the applicants in case a violation was found of Article 8 ECHR in the specified categories. What is remarkable is the quite low numbers of damages. When one applicant was involved, on average, € 896,- was awarded for pecuniary damages per case in which a violation of the right to privacy was established, € 5.906,- for non-pecuniary damages, € 5.488,- in the 'Combination' category, and €4.004,- for costs and expenses. When two applicants lodged a complaint which resulted in a violation of Article 8 ECHR, this was on average € 8.385,- for pecuniary and € 12.374,- for non-pecuniary damage, € 3.989,- for the 'Combination' category, and € 8.705,- for cost and expenses (meaning in total, for both applicants together). These sums are for the applicants jointly and should consequently be divided by two to calculate the average amount of damages awarded per victim. The more applicants join in a case, on average, the more damage is awarded, which was to be expected. Finally, it should be noted that there are very few cases in which more than 50 applicants have submitted a complaint, so that the results from this category are unreliable.

70 Figure 20: Total damages divided by the number of cases in which a violation was found per category:



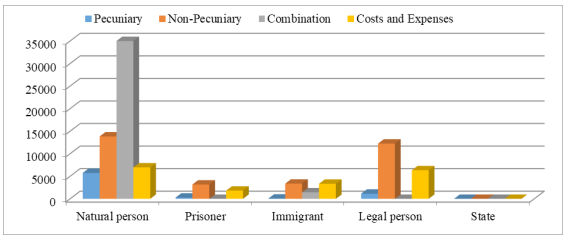
71 Figure 21 shows the total amount of damages that have been awarded by the ECtHR in cases in which a violation of Article 8 ECHR was established until 2010 per category. It should not come as a surprise that the only relevant category in this respect is that of natural persons.

72 Figure 21: Total amount of damages awarded per type of applicant:



73 Figure 22 shows the total amount of damages awarded per category, divided by the number of cases in which a violation of Article 8 ECHR was found with respect to a certain category. For example, the total amount awarded to natural persons by the ECtHR, divided by the 414 cases in which a violation of the right to privacy of a natural person was found by the Court. What is interesting is that on average, prisoners and immigrants have been awarded limited amounts of damages. This is because in many cases, the ECtHR stresses that the establishment of a violation in itself constitutes sufficient satisfaction for the applicant; for example, by holding that an immigrant should not be extradited, or that a prisoner should have more liberties, for example, with respect to family visits. With regard to legal persons, one could have expected that especially the pecuniary damages and the 'combination' category would be high, but the opposite is true. Whether the ECtHR grants non-pecuniary damages to the company or organization itself, or to the owner or other natural persons connected to it, is unclear - further research is needed on this point. Finally, it should be noted that there are very few cases in which inter-state complaints were made, so that the results from this category are unreliable.

74 Figure 22: Total damages divided by the number of cases in which a violation was found per category:



III. Analysis

75 The analysis for this section can be quite straightforward. States seldom submit applications, groups are not allowed to submit claims as a group, and legal persons, such as companies, are only

marginally successful in invoking the right to privacy under Article 8 of the European Convention on Human Rights. Most of the cases are brought before the Court by natural persons. Some of these are prisoners, some immigrants, but most of them are citizens without a special status or legal position. Most damages that are awarded by the European Court of Human Rights go to natural persons, both in total and on average, which is divided by the number of cases.

76 A point of interest is that the damage being awarded to legal persons mostly falls in the category of non-pecuniary damage. Because the Court is so strict on the fact that privacy is the most personal of all human rights and because it feels that consequently, legal persons can only marginally rely on Article 8 ECHR before the Court, it could have been expected that if the ECtHR would find legal persons admissible in their claim, this would not be related to harm to their personality or other immaterial aspects of the right to privacy. Rather, it would seem logical that the majority of damages awarded to legal persons would have been in the more objective material harms category. The opposite, however, is true, as shown in section F.II. When the police raid a business premises, the Court is willing to attribute damages for immaterial harm to businesses, which may be rather surprising.

77 With respect to the number of applicants being involved in a privacy case before the European Court of Human Rights, by far most cases are submitted by individual persons, a small part by 2-5 and 5-10 persons, and only a handful of matters are brought to the Court's attention by a group of 10-50 people or of more than 50 people. Most damages are consequently awarded to individual applicants. When the total amount of damages awarded by the ECtHR in privacy cases is divided by the number of cases per category (1 applicant, 2-5, 5-10, 10-50, or more than 50 applicants), it becomes clear that on average, the ECtHR assigns most damages in cases with 10-50 or more than 50 applicants. However, when the average amount of damages awarded in such cases is divided by the number of applicants, the picture becomes more linear.

G. Types of damages awarded

I. Introduction

78 If the European Court of Human Rights finds a violation of a provision contained in the Convention, it may decide to impose a fine or a sanction. It can hold that a state should stop violating the Convention, that it should abstain from executing its plans (for example, extraditing an immigrant) because that would be in violation of the Convention, or that it should adopt additional policies to prevent others from violating the rights of the applicant (for example, ensuring that the claimants are adequately protected against systematic harassment by third parties). The Court can also impose an obligation on a state to provide financial relief to the claimant. Article 41 of the ECHR holds on this point: 'If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.' The applicant who wishes to obtain an award of just satisfaction under Article 41 of the Convention must make a specific claim to that effect. It is for the applicant to submit itemized particulars of all claims, together with any relevant supporting documents.[40] The Rules of the Court specify the following about harm and satisfaction.

79 The award of just satisfaction is not an automatic consequence of a violation being found by the ECtHR. The Court will only award such satisfaction if it considers that to be "just" in the circumstances of the case. This means that the particular features of each case are taken into account when making that assessment. Importantly, the Court may decide that the finding of a violation constitutes in itself sufficient satisfaction, without there being a need to afford financial compensation. Indeed, the Court adopts this approach in quite a number of cases, as will be explained later in this article. The Court may also find reasons of equity to award less than the value of the actual damage sustained or the costs and expenses actually incurred. A reason for such a decision may be that the complaint put forth, or the amount of damage, or the level of the costs, is due to the applicant's own fault. In setting the amount of an award, the Court may also consider the respective positions of the applicant and the Member State, and the local economic circumstances in a country or region.

80 In general, a clear causal link must be established between the damage claimed and the violation alleged. A merely tenuous link between the alleged violation and the damage or speculations as to what might have been when the infringement would not have occurred is not enough. It is important to point out that the purpose of the damages is to compensate the applicant and not to punish the Member State. Three types of damage may be awarded by the ECtHR: pecuniary damage, non-pecuniary damage, and costs and expenses.[41] These three categories are

40 Rule 60 of the Rules of the Court. <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf>.

41 Rules of the Court, p. 61.

also used in this article when calculating the amount of damages awarded by the Court. One additional category has been added, 'Combination', for cases in which the damages are awarded in total, or in respect of a combination of two of these categories. In general, the Court is very explicit on the point of how much damage is awarded per category, but in a handful of cases, it has stressed that it is unable to determine the damages precisely and that it will consider that, for example, the material and immaterial damages taken together amount to a certain sum.

1. About awarding pecuniary damage, the Rules of the Court make clear that the principle is that the applicant should be placed, to the extent possible, in the position in which he would have been had the violation found not taken place (*restitutio in integrum)*. This can involve compensation for both loss actually suffered (*damnum emergens*) and loss, or diminished gain, to be expected in the future (*lucrum cessans*).[42] Normally, the Court's award will reflect the full calculated amount of the damage, but if the actual damage cannot be precisely calculated, the Court will make an estimate based on the facts and circumstances of the case.

2. On the aspect of awarding non-pecuniary damage, the Rules of the Court emphasize that this is intended to provide financial compensation for non-material harm, for example, mental or physical suffering. Applicants who wish to be compensated for non-pecuniary damage can specify a sum, which in their view would be equitable. Importantly, applicants who consider themselves victims of more than one violation may claim either a single lump sum covering all alleged violations, or a separate sum in respect of each alleged violation.

3. Finally, awarding money for costs and expenses is intended to compensate for the applicant's travel costs, costs for lawyers, and possibly for other expenditures related to the legal proceedings themselves. The Rules of the Court specify on this point that the Court can order the reimbursement to the applicant of costs and expenses, which he has incurred – first at the domestic level, and subsequently in the proceedings before the Court itself – in trying to prevent the violation from occurring, or in trying to obtain redress therefor. Importantly, costs and expenses must have been necessarily incurred, meaning that they must have become unavoidable in order to prevent the violation or obtain redress therefor. They must be reasonable as to quantum.[43]

81 In this study, the amounts awarded by the ECtHR have been calculated in Euros. After the introduction of the Euro, the Court has (with a few exceptions) used the Euro as its standard currency, even for applicants from countries that have a different currency.[44] However, the Euro was introduced virtually in 1999 and in notes and coins in 2002; in cases before 2002, the ECtHR used the currency of the state against which a violation was found. These sums have been converted into Euros using the fixed conversion rates as established by the EU for countries joining the Euro-group;[45] for other currencies, a fixed conversion rate has been set too for the purposes of this study.[46] Choosing a fixed conversion rate means that no account is taken of the fluctuations in currencies. Although for most countries these are relatively stable, some countries, such as Italy, have historically devaluated their currency a number of times, so that picking one fixed rate may give a somewhat distorted picture. Other methodological choices that have been made for this study are:

1. Only the cases in which Article 8 ECHR was violated are included with respect to the damages; cases in which no violation was found, but in which the Court did award damages in relation to a violation of another provision, are not included with respect of the damages. This may occur when a complaint regards both a violation of Article 6 ECHR (fair trial) and Article 8 ECHR, but the court found only a violation of Article 6 ECHR and not of the right to privacy.

2. In cases in which a violation of Article 8 ECHR was found, all damages have been included, even if a violation of more provisions was established. Thus, if the court finds both a violation of Article 6 ECHR and of Article 8 ECHR and awards damages, the total amount of damages are taken into account. The reason for this is that the ECtHR usually awards a total sum for the violations, without differentiating the amount of damages awarded for a violation of Article 8 ECHR and for a violation of another provision.

3. When awarding damages for costs and expenses, the ECtHR usually grants a total sum and makes clear that the relief the applicants received via

42 Rules of the Court, p. 61.

43 Rules of the Court, p. 62.

44 The Euro is the currency introduced by the European Union, not by the Council of Europe. Moreover, some EU countries have decided not to join the Euro.

45 <http://www.ecb.europa.eu/euro/intro/html/index.en.html>.

46 € 1 = £ 0,7734 - € 1 = $ 1,1005 - € 1 = 9.35332 SEK - € 1 = 1.09362 CHF - € 1 = 4,2995 Polish Zloty.

other means must be deducted from that sum; in this study, the total sum is included, because it is mostly unclear whether applicants received relief through other means and if so, how large the sum was that they received.

4. In some cases, the Court stresses that it will calculate the damages to be awarded in a separate decision, but sometimes, the parties have reached a settlement on the compensation before that judgement. These damages are not taken into account, because the amounts agreed upon are usually not disclosed to the public.

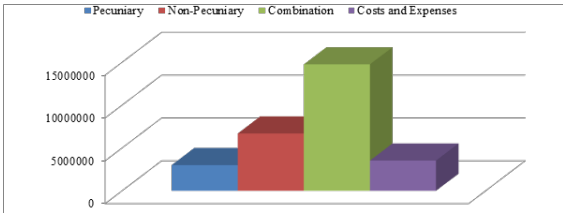
5. The Court often underlines that interest rates should be taken into account, if the country does not pay the damages within the period specified by the Court. These rates have not been taken into account, because it is usually impossible to find out whether the country did pay the damages on time or not.

6. Sometimes, the Court stresses that if a country executes a certain policy, it would act in violation of the ECHR and that if it would go on to execute the policy, it would need to pay damages. These damages have also been taken into account, although it is unclear whether the country has indeed executed its policy or not and thus had to pay damages.[47]

II. Results

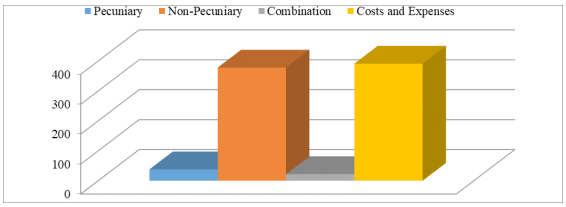
82 Figure 23 shows the total amount of damages the ECtHR has awarded for a violation of the right to privacy in cases until 2010 per category. In total, € 3.001.222,- has been awarded in respect of pecuniary damages. With regard to non-pecuniary damages, this was € 6.689.578,- and € 14.757.151,- was the total amount of euros afforded by the ECtHR to claimants in an unspecified manner (combination category). Finally, € 3.526.334,- was awarded in total for cost and expenses. Divided by the number of cases in which a violation was found of Article 8 ECHR, this means that on average, € 4.632,- for pecuniary damage, € 10.323,- for non-pecuniary damage, € 22.773,- for a combination of categories, and € 5442,- for costs and expenses have been awarded per case. This is remarkable because the ECtHR has only used the category of combined costs in about 20 cases, while it has awarded non-pecuniary damages and awards for costs and expenses in almost 400 cases. In only 38 cases it has granted pecuniary damages.

83 Figure 23: Total amount of Euros awarded in cases in which a violation of Article 8 ECHR was found:



84 In most cases in which it finds a violation of Article 8 ECHR, the Court awards damages for non-pecuniary and/or for costs and expenses, but these are normally relatively small amounts. In a small number of cases, it will award either pecuniary damage or a combination of different types of damages (mostly including material damage) – in these cases, the amount of damages awarded is typically higher. This is evidently true for the combination of damages, but also for the pecuniary damages. Although the Court has awarded about two times more for non-pecuniary damage than for pecuniary damages in total, the number of cases in which it awarded non-pecuniary damage is about 10 times higher. Finally, it is interesting to note that of the 648 cases in which the Court has found a violation of Article 8 ECHR, it awarded some type of relief only in 564 of them and in 440 of the cases, when the mere procedural costs (the awards for costs and expenses) are excluded.

85 Figure 24: Number of cases in which the Court has awarded damages in a certain category:



III. Analysis

86 The character of privacy as a human right, protecting a person against violations related to human dignity,[48] is confirmed by the figures found for this study. In almost two thirds of the cases in which the European Court of Human Rights has found a violation of the right to privacy (Article 8 ECHR), it has awarded some form of non-pecuniary damages for immaterial harm. Per case in which some form of immaterial harm was compensated by the ECtHR,

47 See for example: ECtHR, L. v. Lithuania, application no. 27527/03, 11 September 2007.

48 D. Schroeder, 'Human Rights and Human Dignity: An Appeal to Separate the Conjoined Twins', Ethical Theory and Moral Practice, June 2012, Volume 15, Issue 3.

an average sum of about € 16.000 was awarded. Although this may be a low number when compared to American standards, for European standards, it is quite reasonable or even towards the higher end. One of the reasons for this may be that the European Court of Human Rights is used only if the national remedies have been exhausted.[49] This means that in principle, a claim before the ECtHR will only be declared admissible if the claimant has applied to a court, a court of appeal, and the supreme court, before the claim will be received before the ECtHR. In general, only the victims of more serious claims will take the effort of legal litigation, which could take years. In addition, the human rights courts in principle only accept cases in which significant harm is inflicted to the victim.[50] Human rights under the ECHR lay down the minimum requirements of respect for human dignity, meaning that most legal cases will not qualify as falling under the material scope of the European Convention on Human Rights in general and the right to privacy in particular.

87 Only in about 60 if the 648 cases in which the ECtHR has found a violation of Article 8 ECHR has it provided damages for material harm or a combination of harms, including material harm. This means that in general, the right to privacy is not focussed on material losses. Still, the cases in which it finds that pecuniary damage has been inflicted, the European Court of Human Rights awards high sums of money to the victims. Consequently, when material harm is accepted by the Court to have led to a violation of a person's privacy, the infringement on the right to privacy is quite severe. As will be shown below, a typical example of such a case is one in which the army of a certain country destroys a whole village, or when villages are evacuated for a long period of time. The residents then typically bundle their claims, so that one case is brought by a group of victims, which obviously has an impact on the amount of damages awarded.

H. Types of privacy

I. Introduction

88 Categorizing the cases under the right to privacy, Article 8 ECHR, is very difficult for a number of reasons. First, the ECtHR has chosen a very wide and broad interpretation of the different concepts provided protection under this provision: 'private life', 'family life', 'home', and 'correspondence'.[51] To provide an example, 'correspondence' not only refers to letters or telephony, but also modern forms and means of communication. 'Home' is not only the home of an individual, but any premises in which a person lives on a quasi-permanent basis, with factories, office buildings and restaurants also possibly qualifying as the 'home' of a legal person. A 'family' relation not only exists between a married couple and their children, but can, depending on the circumstances of the case, also exist between grand-children and grand-parents, between non-biological parents and children, between children and great-uncles, and between children and a mentor or supervisor. Finally, 'private life' has been used as a term that may include almost anything that remotely relates to a person's identity or personal development.

89 Second, the original rationale behind the right to privacy was granting the citizen negative freedom in vertical relations, that is the right to be free from arbitrary interferences by the state. In this line, the Court still holds that the 'essential object of Article 8 is to protect the individual against arbitrary action by the public authorities'.[52] However, the Court has gradually diverged from the original approach of the Convention authors by accepting both positive obligations for national states and granting a right to positive freedom to individuals under the right to privacy. The element of positive liberty was adopted quite early in a case from 1976: 'For numerous anglo-saxon and French authors the right to respect for "private life" is the right to privacy, the right to live, as far as one wishes, protected from publicity. [H]owever, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfillment of one's own personality.'[53] Likewise, from very early on, the Court has broken with the strictly limited focus of the authors of the Convention on negative obligations (the obligation not to use power in certain ways) and has accepted that states may under certain circumstances be under a positive obligation (the obligation to use power in certain ways) to ensure respect for the Convention. This has had an enormous impact on both the underlying rationales and the material scope of the right to privacy under the European Convention on Human Rights.

90 Third, the European Court of Human Rights, when discussing cases under the right to privacy, Article 8 ECHR, is often vague about the question of which

49 Article 35(1) ECHR.

50 Article 35(3)(b) ECHR.

51 See on this point: B. van der Sloot, 'Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data"', Utrecht Journal of International and European Law, 2015.

52 ECtHR, Arvelo Apont v. the Netherlands, application no. 28770/05, 3 November 2011, § 53.

53 ECmHR, X. v. Iceland, application no. 6825/74, 18 May 1976.

of the four terms contained in the provision applies to a certain case. Often, it combines two terms, for example stressing that a certain matter affected the applicant's 'private and family life' or his 'private life and home'. Sometimes, the ECtHR merely points out that the case clearly fell 'under the scope of the right to privacy', or that it was not disputed by any of the parties involved that the cases were to be discussed under the right to 'private and family life, home and correspondence.' In some cases, the Court simply ignores the question of whether a case falls under the scope of Article 8 ECHR and sometimes, it clearly avoids it by underlining that 'even if the case fell under the scope of the right to privacy', it must, for example, be rejected because the infringement was prescribed for by law and necessary in a democratic society. This attitude of the Court makes it very difficult to categorize the cases with respect to the type of privacy that is at stake.

91 Fourth, the Court has often stressed that the Convention and its Protocols must be seen as a whole. This means that a number of rights and freedoms that are protected by other provisions of the Convention, are sometimes included under the scope of the right to privacy. For example, the right to marry and found a family, as protected under Article 12 ECHR, is in fact mostly ignored by the Court; instead, questions revolving around, for example, gay marriage and in vitro fertilization are discussed under Article 8 ECHR. Though the right to a fair trial is incorporated in Article 6 ECHR, the ECtHR has made clear that there are also procedural safeguards implicit in the right to privacy, so that a right to a fair trial is also protected under Article 8 ECHR. Although one's bodily and psychological integrity is protected by Articles 2, 3 and 4 ECHR, the ECtHR has treated cases revolving around these types of question primarily under the right to privacy. Although the right to reputation was explicitly excluded from the right to privacy, and moved to paragraph 2 of Article 10 ECHR, concerning the right to freedom of expression, the Court has nevertheless underlined that the right to reputation shall be protected under Article 8 ECHR. Consequently, the realm of the right to privacy has been expanded quite considerably.

92 Fifth and finally, the ECtHR has introduced the 'living instrument' theory when interpreting the Convention. This means that the Court is at liberty to interpret the Convention according to its views in light of current societal tendencies and developments, and to introduce new rights and freedoms under the existing provisions in the Convention. Perhaps quite unsurprisingly, it is primarily article 8 ECHR that has functioned as umbrella for these new rights and freedoms. It is beyond the scope of this paper to discuss these matters in detail,[54] but in general it can be established that the underlying rationale has moved from obligations on states not to abuse their power, to individual and subjective rights of natural persons to protect their individual autonomy, their human dignity, and their personal freedom. Almost everything that is even only remotely connected to personal interests is accepted under the material scope of the right to privacy. For example, the ECtHR has stressed that Article 8 also provides protection to the right to develop one's sexual, relational and minority identity, the right to personal development, the right of foreigners to a legalized stay, the right to property and even work, the right to environmental protection, the right to have a fair and equal chance in custody cases, a right to data protection, the right to a name and/or to change one's name, etc. In terms of material scope, the right to privacy has become by far the largest doctrine protected under the European Convention on Human Rights.

93 Because the scope of Article 8 ECHR has become so broad, this study started by identifying 10 categories: (1) Matters relating to bodily and psychological integrity; (2) family and relational privacy; (3) communicational secrecy; (4) home and locational privacy; (5) protection of honour and reputation; (6) cases on data protection; (7) cases on (mass) surveillance; (8) cases on environmental protection and the right to a healthy living environment; (9) matters in which broader issues relating personality, identity, and personal development were at stake; (10) questions in which the enjoyment of property or primarily economical aspects were discussed. Because it proved impossible to do a reliable analysis on the basis of 10 categories, these have been scaled back to 5 categories. The protection of honour and reputation, cases which concerned the healthy living environment of individuals, and the broader questions regarding personality and identity have all been included in the first category; cases on data protection and mass surveillance have been combined with the category on communicational secrecy; this category is now coined 'informational privacy'.

94 Consequently, five categories are used in this study. The choice of categorizing a case in one or another group is often difficult and to some extent arbitrary. Importantly, there are cases in which there are two separate complaints on the right to privacy; for example, the government has wire-tapped a person's telephone in violation of his informational privacy and has subsequently decided to enter and search that person's house without a warrant, in violation of his locational privacy. In cases in which both complaints lead to a violation or in which both complaints were rejected by the ECtHR, it has been

54 B. van der Sloot, 'Privacy as human flourishing: could a shift towards virtue ethics strengthen privacy protection in the age of Big Data?', JIPITEC, 2014-3.

decided to categorize the cases under the category that seemed most important/prominent. Again, these choices are to some extent arbitrary. If one part of the complaint, for example the part on the telephone tap, resulted in the Court's consideration that the government did not act in violation of Article 8 ECHR, but that it did violate the applicant's right to privacy because the house search was not prescribed for by law, the case has been categorized under the type of privacy in which the violation was established. This is because if damages were awarded by the ECtHR, this would be linked to the corresponding privacy category.

95 The five privacy types now distinguished are:

1. *Bodily and psychological integrity*: this is presumably the broadest of the five remaining categories. It includes, inter alia, cases on one's sexual freedom, for example of homosexuals not to be prosecuted and criminalized;[55] transgender people demanding full recognition of their new gender, inter alia in government documents; the right not to be involuntarily subjected to medical treatment; the right to change one's name; the right to reputational protection; the right to a healthy living environment.

2. *Relational privacy*: this category is used for all cases that related to the possibility of a person to engage with others and to develop relationships. Most prominently, this category contains cases about children being placed out of home, custody cases and visiting rights by parents. Importantly, when a person complains that he is unable to communicate with others, for example a prisoner being prevented from sending letters to his family, this is categorized as relational privacy; when the complaint was about the authorities *reading* the letters, this is categorized as informational privacy.

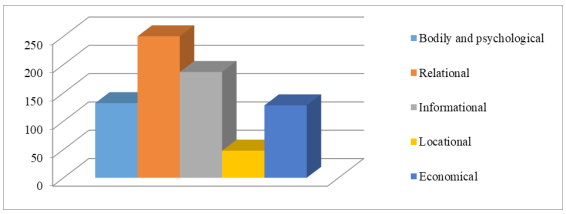
3. *Informational privacy*: this category consists of a combination between different, though related types of cases. It contains matters regarding modern types of surveillance, such as mass surveillance by intelligence services or camera-surveillance through the use of CCTV-cameras. The category also incorporates classic data protection cases, such as people wanting access to documents and information relating to them stored by the government. It also contains cases on communicational secrecy, such as wiretapping telephone conversations by the state; an important part of this category consists of cases in which prisoners complain that their letters are opened and censored by the prison authorities.

4. *Locational privacy*: this category consists of cases in which the government accesses the private home of an individual. In addition, the ECtHR has sometimes allowed legal persons an analogous claim, for example, when the police have searched the premises of a company in relation to tax evasion.

5. *Economical privacy*: while the previous four categories may be seen as linked to or as an expansion of the four terms listed in Article 8 ECHR (private life, family life, home and correspondence), a fifth category is newly introduced by this study. It incorporates cases which revolved primarily around the enjoyment of property and/or economical aspects. For example, there are cases under Article 8 ECHR in which the homes of individuals are destroyed; this is not, in the classic sense, a violation of the locational privacy of individual, because it does not involve entering the home or gathering private information, but primarily relates to the loss of property. Similarly, this category includes cases on the right to inherit family assets by bastard children and the special tax status for unmarried couples compared to married couples. It also includes cases on the inability to get a job in the army, because it has a policy of rejecting openly gay people.

II. Results

96 **Figure 25: Total number of cases per category:**



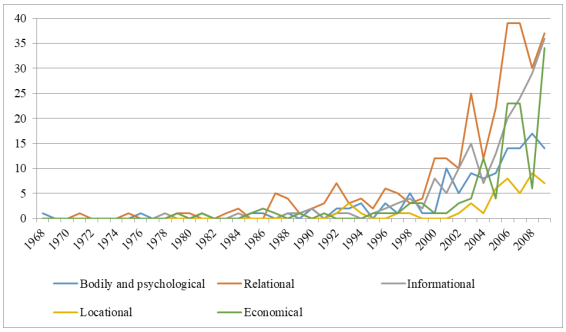
97 Figure 25 shows the total number of cases that have been assessed by the ECtHR (second-tier) until 2010 under the right to privacy, Article 8 ECHR. It is clear that the second category, the right to relational privacy, is the category with the highest number of cases - almost 300, followed by the right to informational privacy, with nearly 190 cases. Interestingly, although the first category is by far the broadest in material scope, it contains a modest number of cases; like bodily and psychological integrity, there are around 130 cases in which the enjoyment of property or economical aspects are central aspects.

55 The Court usually categorizes homosexual relations under 'private life' and heterosexual relations ones under 'family life'.

98 With respect to the latter category, this might be qualified as a high number, as there has been considerable discussion on this point by the authors of the Convention. First, when drafting the Convention, it was discussed at length whether a separate provision should be included on the enjoyment of property, and second, whether Article 8 should make explicit mention of the right to protection of personal property. The authors of the Convention made a conscious decision to exclude the protection of economic interests explicitly from the Convention as a whole and the right to privacy in particular. One of the reasons being that the protection of property is a socio-economic or a so called second generation right, while the European Convention on Human Rights only contains civil and political rights, or so called first generation rights. The socio-economic rights have been transferred to a protocol to the Convention, the ratifying of which was an option.[56] As is apparent from Figure 25, the ECtHR has made a decision to include cases with respect to the protection of personal property, economic affairs and financial protection under the Convention and the right to privacy nevertheless.

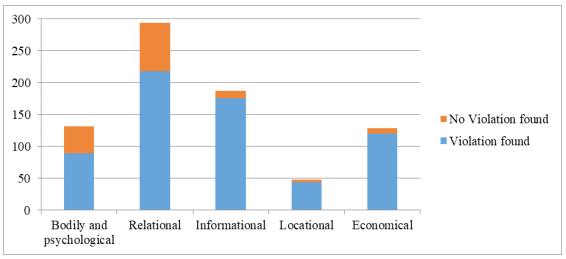
99 Finally, it is interesting to see that there are very few cases on the potential violation of locational privacy, even though this also includes cases in which the office of a company was entered by governmental officials. There are less than 50 cases on this point. On the one hand, this may be considered remarkable because the protection of the home is perhaps the classic aspect of the right to privacy. On the other hand, precisely of this reason, governments might be more hesitant to infringe on the privacy of citizens than they are with respect to, for example, communication over the internet. An additional consideration in this respect may be that in many countries, there is a well-established doctrine providing special protection to the home, often dating back several centuries. Consequently, restraint towards entering the home is often embedded in the legal as well as social practice in a country. This may be an explanation for the low number of cases regarding the locational privacy of citizens, but there may be others.

100 Figure 26: Total number of cases per category per year:



101 Figure 26 shows the total number of cases per category per year. From this graphic, it is apparent that relational privacy has always been the dominant category in the case law of the ECtHR. However, it is also clear that informational and economic privacy are becoming especially important in the latter years. The increase in cases on informational privacy may be correlated with the increased focus on surveillance in light of terrorist attacks, but more research is needed on this point. Why economic privacy has become more important over the years is unclear.

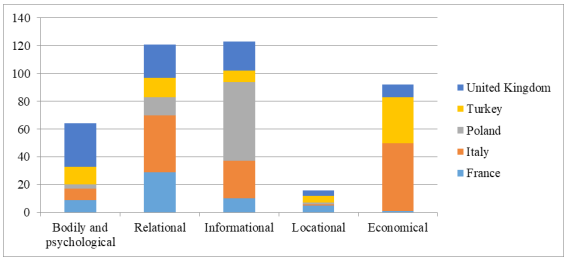
102 Figure 27: Times a violation was or was not found per category:



103 What appears from Figure 27 is that there is a sharp contrast between the five types of privacy with respect to the percentage of cases on Article 8 ECHR (second-tier) in which a violation is found. If a case is declared admissible on the point of informational, locational or economic privacy, it is almost certain that a violation will be found. With respect to bodily and psychological integrity and relational privacy, about one out of three or one out of four cases will get rejected.

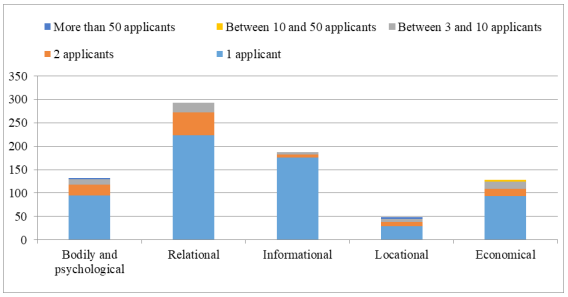
56 First Protocol to the European Convention on Human Rights.

104 **Figure 28: Number of cases per category in relation to five countries:**



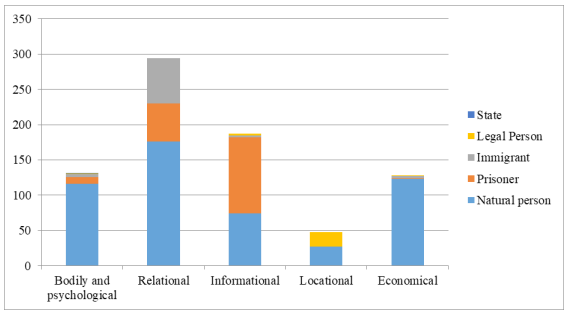
105 Figure 28 shows the number of cases in the different categories, in relation to the five countries against which most cases were assessed by the Court on the point of a potential violation of the right to privacy. What appears is that particular countries have been involved with cases on certain types of privacy significantly more than others. The United Kingdom is primarily responsible for the cases on the point of bodily and psychological integrity. This may be due to the fact that in the recent past, it had quite strict laws on homosexual practices, and medical-ethical issues, as underlined in a previous section. Italy is prominent in cases on relational and economic privacy, France is almost absent in the category of economic privacy and is primarily represented in the figures on relational privacy. Turkey, as has been stressed a number of times, has had quite a number of cases against it regarding the point of the enjoyment of property, and the cases against Poland relate almost entirely on the point of informational privacy.

106 **Figure 29: Number of cases per category in relation to the number of applicants:**



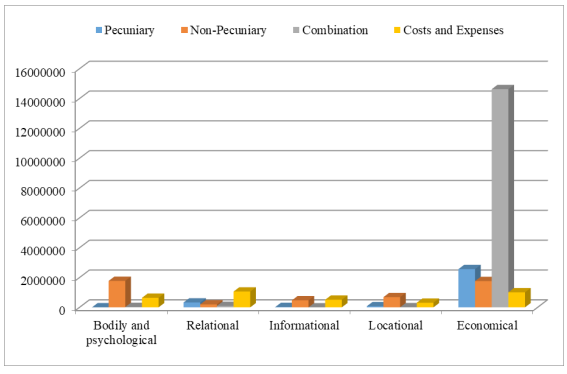
107 From Figure 29, it appears that especially with respect to relational privacy, there are quite a number of cases in which small groups of 2-10 people submit a complaint. These would typically be family units. With respect to informational privacy, cases are almost exclusively lodged by individuals. The other categories have a more equal division in terms of number of applicants.

108 **Figure 30: Number of cases per category in relation to the type of applicant:**



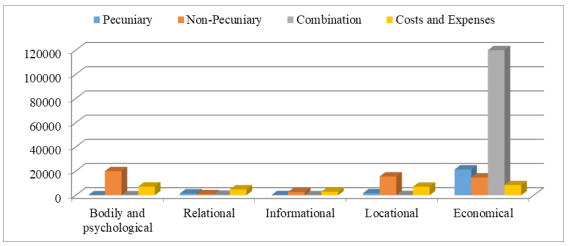
109 Figure 30 shows that prisoners complain almost exclusively about a violation of their relational and informational privacy. These cases typically revolve around either their correspondence being monitored and opened, or around the fact that they are denied contact with others, such as family members, either in real life (visits) or by corresponding with them. Immigrants complain almost exclusively about a violation of their family life. The typical application here would be the claim that if a person gets extradited, this would tear him apart from his family living in that country, which would result in a violation of Article 8 ECHR. This is interesting, because the ECtHR has consistently held that this claim is much stronger than the claim that an extradition would lead to the violation of a person's private life, in the sense that his life, work, friends, future, etc., that he has in a particular country, would be disrupted. Finally, with respect to legal persons, it is clear that these cases are almost exclusively about governmental officials entering their premises.

110 **Figure 31: Total amount of damage awarded per category:**



111 Figure 31 shows the total amount of damages that have been awarded by the Court until 2010 in cases in which it has found a violation of Article 8 ECHR. Obviously, the category of economical privacy represents the highest figures, though immaterial damages are also substantial when a government has invaded a person's bodily or psychological integrity.

112 **Figure 32: Average amount of damage awarded per case in which a violation of a category was found:**



113 Figure 32 has divided the total sum per category by the number of cases in which the ECtHR has established a violation of that type of privacy. Most damages have been awarded for a violation of economic privacy. Judging from the amount of damages awarded in the other four categories, it seems that the Court is inclined to provide higher sums of damages for a violation of a person's bodily or psychological integrity and for an infringement on the privacy of his home, than for a violation of relational or informational privacy. Hypothetically, the cause could be that in those types of cases, the Court holds that the establishment of the violation itself provides sufficient satisfaction, for example stressing that prison authorities cannot monitor all correspondence of prisoners or that a parent was wrongly denied access to his children. However, although this indeed holds true for informational privacy, such a finding by the Court is no more frequent regarding respect to relational privacy than in relation to bodily and psychological, locational and economic privacy. Out of the 89 cases in which the ECtHR found a violation of Article 8 ECHR with respect to bodily and psychological integrity, in 20 it provided no relief for damages or compensated only the legal costs in the Costs and Expenses category; for relational privacy, this was 60 out of 218 cases; for informational privacy, this was 73 out of 176; for locational privacy, this was 10 out of 44; and finally, for economic privacy this was 45 out of 120 cases. Consequently, the explanation must be that with respect to relational privacy, the ECtHR does provide damages, but only small sums.

III. Analysis

114 Five types of privacy have been distinguished. The results from the statistics show that each category has its own characteristics.

- *Bodily and Psychological Integrity:* This category revolves around cases regarding sexual freedom, medical-ethical questions and harm to one's identity and reputation. It is clear from the figures that the majority of cases that regard this type of privacy are brought against the United Kingdom, the reason for which has been explained in section D. Not surprisingly, relatively high sums of damages are awarded by the European Court of Human Rights in this category when it comes to non-pecuniary damage. In contrast to cases with respect to informational, locational and economical privacy, in a relatively substantive part of the cases judged by the ECtHR (second-tier) on the aspect of bodily and psychological integrity, no violation of privacy was found. As explained, because these cases are so essential to human dignity, there is restraint in the first-tier to declare such cases inadmissible. In addition, even if there is no violation of Article 8 ECHR in such cases, the European Court of Human Rights can take the opportunity to lay down a framework or guidelines on these aspects of privacy.

- *Relational Privacy:* Most cases with respect to the right to privacy under the Convention concern the relational aspect; in general, these cases relate to contact with family members. A substantial part of these cases concern prisoners, who claim the prison regimes disable them from seeing their children and/or lovers. Almost all cases that are filed by immigrants revolve around this category of privacy. Typically, it involves an immigrant being extradited, claiming that this would harm the family life that person has built in a certain country. Remarkably, although the European Court of Human Rights often stresses that family life, and in particular the right of parents to have access to their children, is the most fundamental aspect of the right to privacy, the damages provided in this category are relatively low. One of the reasons for this might be that the Court finds that the decision itself provides sufficient relief, for example by ruling that the immigrant in question cannot be extradited or that the prisoner should be allowed to have contact with his family. This needs to be subject of further research. In contrast to cases with respect to informational, locational and economical privacy, in a relatively substantive part of the cases judged by the ECtHR (second-tier), no violation of privacy was found.

- *Informational Privacy:* The majority of the claims about informational privacy aspects are brought by prisoners. Cases typically involve prison authorities checking mail, either analogous or digital, and filtering messages. The ECtHR has stressed that this is only allowed under specific circumstances, and most importantly, must have a basis in law. Although there is a relatively large amount of cases regarding informational privacy, in general, low amounts of damages are

awarded to victims. Poland is the country against which this type of privacy is invoked the most. Almost all cases judged by the Court (second-tier) with respect to this aspect of privacy lead to the conclusion that there has been a violation of Article 8 ECHR.

- *Locational Privacy:* The invasion of the home or private property is the aspect of privacy least brought forth before the European Court of Human Rights (or rather, declared admissible). This may be because these types of privacy violations seldom occur. Alternatively, a reason could be that the state only enters the home of a citizen when it is absolutely certain that this is necessary and is provided for in law. An interesting point is that a relatively high amount of damages are awarded in this category for immaterial harm, that is, non-pecuniary damages. Apparently, the home is essential to human flourishing. Finally, almost all cases submitted by legal persons are in this category; such cases typically revolve around the claim that government authorities have illegally entered the business premises of a company. Almost all cases judged by the Court (second-tier) with respect to this aspect of privacy lead to the conclusion that there has been a violation of Article 8 ECHR.

- *Economical Privacy:* Economical privacy is a category not directly embedded in Article 8 ECHR. Although the authors of the European Convention on Human Rights explicitly chose to reject concerns over property and financial loss from the Convention as a whole and the right to privacy in particular, the ECtHR has gradually decided to bring such matters under the scope of Article 8 ECHR nevertheless. These cases are brought primarily against Italy and Turkey. There are relatively few of such cases before the European Court of Human Rights, but those that do get accepted are important in terms of damages being awarded. Compensation is primarily provided in the 'combination' category, which must be presumed to be made up primarily by material harm. Almost all cases judged by the Court (second-tier) with respect to this aspect of privacy lead to the consideration that there has been a violation of Article 8 ECHR.

I. Grounds for finding a violation

I. Introduction

115 The right to privacy under the European Convention on Human Rights is a so-called qualified right. This means that Article 8 ECHR specifies under which conditions the right can be legitimately curtailed by the government; these conditions are listed in paragraph 2 of Article 8 ECHR, which specifies: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.' Consequently, if the government infringes on a person's privacy, for example by entering his home, this need not be illegitimate or a violation of his privacy. The infringement can be deemed in harmony with the European Convention on Human rights when it abides by three cumulative requirements: (1) the infringement must have a legal basis; (2) must serve one of the legitimate goals as listed in the second paragraph of Article 8 ECHR; and (3) must be necessary in a democratic society.

116 Of the cases assessed by the ECtHR in the second-tier, there may be a number of reasons why no violation of Article 8 ECHR is found. For example, because the Court finds that a case has been wrongfully declared admissible, because a settlement has been reached by the parties in the meantime and the case needs to be struck from the list, or because a violation of another provision under the Convention has been established, and the Court finds it unnecessary to determine whether there has also been a separate violation of the right to privacy (the ECtHR may, for example, hold that in a case, a person's right to freedom from torture (Article 3 ECHR) had been violated and find it unnecessary to analyse to what extent the torture also violated a person's right to privacy). These are preliminary and procedural reasons. Alternatively, the ECtHR may find that although there has been an infringement of the right to privacy (as provided in paragraph 1 of Article 8 ECHR), this was a legitimate one and thus not in violation of Article 8 ECHR. The ECtHR only reaches this conclusion if all three requirements (legal basis, legitimate aim, necessary) have been fulfilled; if the government fails to fulfil either one of these requirements, a violation of the right to privacy will be found.

117 The Court may find that an infringement was not prescribed for by law for a number of reasons – the 'law', in this sense, is always the national law of a country. The ECtHR uses a quite wide definition of law, it includes not only legislation, but also judge-made law typical of common law jurisdictions and secondary sources, such as royal decrees and internal regulations.[57] First, a violation of the Convention will be found on this point if the actions of governmental officials are not based on a legal provision granting them the authority to act in the way they did. Second, a violation will be established if the conditions as specified in the law for using certain authority have not been complied with, for example, if police officials have no warrant for entering the home of a citizen. Third, the actions of the governmental officials may be prescribed for by law, but the law itself may not be sufficiently accessible to the public. Fourth, the law may be so vague that the consequences of it may not be sufficiently foreseeable for ordinary citizens. Fifth and finally, the ECtHR has in recent years developed an additional ground, namely that the law on which actions are based does not contain sufficient safeguards against the abuse of power by the government. This typically applies to laws authorizing mass surveillance activities by intelligence agencies that set virtually no limits on their capacities, specify no possibilities for oversight by (quasi-) judicial bodies, and grant no or very limited rights to individuals, with respect to redress.[58]

118 The Court may also find a violation of Article 8 ECHR if the infringement serves no legitimate aim.[59] The second paragraph specifies a number of legitimate aims, primarily having to do with security related aspects, such as national security, public safety, and the prevention of crime and disorder. These terms are sometimes used interchangeably by the Court, but in general 'national security' is applied in more weighty cases than 'public safety', and 'public safety' in more weighty cases than the 'prevention of crime and disorder'. The right of privacy may also be legitimately curtailed to protect the rights and freedoms of third parties; for example, a child may be placed out of home (an infringement on the right to family life of the parents), because the parents sexually molested the child. The protection of health and morals may be invoked to curtail the right to privacy, though this category is applied hesitantly by the ECtHR, because the protection of the morals of a country may lead to quite restrictive rules. Still with respect to controversial medical or sexual issues, such as euthanasia or BDSM, the ECtHR sometimes allows a country to rely on this ground to curtail the right to privacy. Finally, a country can rely on the 'economic wellbeing of the country'; this ground can only be found in Article 8 ECHR and in no other provision under the Convention. It is invoked by countries in a number of cases; for example, if an applicant complains about the fact that a factory or airport in the vicinity of his home violates his right to private life, the country can suggest that running a national airport is in fact necessary for the economic wellbeing of a country.

119 Much more can be said about the use, extent and interpretation of these aims, but this is unnecessary, because this requirement plays no role of significance. This is due to two factors. First, the ECtHR is often very unspecific about which term exactly applies, stressing that an infringement 'clearly had a legitimate aim', or that 'it is undisputed that the infringement served one of the aims as contained in Article 8 ECHR'. It often combines categories, underlining that the infringement served a legitimate aim, such as "'the prevention of crime', 'the economic well-being of the country' or 'the rights of others'" or it merely lists all different aims and holds that one of these grounds applies in the case at hand. Furthermore, it introduces new aims, not contained in Article 8 ECHR, especially in cases revolving around positive obligations for states (explained below). Second, the Court almost never finds a violation of Article 8 ECHR on this point. It usually allows the government a very wide margin of appreciation with respect to the question of whether and which of the aims apply in a specific case and whether the infringement did actually serve that aim. In many cases, it simply ignores this requirement when analysing a potential violation of the right to privacy or incorporates it in the question of whether the infringement was necessary in a democratic society. Thus, only in 20 cases was Article 8 ECHR violated on this point.

120 Finally, the third requirement that must be fulfilled by a government wanting to curtain the right to privacy is that the infringement must be necessary in a democratic society. This question is approached by the Court primarily as a question of balancing the different interests at stake. 'This test requires the Court to balance the severity of the restriction placed on the individual against the importance of the public interest.'[60] Consequently, to determine the outcome of a case, the Court balances the damage a specific privacy infringement has done to the individual interest of a complainant against its instrumentality towards safeguarding a societal interest, such as national security. It must be noted

57 <http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf>.

58 A recent case is: ECtHR, Zakharov v. Russia, applicaiton no. 47143/06, 04 December 2015.

59 <http://www.tandfonline.com/doi/full/10.1080/13600834.2015.1009714#>.

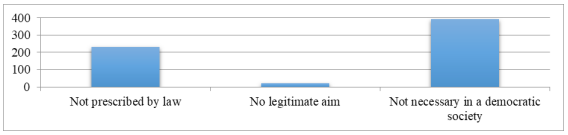
60 C. Ovey & R. C. A. White, "European Convention on Human Rights", Oxford, OUP, 2002, p. 209.

that this category is used in this study for three types of cases:

- First, cases regarding negative requirements of the government, which are or are not necessary in a democratic society.
- Second, as has been stressed earlier in this contribution, the ECtHR has accepted that a government may also be under a duty to use its powers in certain ways – it may have a positive obligation to protect the right to privacy of its citizens. In these types of cases, the Court usually balances the private interest of the applicant with the general interest (taken broadly, that is, not related to any of the official terms named in Article 8 ECHR). For example, is assesses the interests of transgender people in changing their name and weighs it against, the costs for society in setting up such an administrative possibility.
- Third and finally, Article 14 ECHR contains an explicit prohibition of discriminatory practices. The ECtHR has decided that this provision may only be invoked if one of the other material provisions under the Convention, such as the right to privacy or the right to freedom of expression have been infringed. To provide an example, if a country has a law that prohibits homosexuals from joining the army, this might lead to a violation of Article 14 in combination with Article 8 ECHR.

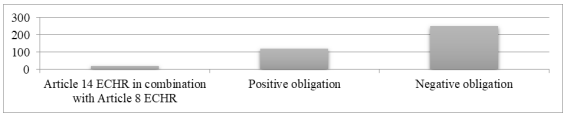
II. Results

121 Figure 33: Number of cases in which a violation of Article 8 ECHR was found on a certain ground:



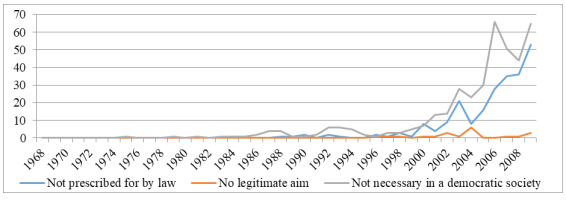
122 Figure 33 shows the number of cases in which the ECtHR has established a violation of the right to privacy per category. In somewhat less than 250 cases, the Court found that an infringement on Article 8 ECHR was not prescribed by law, in some 20 cases that the infringement served no legitimate aim, and in almost 400 cases that the infringement was not necessary in a democratic society. It should be noted that this does not mean that the ECtHR did establish that a violation was prescribed for by law and served a legitimate aim per se; although the Court usually runs through these three requirements meticulously, it will sometimes also use an 'even if' argumentation to avoid difficult discussions. For example, it may stress that 'even if the infringement was prescribed by law', there has in any case been a violation of the right to privacy because the infringement was not necessary in a democratic society.

123 Figure 34: Further division of the cases in which the necessity-requirement was breached:



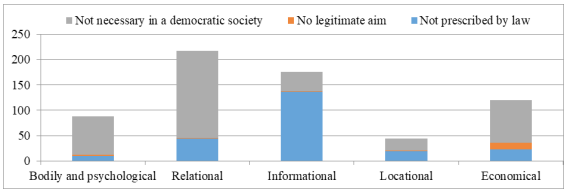
124 Figure 34 takes the cases which are categorised as violating the necessity-requirement. In reality, this category is a combination of three types of cases: matters regarding negative obligations by the state, positive obligations by the state, and cases in which a violation of the right to be free from discrimination was established, in combination with a violation of Article 8 ECHR. It appears that most violations are found on the basis of negligence in relation to the negative obligations by the state, followed by the cases in relation to positive obligations. Still, it must be pointed out that it is often very difficult to establish whether a case revolves around a negative or a positive olbigation and even the ECtHR has noted time and again that no real distinction can be made between these two categories. Hence, there is a considerable margin of interpretation and arbitrariness with respect to these numbers, which must consequently primarily be taken as indications rather than exact numbers. Finally, the Court has found a violation of the right to discrmination in combination with the right to privacy in less than 20 cases, and even in these cases, it was sometimes one of the less substantial points of the decision. For example, having already established that the right to privacy and/or another substantial provision under the Convention was violated, the Court pointed out briefly that there might also have been a violation of Article 14 and Article 8 combined. In fact, the ECtHR is often willing to judge cases regarding potential discriminatory practices with respect to the right to privacy under Article 8 ECHR, without additionally refering to Article 14 ECHR. Consequently, this latter provision plays only a minor role of significance in relation to the right to privacy.

125 Figure 35: Ground on which a violation of Article 8 ECHR was found divided per year:



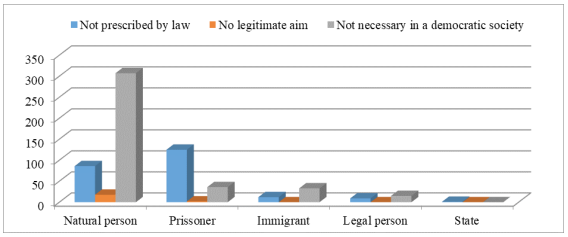
126 Figure 35 shows the number of cases in which a violation of Article 8 ECHR was established per category per year. The percentages of cases in which certain grounds led to the establishment of a violation of the right to privacy are relatively stable. The necessity-requirement has almost always been the most frequent ground, followed closely by the requirement of having a legal basis for the infringement. It may be pointed out that in more recent years, there seems a slightly higher percentage of cases in which a violation of the right to privacy was found on the ground that the infringement had no legal basis, but the period is too short to draw reliable conclusions on this point.

127 Figure 36: Ground on which a violation of Article 8 ECHR was found per type of privacy:



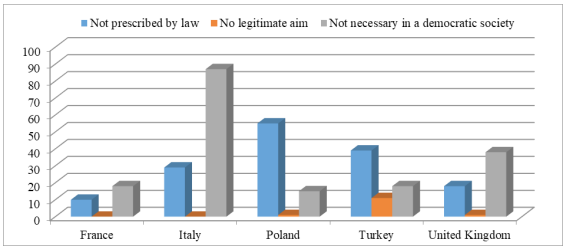
128 Figure 36 shows the ground on which a violation of the right to privacy was found, divided by type of privacy. It appears that in most categories, it is the necessity requirement that led to a breach of Article 8 ECHR most commonly, but with respect to locational privacy, around half of the cases in which a violation was established were due to the fact that the infringement had no legitimate basis, and with respect to informational privacy, this is true for almost 4/5 of the cases. A typical example of the first is when the private home of an individual is entered without a warrant and of the second is when the correspondence of a prisoner is monitored by prison authorities without a legal basis. Finally, it should be noted that the cases in which a violation of Article 8 ECHR was found because the infringement served no legitimate aim regarded almost exclusively economical privacy.

129 Figure 37: Ground on which a violation of Article 8 ECHR was found per type of applicant:



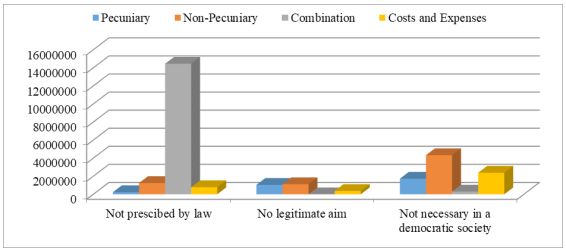
130 Figure 37 shows the reason for establishing a privacy violation divided per type of applicant. Figure 38 does the same with respect to the five countries against which most cases have been assessed by the Court (second-tier). With respect to prisoners, a violation of Article 8 ECHR is mostly established on the ground that the infringement was not prescribed for by law. Poland is the country against which these types of cases are most commonly established. Turkey is also involved in a number of these cases, as well as in cases in which it had destroyed or evacuated towns. The ECtHR has found a violation of Article 8 ECHR in these types of cases typically because no legal basis was found or because these actions served no legitimate aim.

131 Figure 38: Ground on which a violation of Article 8 ECHR was found per country:



132 Figure 39 shows the total amount of damages awarded by the ECtHR in cases in which a violation of Article 8 ECHR was found, divided per category. It seems that when the ECtHR finds that an infringement has no legal basis, it will provide a larger sum of damages than in other cases. This, however, is slightly misleading. In fact, this number is influenced by a few cases against Turkey, discussed earlier. In most cases in which a violation was found on this point, no or very low sums of damages were awarded. The Court found a violation of Article 8 ECHR in only 68 of the some 230 cases because the infringement was not prescribed by law has the Court granted more than € 3.000,- for either material or immaterial damages or in the combination category. Of the slightly more than 230 cases in this category, in almost 90, the ECtHR granted no damages in either one of these three categories.

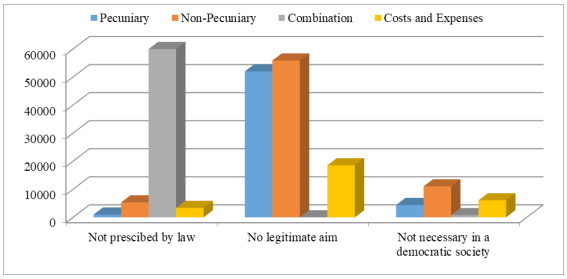
133 Figure 39: Total amount of damage awarded per category:



134 In fact, it seems that on average, the Court affords most damages to applicants if no legitimate aim was found for the infringement of Article 8 ECHR. But again, these are quite exceptional cases and moreover, the number of cases is rather small, so

that no reliable conclusions can be drawn on this point. With respect to the necessity-requirement, it appears that especially quite considerable amounts are offered to applicants for the relief of non-pecuniary damages.

135 **Figure 40: Average amount of damage awarded per case in which a violation of a requirement was found:**



III. Analysis

136 In this final substantial section, the reasons for finding a violation of Article 8 of the European Convention on Human Rights have been analysed. An infringement on the right to privacy (paragraph 1 of Article 8 ECHR) will be considered a violation if it is not prescribed by law, if it does not serve one of the legitimate aims listed in the second paragraph of Article 8 ECHR, or when the infringement cannot be deemed necessary in a democratic society. As shown in section I.II, each condition has its own set of particularities.

- Prescribed by law: this requirement seems to have become more important in recent years. An analysis of the case law of the Court on the right to privacy between 2010 and now must show whether these numbers are incidental or are part of a bigger trend. On average, relatively high amounts of damages are awarded to victims of privacy violations where the violation was found because of the lack of a legal basis. Still, this is due to a relatively small amount of cases where exceptionally high damages were awarded. In fact, in a most cases falling in this category, no or rather small sums of damages were awarded. Poland is the champion of infringing upon the right to privacy without a legal basis. There is a relatively high number of prisoners that are successful in claiming their right to privacy on this point. Moreover, the category of privacy that is mostly at stake when there is a problem with the legal basis is informational privacy. These three elements must be seen in relation to each other, because they revolve around cases in which the communication of Polish prisoners is monitored without a legal basis. Although Poland has been convicted for such behaviour a number of times, it apparently did not change its behaviour. In addition, with respect to a violation of locational privacy, the ECtHR often finds that there is no legal basis. Presumably, this is because the conditions specified in law, such as obtaining a warrant before entering the private domain of a citizen, were ignored.

- Legitimate aim: this requirement plays no role of significance in the jurisprudence of the European Court of Human Rights. It only finds a violation of the right to privacy on the basis of this ground in a handful of cases. Consequently, the conclusions gained from the results section must be approached with caution. What can be said is that, in general, relatively high amounts of damages are awarded for violations of privacy in this category. Turkey is involved with violations of Article 8 ECHR found in this category almost without exception; it mostly involves the aspect of economical privacy.

- Necessary in a democratic society: this requirement is the broadest and also the ground on the basis of which most violations of the right to privacy under the European Convention on Human Rights is found. Still, relatively small amounts of damages are awarded in this category on average. Italy and the United Kingdom are found in violation of this specific principle the most. With respect to the U.K., one explanation could be that the European Court of Human Rights has generally been hesitant to accept limitations on sexual freedom and a restrictive approach towards medical-ethical issues. The Court finds that a privacy infringement was not necessary in a democratic society in particular in relation to economical privacy, relational privacy, and the protection of one's bodily and psychological integrity.

J. Conclusion

137 This contribution has analysed the judgements delivered by the European Court of Human Rights on the point of Article 8 ECHR until 2010. It has tried to paint a broader picture with respect to the types of cases before the ECtHR, but has focused in particular on the question of how the Court calculates the damages afforded to the victims of a privacy violation. The ten most important findings of this study are:

1) Most damages have been awarded in the Combination category, which consists primarily of material damages, but also of immaterial damages or financial compensation for costs

and expenses made by the victims during their legal procedure. This is remarkable because the Combination category is used in a very limited number of cases. These are typically cases in which Turkey has engaged in gross human rights violations, for example by evicting people from their villages for a year.

2) There are clusters of cases to be made, which can be useful for further research. A cluster could be cases in which Poland is involved, the claimant is a prisoner, the type of privacy complained is informational privacy, and a violation is found because of the absence of a legal basis. Another may be cases with respect to the United Kingdom, involving ordinary natural persons, in which their bodily or psychological integrity is at stake and in which an infringement was not deemed necessary in a democratic society. A final example of such a cluster may be cases in which Turkey was involved, and natural persons invoked their economical privacy, a violation of the right to privacy was found because there was no legal basis or no legitimate aim involved and very high sums of damages were rewarded by the European Court of Human Rights.

3) Of the 648 cases in which the Court has found a violation of Article 8 ECHR, it awarded some type of relief in 564 of them, or in 440 of them, when the mere procedural costs (the awards for costs and expenses) are excluded. In almost 400 cases, the Court has awarded relief for non-pecuniary damages and in a similar number of cases, it has compensated the costs and expenses of the applicants. The damages awarded are usually relatively small figures. Per case in which a violation of the right to privacy was found, on average, € 4.632,- was awarded for pecuniary damage, € 10.323,- for non-pecuniary damage, € 22.773,- for a combination of categories, and € 5442,- for costs and expenses.

4) The total number of cases has increased exponentially over the years and from 2000 onwards, the ECtHR has held a violation of Article 8 ECHR in a significantly higher percentage of the cases before it. Consequently, the majority of the damage that has been awarded by the Court was granted in the last decennium. The non-pecuniary damage awarded per case has steadily but slowly increased over time. Perhaps more remarkable is that the costs and expenses awarded by the Court on average per case has dropped in the last decennium. It is unclear why. From the comparison between the last two decennia studied for this contribution, 1990-2000 and 2000-2010, it appears that the categories of pecuniary damage and of the combination of damages are communicating vessels. When the pecuniary damages are high, the combination category is relatively low and vice versa.

5) If the 5 countries are analysed against which the most cases under Article 8 ECHR were assessed by the European Court of Human Rights (second tier), it appears that a significant difference arises. While Poland is the country, which is held in violation of Article 8 ECHR most often after Italy, it is required to pay only minimal damages. Italy is primarily required to compensate non-pecuniary damages, while the United Kingdom has to pay quite significant amounts for both material and immaterial damages and for the costs and expenses. Turkey is the champion on the point of both material and immaterial costs, and in particular the 'Combination' category.

6) It appears that the Fourth section of the Court has in particular dealt with the cases in which the 'Combination' category was used. Apart from that, it is clear that especially the First and the Second section and the Grand Chamber attribute higher sums for immaterial damage than the other chambers. It also appears that the Third and Fifth section, as opposed to some other sections, have a quite even spread across the Pecuniary, Non-Pecuniary and Costs and Expenses categories.

7) When one applicant was involved with a complaint, on average, € 896,- was awarded for Pecuniary damages per case in which a violation of the right to privacy was established, € 5.906,- for Non-Pecuniary damages, € 5.488,- in the 'Combination' category, and €4.004,- for Costs and Expenses. When two applicants lodged a complaint, which resulted in a violation of Article 8 ECHR, this was on average € 8.385,- for Pecuniary and € 12.374,- for Non-Pecuniary damage, € 3.989,- for the 'Combination' category, and € 8.705,- for Cost and Expenses. These sums are for the applicants jointly and should consequently be divided by two to calculate the average amount of damages awarded per victim. The more applicants join in a case, on average, the more damage is awarded, which was to be expected.

8) Most damages have been awarded to ordinary natural persons. What is interesting is that on average, prisoners and immigrants have been awarded limited amounts of damages. This is because in a number of cases, the ECtHR stresses that the establishment of a violation in itself constitutes sufficient satisfaction for the applicant, for example, by holding that an immigrant should not be extradited or that a prisoner should have more liberties,

for example, with respect to family visits. With regard to legal persons, one could have expected that especially the pecuniary damages and the 'combination' category would be high, but the opposite is true.

9) It should not come as a surprise that most damages have been awarded for a violation of economical privacy. Judging from the amount of damages awarded in the other four categories, it seems that the Court is inclined to provide higher sums of damages for a violation of a person's bodily or psychological integrity and for an infringement on the privacy of his home than for a violation of relational or informational privacy. Out of the 89 cases in which the ECtHR found a violation of Article 8 ECHR with respect to bodily and psychological integrity, in 20 it provided no relief for damages or compensated only the legal costs in the Costs and Expenses category; for relational privacy, this was 60 out of 218 cases; for informational privacy, this was 73 out of 176; for locational privacy, this was 10 out of 44; and finally, for economical privacy this was 45 out of 120 cases. Consequently, the explanation is presumably that with respect to relational privacy, the ECtHR does provide damages, but only small sums.

10) Finally, it seems the case that when the ECtHR finds that an infringement has no legal basis, it will provide a larger sum of damages than in other cases. This number is, however, inflated by a few cases against Turkey, discussed earlier. In fact, in most cases in which a violation was found on this point, no or very low sums of damages were awarded. Only in 68 of the some 230 cases in which the Court found a violation of Article 8 ECHR because the infringement was not prescribed by law, has the Court granted more than € 3.000,- for either material or immaterial damages or in the combination category. Of the slightly more than 230 cases in this category, in almost 90, the ECtHR granted no damages in either one of these three categories. In fact, it seems that on average, the Court affords most damages to applicants if no legitimate aim was found for the infringement of Article 8 ECHR. But these are quite exceptional cases and moreover, the number is so small that no reliable conclusions can be drawn on this point. With respect to the necessity-requirement, it appears that quite considerable amounts are offered to applicants for the relief of non-pecuniary damages.

138 To conclude, this research has been a first enquiry into the way the ECtHR calculates damages afforded to victims of a privacy violation. It is based on the first results of a preliminary database of the jurisprudence of the ECtHR. It should be expanded further to include the cases after 2010. It could be equally interesting to include the cases on the admissibility of complaints under Article 8 ECHR (first-tier). Some additional factors could in time be developed, determining for example the type of interest that is relied on by the state or the way in which the Court reaches its conclusion.[61] It can also be the basis for comparative research, for example between Europe and the United States of America. Little comparative empirical data is available on privacy regulation on both sides of the Atlantic, so that reality and myth, fact and fiction, often go hand in hand and broad and vague contrast ('in Europe, privacy is protected by the state, in America, privacy protects citizens from the state', 'in Europe, privacy is dignity-based, in America, it is freedom-based' and 'in Europe, privacy is a human right, in America, it is a contractual freedom'), can be posed without a reality check.

139 This article has focused on the damages afforded. The reason is that recent literature and jurisprudence on privacy is especially focused on which types of interests the right to privacy should protect, which types of harms should be afforded damages in court cases, and whether in the Big Data era, individual harm can be taken as the corner stone of privacy case law at all. This article has done the opposite from what most other scholars have done; instead of focusing on the values privacy is said to protect, it starts with the end – the damages afforded in privacy cases, and rolls back from there. Although obviously, the damages awarded in cases in which a privacy violation is established is not the same as the values privacy protects, it can be taken as indicative all the same. The article has also done the opposite of most scholars, in that it has avoided normative speculations and interpretations, instead relying on empirical data. Obviously, subjective choices and normative decisions are also made when categorizing data, but there has been no agenda or specific hypothesis in mind when designing the database. It has taken a data-driven approach and has provided limited interpretation of the data – rather, it has remained mainly descriptive and explanatory in nature. It is up to the reader and other scholars to take these data and figures further and develop what they might say about the various normative debates.

61 See also: B. van der Sloot, 'How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one', Information & Communications Technology Law Volume 24, 2015.

jipitec

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

www.jipitec.eu