jipitec

3 | 2022

Volume 13 (2022)
Issue 3 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 13 Issue 3 September 2022
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

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

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

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

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

ISSN 2190-3387

Funded by

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

Articles

Reports

Editorial

by **Karin Sein**

Recommended citation: Karin Sein, Editorial, 13 (2022) JIPITEC 175 para 1.

This autumn issue of JIPITEC will be impossible to read in one extended evening: eight articles and one study summary will provide insights on different topics which will easily fill the whole weekend. Whereas most of the contributions address one or other aspects of intellectual property law in the digital realm, topical issues related to digital markets, Digital Content Directive as well as the proposal of the Data Act are examined as well.

The first three articles in this issue address the evergreen topic of digital platforms. Toygar Hasan Oruç questions the necessity to keep the prohibition of general monitoring obligations for video-sharing platforms on the background of the recent trend in the EU legislation to widen the responsibility of online intermediaries for illegal content. Karin Jackwerth tackles the hotly debated issue of the data-related market dominance of large online platforms, describing the response of the German legislator that was strongly influenced by the German competition agency's case against Facebook, and comparing it with the UK approach. She further examines the rules of the upcoming EU Digital Markets Act concerning the so-called gatekeepers and how they interact with the national legislation. The last 'platform article', written by Carlos Muñoz Ferrandis and Marta Duque Lizarralde, takes a yet different approach and investigates the commercial and policy strategic reasons behind the increasing use of open-source licensing of AI. They show that some players on the market are using open-source licensing to attract users and create an ecosystem around their AI platform: open-source licensing has become a competitive advantage for them as it reduces transaction costs, promotes faster technology adoption, and facilitates a free testing area.

The next two articles explore some less travelled roads of copyright law. First, Linda Kuschel and Jasmin Dolling analyse the legal framework in which research data can be accessed and used in EU copyright law, including the intriguing question of the applicable law in case of international research projects. Sunimal Mendis then challenges the copyright's individualistic conception of authorship and its exclusivity-based narrative, pleading for a collaborative (Wiki) authorship model that would regulate adequately the relationships between co-authors engaged in collaborative creation. The last article in this issue dealing with IP law written by Eleni Tzoulia investigates under which conditions blockchain as a standalone product or its individual components can be protected under the current EU intellectual property legislation, be it copyright, patent, or trade secret law – or whether blockchain may be subject to IP rights at all.

Legal science has its limitations when dealing with the complex societal issues posed by technical innovations and therefore JIPITEC is increasingly publishing interdisciplinary contributions. The question of why and when do readers trust the news that they read on the internet, for example, cannot be answered by legal scholars alone. Max van Drunen, Brahim Zarouali, and Natali Helberger offer us a valuable legal as well as empirical perspective on the role that law can play to support trust in the context of news personalization, concentrating on transparency and control measures.

Finally, Vadim Mantrovs, Jānis Kārklinš, Irēna Barkāne, Zanda Dāvida, Salvis Kārklis and Kristaps Silionovs provide a thorough analysis of Article 8(5) of the Digital Content Directive regulating the possibility to deviate from the objective conformity requirements in digital content or digital service contracts and offer useful insights regarding its interpretation.

Most of the articles in this autumn issue deal in one way or another with the recently adopted or soon-to-be-adopted EU legislation related to the digital economy, highlighting its increasing importance in this area. The summary of a study by Matthias Leistner and Lucie Antoine on the proposed EU Data Act not only helps to keep our readers updated with these developments but also provides a critical view of this proposal, describes its intersections with other legal acts, and offers concrete recommendations for its improvement.

Enjoy the read!

Karin Sein

The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it?

by **Toygar Hasan Oruç***

Abstract: The absence of a uniform notion of general monitoring, introduced under the E-Commerce Directive 2000/31/EC, leads to different interpretations of the scope and the role of the prohibition on general monitoring obligations by the EU legislators and by the Court of Justice of the European Union. While the Court of Justice of the European Union balances freedom of expression and information, right to privacy and protection of personal data and right to property on the same level of importance in determining the scope of general monitoring, this article shows that special protections attributed to the interests that are fundamental to human life and to our modern democracies under primary EU laws are ignored. Unfortunately, this further deepens the segregation in the different interpretations of general monitoring and creates an inconsistency among the recent EU legislations. The article notes that this inconsistency eventually causes a legal uncertainty for the video-sharing platforms regarding their content moderation practices and thus turning the prohibition into an empty shell. At the current stage, the article reveals the need for a clear distinction for VSPs between vertically applicable content moderation measures arising from content or sector specific regulations from the prohibition on general monitoring obligations. However, for future regulation in the EU, it is suggested to find an alternative solution to online monitoring which can suppress the impact of online illegal activities without restricting fundamental rights of individuals.

Keywords: monitoring; online; EU; intermediary; filter

Recommended citation: Toygar Hasan Oruç, The Prohibition of General Monitoring Obligation for Video-Sharing Platforms under Article 15 of the E-Commerce Directive in light of Recent Developments: Is it still necessary to maintain it? 13 (2022) JIPITEC 176 para 1

A. Introduction

1 In May 2015, the European Commission ("EC") set a goal to find how to best tackle illegal content on the Internet within the European Digital Single Market Strategy.[1] In the following year, the EC prioritised several issues relating to illegal online activities and their primary targets became, among others, the proliferation on video-sharing platforms ("VSP") of illegal content including terrorist content, child sexual exploitation, hate speech, the exposure of children and the general public to such content and the increasing inequity in the allocation of revenues generated by unlawful use of copyright-protected content between the rightsholder and VSPs.[2] The EC's Communication in 2017 marked the shifting policy discourse within the European Union ("EU") towards an enhanced responsibility of online intermediaries in the fight against these issues due to their central role in the dissemination of illegal content online.[3] The EC called, under the follow-up Recommendation, online intermediaries to adopt proactive measures and underlines the effectiveness of automated systems for the prevention of manifestly illegal content.[4]

2 On the other hand, this trend of widening the responsibility of online intermediaries in the crusade against illegal content and to ask them to implement proactive measures based on automatic filtering and detection technologies systems conflicts with the prohibition on the general monitoring obligation established under the Directive on Electronic Commerce ("ECD").[5] Although, the EC warned that the imposition of such proactive measures should respect the prohibition on general monitoring obligations, the absence of a uniform notion of general monitoring and the description of the prohibition creates legal uncertainty.[6] Particularly, while the recent EU legislations seem to require online intermediaries to implement measures to tackle the dissemination of illegal content, they also preclude those measures from leading to the ambiguous concept of *general monitoring*.[7] Therefore, this article aims to critically assess the role of the prohibition on general monitoring obligations under the evolving legislative landscape for VSPs in the EU.

3 The article starts with introducing the role of the prohibition on general monitoring within the online intermediary liability regime established under the ECD. Then, it reviews the interpretative case-law of the Court of Justice of European Union ("CJEU") concerning this prohibition and the intersection between the prohibition of general monitoring obligations and the fundamental rights protected by the Charter of Fundamental Rights of the EU ("Charter")[8] in order to identify the scope of general monitoring obligation. Chapter III discusses the interplay between the prohibition on general monitoring obligation and the recent EU legislations, the Audiovisual Media Services Directive amended in 2018 ("AVMSD")[9], the Regulation on Preventing Dissemination of Terrorist Content Online ("Terrorist Con-

* LLM, CIPP/E; Legal Counsel at Arthur's Legal B.V., Amsterdam; LLM in Innovation, Technology and the Law with Distinction, University of Edinburgh, 2020-2021. Email: toygaroruc@gmail.com. I would like to thank Joke Van Steenkiste for her continued support and Dr Paolo Cavaliere for his helpful comments on earlier drafts.

1 European Commission, 'A Digital Single Market Strategy for Europe' COM (2015) 192 final.

2 European Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' COM (2016) 288 final.

3 European Commission, 'Tackling Illegal Content Online Towards an enhanced responsibility of online platforms' COM (2017) 555 final.

4 European Commission, 'Recommendation on measures to effectively tackle illegal content online' C(2018) 1177 final.

5 Directive (EU) 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 L178/1.

6 Thomas Riis and Sebastian Felix Schwemer, 'Leaving the European Safe Harbor, Sailing Towards Algorithmic Content Regulation' (2019) 22 Journal of Internet Law 1; Maria Lillà Montagnani, 'A New Liability Regime for Illegal Content in the Digital Single Market Strategy' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138> accessed 16 August 2021.

7 Carsten Ullrich, 'Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective' (Social Science Research Network 2017) SSRN Scholarly Paper ID 3037744 <https://papers.ssrn.com/abstract=3037744> accessed 16 August 2021; Montagnani (n 7).

8 Charter of Fundamental Rights and Freedoms of the European Union [2012] OJ C 326/02.

9 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version), [2018] OJ L 095/1

tent Regulation")[10] and the Directive on Copyright in the Digital Single Market ("Copyright Directive")[11]. Particularly, by analysing the permissible scope of the measures introduced under these new legislations with the CJEU's interpretation of general monitoring, the article aims at revealing the discrepancy in the implementations of the prohibition under the new EU liability regime for online intermediaries. Lastly, Chapter IV explains how this discrepancy creates legal uncertainty for the VSPs providers.

B. Understanding the Prohibition on General Monitoring Obligation

I. The Prohibition of General Monitoring Obligations under the E-Commerce Directive

4 At the EU level, the general legal framework for the online intermediary liability regime was established under the ECD in 2000. It introduced harmonised rules which apply to all providers of *information society services*, commonly referred to as o*nline intermediary services*, defined as services that are normally provided for remuneration or as a part of the economic activity, at a distance, by electronic means for the processing and storage of data upon an individual request of their user.[12] Article 14 of the ECD provides a special safe harbour regime for hosting service providers which store and host information by and at the request of their users, such as online marketplaces, social media networks, VSPs, etc. Due to its very nature, hosting services are often prone to be contaminated with illegal content uploaded by their users and therefore are subject to stricter exemption rules than other types of online intermediaries such as conduit and cashing service providers.[13] Accordingly, these providers are exempted from liabilities for the illegal content on their services uploaded by a user as long as (i) it has no actual knowledge of its user's illegal activity and is not aware of facts, and circumstances from which the illegal activities or information is apparent[14] and (ii) once it obtains such knowledge/awareness, it acts expeditiously to remove or disable access to the information.[15] This exemption is applicable only to those cases where the activity of the hosting service providers is deemed merely technical, automatic and passive which implies that the online intermediary has neither knowledge of nor control over the information which is transmitted or stored.[16]

5 This safe harbour regime is supplemented by Article 15(1) which prohibits member states from imposing general obligations on online intermediaries to monitor the information transmitted or stored on their services, or to actively look for facts or circumstances indicating illegal activity. According to the EC's Communication 'A European Initiative in Electronic Commerce' in 1997[17], the European Parliament Resolution on this Communication in 1998[18] and the First Report on the application of the ECD in 2003, this safe harbour regime including the prohibition on general monitoring obligation was rested mainly on five reasons: (i) online intermediaries, while in their infancy, lacked the technical capacity to actively and accurately monitor the massive amount of information transmitted via their services,[19] (ii)

10 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online [2021] OJ L 172/79 (Regulation on Preventing Dissemination of Terrorist Content Online).

11 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92 (The Directive on Copyright in the Digital Single Market).

12 The E-Commerce Directive, Article 2(a), Recital 18; Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, [2015], OJ L 241/1, Article 1(1)(b).

13 Edwards (n 19); De Streel and others (n 9).

14 The E-Commerce Directive Art 14(1)(a).

15 The E-Commerce Directive Art 14(1)(b).

16 The E-Commerce Directive, Recitals 42; Case C-236/08, *Google France, Google Inc v Louis Vuitton Malletier SA and Others* [2010], ECLI:EU:C:2010:159, paras 113-116.

17 The European Commission, 'A European initiative in electronic commerce. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions' COM (97) 157, 16 April 1997.

18 The European Parliament, 'Resolution on the communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on a European Initiative in Electronic Commerce (COM(97)0157 C4-0297/97)' C 167/203, 1 June 1998.

19 Commission, 'First Report on the Application of 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' COM/2003/0702 final, p 14.

such monitoring obligation was deemed unfair as it creates a burden on those acting as passive mere intermediaries,[20] (iii) a desire not to deter a developing online commerce industry in the EU with "over-regulation", (iv) the risk of over-blocking of legitimate content, i.e. free flow of information within the single market, due to the false positives of automated system or due to the tendency to avoid liability[21], and (v) the risk of creating actual knowledge and awareness which would result from an illegal content that slipped away from general proactive monitoring.[22] On the other hand, both the EC's first report as well as Recital 47 of the ECD note that this prohibition covers only the monitoring obligation in a general manner and does not include monitoring obligations in a specific case. Furthermore, it does not preclude national courts to order the online intermediary to prevent an infringement[23] nor member states to impose a duty of care to hosting service providers to detect and prevent certain types of illegal activities.[24]

6 Although, it is obvious that *monitoring* means the supervision of data traffic on the service, the ECD fails to provide guidance on the difference between the monitoring obligation "of a general manner" and "in a specific case".[25] Since the general monitoring prohibition determines the permissible scope of the measures which can be imposed on online intermediaries against illegal content, this ambiguity would likely cause problems in practice. Given that hosting service providers can still be required to prevent a specific infringement or certain illegal activities under the ECD[26], it becomes important to determine the extent of such preventive measures.[27] In fact, for the prevention of illegal content, the most effective option[28] becomes the adoption of filtering systems that monitor content either before or very shortly after it has been posted by its user.[29] Due to this ambiguity, the question as how to distinguish prohibited general monitoring obligations from permissible monitoring obligations has been addressed by the CJEU under the several preliminary rulings.

II. The CJEU's Interpretation of General Monitoring Prohibition

7 *L'Oréal v eBay* is the first case in which the CJEU assessed the compatibility of a court injunction on an online marketplace to prevent the future infringement of the trademark rights by internet users. The CJEU found that such preventive injunction would require eBay to conduct "active monitoring of all the data of each of its customers in order to prevent any future infringement" of L'Oréal trademarks and thus constitute general monitoring.[30] Instead, the CJEU suggested two measures: firstly,

20 Ibid.

21 Christophe Geiger, Giancarlo Frosio and Elena Izyumenko, 'Intermediary Liability and Fundamental Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 146 <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138> accessed 23 August 2021.

22 Edwards (n 19); Carsten Ullrich, 'A Risk-Based Approach towards Infringement Prevention on the Internet: Adopting the Anti-Money Laundering Framework to Online Platforms' (2018) 26 International Journal of Law and Information Technology 226; Giovanni Sartor, 'Providers Liability: From the ECommerce Directive to the Future' (European Parliament 2017) PE 614.179. <https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA(2017)614179> accessed 10 August 2021.

23 This conclusion is based on interpretation made by reading Recital 47 together with Article 14(3) of the ECD.

24 The E-Commerce Directive, Recitals 48.

25 Graham Smith, 'Time to Speak up for Article 15' (21 May 2017) <https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html> accessed 23 August 2021.

26 The E-Commerce Directive Article 14(3), Recital 48.

27 Madiega (n 9); Martin Senftleben and Christina Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3717022 <https://papers.ssrn.com/abstract=3717022> accessed 21 May 2021.

28 Carey Shenkman, Dhanaraj Thakur and Emma Llansó, 'Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis' (Center for Democracy & Technology 2021) <https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/> accessed 18 August 2021; Sartor and Loreggia (n 9) 23 et seq. This report indicates effectiveness of automated systems for finding duplicates of identical or equivalent content to pre-identified illegal content under sufficient human supervision.

29 Aleksandra Kuczerawy, 'To Monitor or Not to Monitor? The Uncertain Future of Article 15 of the E-Commerce Directive' (*CITIP blog*, 10 July 2019) <https://www.law.kuleuven.be/citip/blog/to-monitor-or-not-to-monitor-the-uncertain-future-of-article-15-of-the-e-commerce-directive/> accessed 25 July 2021.

30 *L'Oréal SA and Others v eBay International AG and Others* [2011]

the suspension of the infringing users who sold the counterfeit L'Oréal products on the platform in order to prevent further infringements of L'Oréal's rights by the same users and secondly, the adoption of user identification measures to identify real persons behind the user accounts infringing copyrights and thus to prevent those suspended infringers from operating on the same platform under different user accounts.[31] The rationale of these suggestions is found in the analysis made by Advocate General ("AG") Jääskinen who determined double requirements of identifications of infringed right and of the infringer as an appropriate limit of a preventive measure. He opined that an injunction requiring an online intermediary to only target an infringement of the same trademarks by the same users would be permissible under Article 15(1) ECD.[32] It is argued that the CJEU's suggestions are based on this opinion since both measures require the collective application of the detection of infringement of the specific trademark and identification of specific users.[33] This means that monitoring in a "specific case" must be understood in the sense of a specific incident of infringement, i.e. infringement by the specific users, rather than in the sense of all incidents of the same trademark infringement. The latter is found to require active monitoring of all the data of each of eBay's customers, which therefore violates the prohibition on general monitoring.[34]

8 This interpretation was later tested in both the *Scarlet Extended v SABAM*[35] and the *SABAM v Netlog* cases[36] in which the CJEU discussed whether an injunction ordering a mere conduit provider and a hosting service provider, respectively, to implement a permanent filtering system to prevent infringement of specific copyright-protected works, i.e., those listed in the repertoire of the Belgian collecting society SABAM, complies with Article 15(1) ECD. The CJEU noted that the implementation of such filtering system needs three main functions: (i) to identify content that includes copyright-protected works within all the content moving through the service, (ii) to assess whether those works are used unlawfully; and, if so, (iii) blocking or removing access to the content containing such illegal use of copyright-protected works.[37] Considering these functions, the CJEU concluded that such filtering mechanism would eventually require the *active observation* of *all information* provided by *all users* and thus it would amount to general monitoring.[38]

9 This conclusion is in line with the L'Oréal judgement. Although the injunctions in both cases were targeted to specific content, i.e. L'Oréal's trademarks and SABAM's works, the CJEU considered the blanket monitoring of all activity by all users as general monitoring regardless of whether such monitoring is targeting only the infringements of specific rights. This means, due to its basic working principle, i.e., monitoring all users' content, all possible filtering measures would fall under this classic generality. In fact, this *ratione materiae* is also adopted by AG Villalón Cruz in the *Scarlet Extended v SABAM*. He stated that the implementation of filtering measures requires prior monitoring of all information and without prior monitoring, these filtering measures cannot succeed.[39] Similarly, in the *McFadden v Sony Music* case, an injunction requiring a mere conduit provider to examine all information transmitting through its internet connection services in order to prevent third parties from infringing the particular copyright-protected works of Sony is found incompatible with Article 15(1) as it would require monitoring of all information from all users.[40] According to Senftleben and Angelopoulos (2020)[41] and Kulk and Borgesius (2013)[42], the CJEU's findings in all these cases suggest that the permissible *specific* monitoring under Article 15(1) would be a filter system targeting specific, pre-notified infringements within the content posted by a specific group from among

CJEU C-324/09, 2011 I-06011 [139].

31 Ibid 141.

32 *L'Oréal SA and Others v eBay International AG and Others* [2011] CJEU C-324/09, Opinion of AG Jääskinen [181, 182].

33 Senftleben and Angelopoulos (n 32); Julia Reda, Joschka Selinger and Michael Servatius, 'Article 17 of the Directive on Copyright in the Digital Single Market: A Fundamental Rights Assessment' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3732223 <https://papers.ssrn.com/abstract=3732223> accessed 19 August 2021; Frosio (n 9).

34 *L'Oréal SA and Others v eBay International AG and Others* (n 35) para 139.

35 *Scarlet Extended v SABAM* [2011] CJEU C-70/10.

36 *SABAM v Netlog NV* [2012] CJEU C-360/10.

37 *Scarlet Extended v SABAM* (n 40) para 38; *SABAM v Netlog NV* (n 41) para 36.

38 *Scarlet Extended v SABAM* (n 40) para 40.

39 Case C-70/10 *Scarlet Extended v SABAM* [2011] ECR I– 11959, Opinion of AG Villalón Cruz, para 46.

40 Case C-484/14 McFadden v Sony Music [2016] ECLI:EU:C:2016:689, para 87.

41 Senftleben and Angelopoulos (n 32).

42 Stefan Kulk and Frederik Zuiderveen Borgesius, 'Filtering for Copyright Enforcement in Europe after the Sabam Cases' (2013) 34 European Intellectual Property Review 791.

all of an intermediary's users who are pre-identified as likely to share infringing content.

10 In 2019, the CJEU introduced a significant addition to this interpretation and widened the scope of permissible *specific* monitoring in the *Glawischnig-Piesczek v Facebook* case.[43] The CJEU permitted an injunction ordering a hosting service provider, Facebook, to remove content containing identical or essentially unchanged defamatory content that was previously declared illegal by a national court, "irrespective of who requested the storage of that information"[44], on condition that clear instructions must be given to the provider on how to identify such content so that it would not have to adjudicate the legality of the content.[45] For instance, any content containing the plaintiff's picture alongside a combination of certain insulting words, which have the same meaning to those used in the defamatory content, were determined as equivalent content in this context by the Austrian court. This means that to prevent the recurrence of such defamatory content, the online intermediary does not have any option but to monitor all information uploaded by all users which was explicitly rejected by the CJEU in the previous McFadden, SABAM and L'Oréal cases.

11 The reason behind this widening approach seems to be the CJEU's acknowledgement of the dynamic nature of the social network environment which allows a swift flow of the same information among its users and thus making monitoring meaningless to focus on pre-identified users.[46] Therefore, this judgement changed the scope of general monitoring, at least for defamatory cases, by allowing the active observation of all information uploaded by each service user in order to prevent *pre-identified* infringements.[47] According to the CJEU, the defining character of *prohibited* general monitoring becomes the requirements for online intermediaries to carry out an independent legal assessment of the illegal nature of the content.[48]

12 This broad interpretation was supported and the permissible scope of monitoring was further extended to copyright infringements in the *Petersons/Elsevier v Youtube/Cyando* case. The CJEU was asked whether an injunction for the removal and prevention of copyright infringing content, which exposes its addressee to unduly court costs, can be imposed on online intermediaries even if they fulfil the conditions of the safe harbour rules for hosting service providers under Article 14(1).[49] The CJEU noted that such an injunction would amount to the general monitoring obligation as it may force online intermediaries, which want to avoid court expenses, to actively monitor all the content uploaded by their users to prevent any copyright infringement.[50] However, it is allowed to impose a pre-condition for such an injunction requiring rightsholders to notify the online intermediary of an infringement prior to the commencement of court proceedings, in order to allow online intermediary to take necessary measures to prevent those notified infringements from recurrence and thus avoid being the subject of an injunction and subsequently court costs would not constitute general monitoring obligation.[51]

13 Although, the CJEU did not settle its ruling with the previous interpretation in the Glawischnig-Piesczek case, with respect to targeting copyright infringements instead of defamatory content, the AG Saugmandsgaard Øe's opinion provides a convincing reconciliation. Upon assessing the identical and equivalent content standard determined in the Glawischnig-Piesczek case in the context of copyright law, he concluded that identical content means the content that contains the exact use of the same copyright-protected work which was previously found to be infringing, whereas equivalent

43 Case C-18/18, *Eva Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821.

44 Ibid para 37.

45 Ibid para 53.

46 Ibid 36.

47 Eleftherios Chelioudakis, 'The Glawischnig-Piesczek v Facebook Case: Knock, Knock. Who's There? Automated Filters Online' (*CITIP Blog*, 12 November 2019) <https://www.law.kuleuven.be/citip/blog/the-glawischnig-piesczek-v-facebook-case-knock-knock-whos-there-automated-filters-online/> accessed 15 August 2021; Eleonora Rosati, 'Material, Personal and Geographic Scope of Online Intermediaries' Removal Obligations beyond Glawischnig-Piesczek, C-18/18 and Defamation' (2019) 41 European Intellectual Property Review 672; Paolo Cavaliere, 'Glawischnig-Piesczek v Facebook on the Expanding Scope of Internet Service Providers' Monitoring Obligations (C-18/18 Glawischnig-Piesczek v Facebook Ireland)' (2019) 5 European Data Protection Law Review 573; Kuczerawy (n 34); Daphne Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling' (2020) 69 GRUR International 616.

48 Ibid 46. The CJEU notes that monitoring for identical and equivalent content which contains specific elements pre-identified by a national court would be done by automated tools and technologies without having online intermediary conduct an independent legal assessment.

49 *Frank Peterson v Youtube Inc and Elsevier Inc v Cyando AG* [2021] CJEU Joined Cases C-682/18 and C-683/18.

50 Ibid 129.

51 Ibid 136, 137.

content includes identical files that use the same work in the same way but which may have been uploaded in a different format.[52] For instance, a video showing an entire movie in a smaller screen frame on YouTube without any additional contextual information would comply with this equivalent infringing use of copyright-protected work standard.[53]

14 Moreover, the CJEU did not explain how exactly an online intermediary that previously was informed of an infringement should prevent the recurrence of that infringement. However, by analogy with the permissible duty of care obligation to prevent certain types of illegal content under Recital 48 the ECD, the CJEU's judgement can be interpreted as: online intermediaries may be forced to filter all information on their services to detect certain infringing content which is pre-identified by a national court in line with Saugmandsgaard Øe's standards. In fact, before the CJEU approved the contested condition for the preventive injunction in YouTube/Cyando case, it reiterated from the SABAM judgements that "requiring a service provider to introduce, ('...') [a] system which entails general and permanent monitoring in order to prevent any future infringement of intellectual property rights were incompatible with Article 15(1)".[54] The difference between the contested condition and this quotation is that monitoring in the former is limited with the pre-notified copyright infringement and its obligation starts upon the receipt of a notification while the injunction in SABAM cases requires monitoring of any infringements containing specific copyright-protected works which needs a contextual analysis from an online intermediary for an indefinite time. As explained in the foregoing paragraph, this conclusion also reconciles with the CJEU's approval for monitoring obligation for specific defamatory content in Glawischnig-Piesczek case.[55]

15 In the very recent ruling of *Poland v European Parliament and the Council of the European Union C-401/19* case ("Poland v Parliament and Council")[56], the CJEU confirmed this conclusion by reiterating its interpretations of general monitoring in both YouTube/Cyando and Glawischnig-Piesczek cases. The CJEU was asked to annul Article 17(4) of Copyright Directive which provides for the obligation for online content sharing services, a type of hosting service providers, to make their best effort, with high industry standards of professional diligence, to prevent the occurrence of a copyright infringement if the service providers concerned have received from the rightsholders sufficiently substantiated, relevant and necessary information of specific copyright infringement. First of all, the court concluded that requirement of best effort with high industry standards of professional diligence to prevent the occurrence of a copyright infringement obliges very large content sharing services, which receive thousands or millions of daily uploads, to carry out prior review and filtering of online content via automatic recognition and filtering tools.[57] However, the court also notes that this obligation becomes applicable only after the service provider receives *sufficiently substantiated* notice the specific infringement or *relevant and necessary* information regarding the copy-right protected work which must enable the service provider to identify the unlawful content without conducting legal assessment.[58] Lastly, once again the court pointed out that generally the service providers "cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright ('...')" as this leads to general monitoring obligation.[59]

16 The CJEU's recent clarification of general monitoring obligation confirms that any obligation to online intermediaries requiring filtering all the information on their services to detect and remove the illegal content on condition that the identification of such content must not require "an independent assessment" or "legal examination". This means online intermediaries should not be required, for example, to carry out a contextual analysis of content that contains the defamatory content pre-identified by a court but in a significantly different context or which includes a copyright protected work used in such a way that contrast the information provided by rightsholders with applicable copyright exceptions.[60] In line with Saugmandsgaard Øe's opinion in both the Poland v Parliament and Council case

52 *Frank Peterson v. Youtube Inc and Elsevier Inc. v. Cyando AG* Joined Cases C-682/18 and C-683/18 Opinion of the AG Saugmandsgaard ØE, 16 July 2020.

53 Reda, Selinger and Servatius (n 38) 17.

54 *Frank Peterson v. Youtube Inc and Elsevier Inc. v. Cyando AG* (n 49) para 135.

55 Reda, Selinger and Servatius (n 38).; *Eva Glawischnig-Piesczek* (n 24) paras 45-46.

56 Republic of Poland v European Parliament and Council of the European Union [2022] CJEU C-401/19.

57 ibid 54.

58 ibid 89–90.

59 ibid 90.

60 Republic of Poland v. European Parliament and Council of the European Union, Case C-401/19 Opinion of the AG Saugmandsgaard ØE, 15 July 2021, para 198.

and the Youtube/Cyando case, the CJEU seems to agree that any obligation to implement upload filters against manifestly illegal content, the illegal nature of which either is clear and obvious to a reasonable person or has been previously determined by a court, does not constitute general monitoring obligation.[61]

III. Intersection with Fundamental Rights and Freedoms

17 Within its interpretative case-law, the CJEU noted that while the monitoring obligations generally aim to protect the rights and interests of the people, e.g. the right to intellectual property[62], the right to reputation[63] from the infringements by internet users, it also burdens the internet users' rights to privacy and data protection, freedom of expression and information and the online intermediary's freedom to conduct a business under Articles 8, 11, and 16 of the Charter respectively.[64] In the face of this clash, the CJEU developed a *fair balance* test to strike the balance between these competing rights and interests within the framework of the online intermediary liability regime. The analysis of the CJEU's fair balance test would present how permissible *specific* monitoring obligations can be implemented. The justification for the imposition of liability on online intermediaries is supplemented by the context of the rulings of the European Court of Human Rights in which freedom of expression and information are balanced against the right to privacy in reputation.[65]

18 Apart from these fundamental rights, scholars have also raised concerns over the negative impacts of automated monitoring systems on the internet users' rights to equality and non-discrimination due to inherent bias in algorithms and thus the absence of the rights to a fair trial and effective remedy of those whose online expression is restricted by the over-blocking.[66] As both of these issues are discussed by the CJEU and AGs in relation to the risk of *over-blocking* of the users' legitimate expressions, this section will evaluate the impact on these two fundamental rights under the CJEU's fair balance test for freedom of expression and information and then the suitability of the balancing approach in the context of general monitoring of online content will be questioned below.

1. Striking a Fair Balance Between the Fundamental Rights

19 In the Promusicae case, the CJEU acknowledged that the provisions of ECD must be interpreted in such a way that it strikes a fair balance between different fundamental rights involved.[67] In the following L'Oréal case, after finding the double targeting preventive measure compatible with Article 15(1) ECD, the CJEU noted that a fair balance must be

61 Ibid.

62 *L'Oréal SA and Others v eBay International AG and Others* [2011] CJEU C-324/09, 2011 I-06011; *Scarlet Extended v SABAM* [2011] CJEU C-70/10; *SABAM v Netlog NV* [2012] CJEU C-360/10; *Frank Peterson v. Youtube Inc and Elsevier Inc. v. Cyando AG* (n 49); *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

63 *Eva Glawischnig-Piesczek* (n 24)

64 *Scarlet Extended v SABAM* (n 14) paras 48, 50, 52; *SABAM v Netlog NV* (n 15) paras 47-48; *Peterson/Elsevier v Youtube/Cyando* (n 47) para 138.

65 The ECtHR has discussed, in multiple disputes, whether a hosting service provider should be liable for user-generated content and obliged to monitor and filter proactively its networks to avoid liability. Although the ECtHR's role as adjudicator of the European Convention on Human Rights ("**ECHR**") does not include to interpret EU laws, its rulings concerning the human rights-based limits on monitoring in the context of online intermediary liability still are relevant for current policy discussions on monitoring obligation in the EU. Because Article 51(3) of the Charter indicates that the meaning and scope of the rights that are protected both in the Charter and the ECHR should be the same, unless the Charter provides more extensive protection and thus ECHR-based fundamental rights constitute an integral element in the EU's constitutional order. Therefore, this section will use the ECtHR's case-law to understand the role of fundamental rights in general monitoring prohibition.

66 Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 10,11 <https://doi.org/10.1177/2053951719897945> accessed 2 April 2021; Keller (n 52) 617; Reuben Binns and others, 'Like Trainer, Like Bot? Inheritance of Bias in Algorithmic Content Moderation' in Giovanni Luca Ciampaglia, Afra Mashhadi and Taha Yasseri (eds), *Social Informatics* (Springer International Publishing 2017); Christophe Geiger and Bernd Justin Jütte, 'Platform Liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70 GRUR International 517. Based on several studies, it is noted that automated filtering systems have unequal impacts on different populations is it will inevitably have to privilege certain formalisations of offence above others and disproportionately silence lawful of certain groups.

67 Case C-275/06, *Promusicae v Telefónica de España SAU* [2008] ECLI:EU:C:2008:54, para 63.

struck when implementing these measures.[68] In the very recent Poland v Parliament and Council case, the CJEU clarified how to carry out a fair balance test when a legal obligation targeting protection of right to intellectual property clearly entails a limitation on the exercise of the right to freedom of expression and information.[69] Pursuant to these three judgements, it is evident that even though the monitoring obligations satisfy the specificity standards as discussed in preceding Section II, they must still not constitute an excessive restriction on the fundamental rights.

a) Online Intermediary's Freedom to Conduct a Business

20 In the SABAM cases, the CJEU ruled that an injunction requiring an online intermediary to install filtering systems, at its own expenses, to monitor all the electronic communications to filter any copyright infringement, fails to find a right balance between the intermediary's freedom to conduct a business and the right to intellectual property. It noted that such system would be too sophisticated since it targets infringements of not only existing works, but also of future works that have not yet been created.[70] Therefore, obliging online intermediaries to implement such a complex system for an unlimited time was found to be an unproportionate burden on their business.

21 Similarly, in the later *UPC Telekabel v Constantin* case, the CJEU noted that imposing an open-ended injunction requiring a mere conduit provider to block access to a website with copyright infringing content would constitute a burden as it requires an online intermediary to implement complex technical solutions that would result in significant costs and have a considerable impact on the organisation of the online intermediary's activities.[71] On the other hand, the CJEU noted that it would strike a fair balance between the right to intellectual property and the intermediary's freedom to conduct business under certain conditions. First, the online intermediary must be given the freedom to choose how to block specific content in proportion to its resources and abilities.[72] Secondly, the measure implemented by an intermediary must be reasonable in light of the technical and financial capacity of that intermediary, and capable of making it difficult to commit an illegal act by internet users.[73]

22 Although the CJEU did not conduct a detailed fair balance test in the Glawischnig case, the AG Szpunar's opinion may provide some guidance. Accordingly, imposing the obligation to monitor all information in order to filter the content identical to those previously identified as defamatory content by the court would not require sophisticated technology and therefore would strike a fair balance between intermediaries' freedom to conduct a business and the right to reputation.[74] On the other hand, he warned that extending the scope of monitoring from identical to the equivalent content would not be compatible with the fair balance test. This was because the monitoring obligation to target equivalent content would require contribution of the provider in the legal assessment of the content and thus, it would be costly and require sophisticated solutions for the intermediary to develop.[75] The CJEU seemed to share the AG Szpunar's concern over the legal assessment requirements in its judgement as it concluded that the scope of monitoring must be limited with the content containing properly identified specific elements which can recourse to automated search tools and technologies and thus will not require further an independent assessment of the provider.[76]

23 In the YouTube/Cyando case, AG Saugmandsgaard ØE took a similar position by noting that a sufficiently precise or adequately substantiated notification regarding a copyright infringement enables the online intermediary to detect the infringing nature of the content without conducting a legal examination and therefore any monitoring obligation targeting such infringement would not constitute a burden on the intermediary's freedom to conduct a business.[77] In line with the Telekabel judgement, he warned that imposition of such monitoring obli-

68 *L'Oréal SA and Others v eBay International AG and Others* (n 10) para 143.

69 *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

70 *Scarlet Extended v SABAM* (n 14) paras 47,48; *SABAM v Netlog NV* (n 15) paras 46, 47.

71 C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH* [2014] ECLI:EU:C:2014:192 (UPC Telekabel case), para 50.

72 Ibid paras 51, 52.

73 Ibid paras 59, 60.

74 Case C-18/18, *Eva Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821, Opinion of AG Spunzar, paras 62, 63.

75 Ibid paras 73, 74.

76 *Eva Glawischnig-Piesczek* (n 24) para 47.

77 Joined Cases C-682/18 and C-683/18, Peterson/Elsevier v Youtube/Cyando [2021] ECLI:EU:C:2021:503, Opinion of the AG Saugmandsgaard ØE, paras 188,189,194, 221.

gation must be proportionate with the available resources of the providers since not all service providers have the necessary technical and financial resources to implement it.[78] It is not clear how the CJEU applied this proportionality requirement in its judgement. However, considering that the CJEU found YouTube's Content ID[79] as an "appropriate technological measure" to counter effectively infringements of pre-identified copyrights on intermediary service,[80] it can be argued that filtering obligations on financially and technically resourceful online intermediaries, like YouTube, against pre-identified illegal content that are capable of being identified solely by automated means, will not constitute a burden on their freedom to conduct a business. Because first, such an automated monitoring system will not be too sophisticated as no contextual judgement is required and second, its development costs would be proportionate in accordance with available resources. This interpretation also aligns with the CJEU's emphasis on automated tools in the Glawischnig judgement as well as in the Poland v Parliament and Council judgement.[81]

b) Internet Users' Freedom of Expression and Information

24 Secondly, in both the SABAM cases and in the Poland v Parliament and Council case[82], the CJEU noted that requiring providers to implement an ex-ante filtering system *could* limit the users' freedom of information, because the technology may not adequately distinguish legal content from illegal ones, so its application could lead to the blocking of legal communication.[83] Likewise, the Telekabel judgement noted that in order not to unnecessarily deprive internet users of the possibility of lawfully accessing the information available, any blocking measures must be *strictly targeted* so that the rights of non-infringing users should not be affected.[84] This reasoning also explains the rationale behind the double identifications requirement in the L'Oréal judgement. More importantly, the CJEU requires that internet users whose information at risk of over-blocking should be given *locus standi* to defend their rights in order to legitimately restrict users' freedom of expression and information.[85]

25 AG Spunzer, in the Glawischnig case, opined that imposing a filtering obligation for pre-identified specific content would not impair the internet users' freedom of expression if it does not require the active participation of the intermediary in legal assessment of the content.[86] Because this poses a risk of losing the liability exemption under the ECD, online intermediaries would be inclined to remove the content on which they cannot ensure its illegality and therefore, would end up with systematically restricting internet users' freedom of expression and information.[87] Perhaps, the CJEU's explicit emphasis on the use of an automated system which does not require an independent assessment by the provider for the filtering of defamatory content[88] could be the result of the same concern. Interestingly, the CJEU made no point on the over-blocking risk caused by the inaccuracy of filtering technologies as it was the issue in the SABAM cases. Possibly, in these judgments, the CJEU shared the opinion of AG Szpunar on that the current technology can distinguish the reproduction of identical unlawful content, which had been pre-identified and notified to the service provider, from other lawful communications.[89]

26 Similarly, in line with AG Saugmandsgaard ØE emphasis on the risk of "over-removal"[90], the YouTube/Cyando judgement highlights the importance of the provider's neutrality in the decision-making process and thus requires that any notification of an infringement must "contain sufficient information to enable" the online intermediary "to satisfy itself, without a detailed legal examination, that the content is illegal, and its removal is compatible with freedom of expression".[91] This interpretation is fur-

78 Ibid paras 195, 222.

79 'How Content ID Works' (*YouTube Help*) <https://support.google.com/youtube/answer/2797370?hl=en-GB> accessed 23 June 2021.

80 Ibid 94, 102.

81 *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

82 ibid.

83 *Scarlet Extended v SABAM* (n 14) para 52; *SABAM v Netlog NV* (n 15) para 50.

84 *UPC Telekabel Wien GmbH v Constantin Film* (n 41) paras 55, 56.

85 Ibid 57.

86 *Eva Glawischnig-Piesczek v Facebook*, Opinion of AG Spunzar (n 44), para 65.

87 Ibid 73-75.

88 *Eva Glawischnig-Piesczek v Facebook* (n 24) para 46.

89 Case C-18/18, *Eva Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821, Opinion of AG Spunzar, para 61.

90 *Peterson/Elsevier v Youtube/Cyando,* Opinion of the AG Saugmandsgaard ØE (n 48) para 189,243, 244.

91 *Peterson/Elsevier v Youtube/Cyando* (n 28) para 116.

ther confirmed by CJEU in the Poland v Parliament and Council case. Before applying the fair balance test, the court acknowledged that the use of automatic recognition and filtering tools, such as digital fingerprinting technology, become the only means to comply with monitoring obligation targeting to prevent occurrence of pre-identified infringements for certain online intermediaries hosting a large amount of content being uploaded on daily basis.[92] Furthermore, the court has confirmed that this monitoring and filtering method, by default, restricts an important means of disseminating online content and thus constitutes a limitation on the right to exercise freedom of expression and information of the users of those online intermediaries.[93]

27 Recognising the limitation on this fundamental freedom by monitoring obligations, the CJEU carried out a balancing test between the freedom of expression and information of internet users and the right to intellectual property of the rights holders. Accordingly, in addition to the provision of sufficient information to service providers as determined in the YouTube/Cyando judgement, the CJEU stated that two of the following preconditions must also be satisfied: i) the users of those service providers must be informed about prohibited contents as well as the functioning of automatic recognition and filtering systems in place, and ii) there must be an effective and expeditious complaint and redress mechanisms for users whose content was wrongly disabled or has been wrongly removed, and any complaint must be processed without undue delay and subject to human review.[94]

28 The ECtHR, has also consistently recognised the crucial role of online intermediaries for the internet users' freedom of expression as a provider of an unprecedented platform for "the free exchange of information and ideas".[95] In fact, in *Yildirim v Turkey* which involved the incidental shutting down of Google and third-party websites as a result of an interim Turkish court order targeting a website that was the subject of domestic criminal proceedings, the ECtHR, found a violation of freedom of expression and information by recognising that the internet has become one of the principal means by which individuals exercise not only their right to express their ideas but also their rights to receive information.[96] Like the CJEU's position, the ECtHR also acknowledged that compelling intermediaries to find and remove all illegal content online that is often legally disputed would force them to limit the ability to impart and receive information of ordinary Internet users and thus would have a chilling effect on their freedom of expression.[97]

29 In the *Delfi v Estonia* case, the ECtHR ruled that the imposition of the monitoring obligation against an online intermediary to filter specific illegal content, i.e. hate speech and incitement to violence, would not violate freedom of expression and information so long as the targeted illegal content is clearly identifiable in such a degree that "the establishment of their unlawful nature did not require any linguistic or legal analysis since the remarks were ('....') manifestly unlawful.".[98] In the following year, the ECtHR noted that expecting online intermediaries to take measures against unlawful online amounts to "requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the internet" in *MTE and Index v Hungary* case.[99] Although the ECtHR assessed the impact on the intermediary's freedom instead of its users in the Delfi case, the MTE and Index v Hungary case and following cases showed that the same consideration is also applied for the balancing test with internet user's freedom of expression.[100] Perhaps, this position can be reconciled with the CJEU's concern over the *independent legal assessment* of content by providers. It seems that both European courts accepted the fact that without providing well defined illegal content, intermediaries would start systematically removing offensive, criticising, or even injurious but still lawful expression in order to avoid liability.

30 Additionally, the ECtHR also assessed the potential impact of illegal content as another parameter that

92 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 54.

93 ibid 55.

94 ibid 88, 94.

95 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* [2016] ECtHR 22947/13) [61]; *Payam TAMIZ v the United Kingdom* [2017] ECtHR 3877/14 [87]; *Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10; *Vladimir Kharitonov v Russia* [2020] ECtHR 10795/14; *Jezior v Pologne* [2020] ECtHR 31955/11.

96 *Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10.

97 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88) para 86; *Rolf Anders Daniel Phil v Sweden* [2017] ECtHR 74742/14 [35]; by analogy, *Kablis v Russia* [2019] ECtHR 48310/16, 59663/17; *Ahmet Yildirim v Turkey* [2012] ECtHR 3111/10.

98 *Delfi AS v Estonia* [2015] ECtHR 64569/09.

99 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88).

100 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88) paras 91; *Rolf Anders Daniel Phil v Sweden* (n 13), Para 31; *Payam TAMIZ v the United Kingdom* (n 74) paras 80-81.

needs to be considered for the justification by the national court for restricting the intermediary's and users' freedom of expression.[101] Therefore, in case of the imposition of monitoring obligation against manifestly unlawful content, the size and reach of that online intermediary must also be taken into account for the balancing exercise.[102] In *MTE and Index v Hungary* case, the ECtHR concluded that large online platforms which run on a commercial basis and as part of their business model, try to attract a large number of users engagement should have a higher level of duty and responsibility because any unlawful content published on such platform has significantly more detrimental effect than other content on amateur or non-commercial websites or blogs.[103] The Court again applied this criteria in *Phil v Sweden*, where defamatory content was also published on a blog run by a small non-profit association.

31 In *Tamiz v UK* where a defamatory content published on Blogger.com, an online blog-publishing platform run by Google and reaching a wide audience, the ECtHR further elaborated this criteria by separating hosting service providers that do not provide any online content and merely host internet user's posts or which are private persons running a website or blog as a hobby from other platforms which actively compete for users' interaction and attention through notifications, invitations or other stimulus online and thus should bear more responsibility for user's illegal content.[104] Similarly, in the *Høiness v Norway* case that arose from a defamatory content published on a debate forum—a part of a news portal running on a commercial basis and which produces content to attract user interaction—the ECtHR again held that expecting a reactive approach from online intermediary against defamatory content, instead of proactive one such as upload filters, is proportionate limitation on freedom of expression and information.[105] Lastly, *Jezior v. Poland*, where the court applied this criteria to a defamatory content published on a privately run blog with a limited local scope and where an online intermediary which was notified of such content failed to prevent the reoccurrence, reaffirms that imposing the liability of internet user's manifestly unlawful content to an online intermediary which runs on non-commercial basis constitutes an unjustified limitation on the right to exercise of freedom of expression and information online.[106]

32 Perhaps, this soft approach on online intermediary regarding defamatory content is related to the contradictory and subjective nature of defamation cases, identification of which requires legal assessment by national courts in accordance with the national legislation.[107] Although, this issue was not explicitly discussed by the CJEU within the above-mentioned case-law, given the binding effects of the ECtHR's rulings[108], the article considers the potential reach of negative impacts of illegal content for the determination of the permissible scope of online monitoring.

33 One of the last criteria of ECtHR's fair balance exercise between freedom of expression and information of internet users and others' rights and freedoms is the availability of sufficient safeguards against the risk of over-blocking of lawful content. Although, the website blocking measures applied by a regulatory authority are discussed in both *Ahmet Yildirim v Turkey* and *Vladimir Kharitonov v Russia* cases as a prior restraint without being ordered by a court, the ECtHR noted that legitimate online blocking measure is likely to result in over-blocking and therefore requires an adequate safeguard.[109] It should be noted that the requirement of appropriate safeguard to be put in place against blocking measures is also adopted by the CJEU in Poland v Parliament and Council when defining lawful monitoring practices.[110]

34 In light of this, one can conclude that monitoring obligations that do not require legal assessment of online intermediaries for the identification of manifestly illegal content, supported by an effective redress mechanism for users whose content will be subject to such monitoring and imposed only for those intermediaries whose service reach might enable illegal content cause extensive damage do not

101 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88); *Rolf Anders Daniel Phil v Sweden* (n 89); *Payam TAMIZ v the United Kingdom* (n 88).

102 Giancarlo Frosio and Sunimal Mendis, 'Monitoring and Filtering: European Reform or Global Trend?' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) <http://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138> accessed 10 August 2021.

103 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* (n 88).

104 *Payam TAMIZ v the United Kingdom* (n 88) para 85.

105 *Høiness v Norway* [2019] ECtHR 43624/14.

106 *Jezior v. Pologne* (n 88).

107 *Axel Springer AG v Germany* [2012] ECtHR 55, 6.

108 For explanation, please see fn 66.

109 *Ahmet Yildirim v. Turkey* (n 88); *Vladimir Kharitonov v. Russia* (n 88).

110 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 94.

violate the freedom of expression and information of both internet users and online intermediaries.

c) Internet Users' Rights to Privacy and Protect Personal Data

35 Finally, blanket filtering and monitoring obligations have a serious impact on the internet user's right to protection of personal data.[111] When the CJEU was drawing the permissible scope of filtering in the L'Oréal case, it warned that in order to protect privacy and personal data of ordinary users, any identification measures should be taken against those internet users operating in the course of trade and not in a private matter.[112] Likewise, in the *SABAM v Netlog* case, the CJEU noted that the installation of a filtering system which indiscriminately monitors all information would *de facto* require the identification, systematic analysis, and processing of all the data relating to all of the service users and their profiles. Therefore, it was found that such filtering would infringe Article 8 of the Charter.[113]

36 However, under the recent Poland, YouTube/Cyando and Glawischnig cases, neither AGs nor the CJEU conducted any balancing test for this specific fundamental right even if both cases discussed injunctions requiring online intermediaries to monitor all information of all users. In fact, none of the parties to these cases have briefed the courts about privacy and data protection concerns. Perhaps, such claims would be a weak defence for YouTube and Facebook who have been dealing with privacy and data protection claims and investigations for their use of users' personal data for targeting practices.[114] However, given that both cases were preliminary rulings for the interpretation of EU law, i.e. Articles 14 and 15 of the ECD, the CJEU would be expected to consider such interpretations in light of fundamental rights and freedoms safeguarded under the Charter.[115] Therefore, it can be argued that the CJEU may accept the processing of users' personal data for filtering measures as legitimate given that all these major hosting providers have already adopted EU data protection standards into their data processing activities within their services. Perhaps, it should be discussed to what extend any automated proactive measure would comply with the requirement of GDPR[116] since some scholars have already raised their concerns over the potential violation of the automated decision-making requirements under Article 22 of the GDPR due to the opaqueness of the algorithms.[117] Due to its limited scope, this article assumes that these concerns can be balanced with the need to prevent online abuses and further, the implementation of automated filtering measures by online intermediaries will be supported by granting users the right to obtain human intervention as required by Article 22 of the GDPR.

2. Problem with Balancing in the Interpretation of General Monitoring

37 Before moving to the conclusion, it is important to point out the underlying problem with the balancing exercise of the CJEU and the ECtHR: interpreting the scope of general monitoring that compromises the very essence of freedom of expression and information and right to privacy of internet users. Although balancing is used by European courts as one of the standard ways through which to determine the outcome of a case where two fundamental rights conflict with each other, weighing two individual-centric, higher rights in a hypothetical scale as a way of human or fundamental rights adjudication has been

111 Keller (n 52); C Angelopoulos and others, 'Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation' (IViR 2015) <https://dare.uva.nl/search?identifier=7317bf21-e50c-4fea-b882-3d819e0da93a> accessed 6 August 2021.

112 *L'Oréal SA and Others v eBay International AG and Others* (n 10) para 142.

113 *SABAM v Netlog NV* (n 15) paras 48 and 49; The CJEU determined that the collection of IP addresses of internet users by internet access provider would impair user's right to protect personal data, *Scarlet Extended v SABAM* (n 14) para 51.

114 Keller (n 52).

115 *Scarlet Extended v SABAM* (n 14) para 39; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB and Watson and Others* [2016] ECLI:EU:C:2016:970 para 91 et seq.

116 Regulation (EU) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

117 Christoph Schmon, 'Copyright Filters Are On a Collision Course With EU Data Privacy Rules' (*Electronic Frontier Foundation*, 3 March 2020) <https://www.eff.org/deeplinks/2020/02/upload-filters-are-odds-gdpr> accessed 23 August 2021; Sophie Stalla-Bourdillon, 'Data Protection and Copyright: Could Art. 29 WP Guidance on Automated Decision-Making "Help" with Filters?' (*Peep Beep!*, 30 October 2017) <https://peepbeep.wordpress.com/2017/10/30/data-protection-law-and-copyright-could-art-29-wp-guidance-on-automated-decision-making-help-with-filters/> accessed 23 August 2021; Reda, Selinger and Servatius (n 38).

criticised.[118]Accordingly, the main criticism is that while qualified fundamental rights, such as the right to property, freedom of expression, the right to privacy, precisely aim to act as a barrier for individuals against state interferences which is often supported by or based on majority's view in a democratic society, the identification of interests, assigning commensurable values to those interests on the case by case basis and ultimately to "deciding which interest yields the net benefit" under the test of *balancing* contradicts with the core rationale of the fundamental right concept and consequently constrain themselves to a test of utilitarianism.[119]

38 Furthermore, the necessity test stipulated under Article 52 of the Charter and under Articles 8 and 11 of the Convention allowing limitations on the exercise of the fundamental freedom and rights only if it is necessary in a democratic society in accordance with the principle of proportionality which requires the intensity of the limitation not to be excessive in relation to the protection of the rights and freedoms of others is also accepted as a type of balancing exercise. Because it naturally leads to balancing of interests arising from these competing fundamental rights.[120] Eventually, due to the balancing approach, the courts might no longer seek to determine what is right or wrong in the dispute but, instead, try to investigate which fundamental right yielding net interest for the society concerned in relation to values and priorities upheld at the time. In other words, the balancing approach erodes the very essence and distinctive meaning of fundamental rights by "transforming them into something seemingly quantifiable".[121]

39 Through exploring the CJEU and ECtHR case law, Part 1 presents how general monitoring obligations lead to the clash between two opposing sides: in one corner freedom of expression, the right to privacy and protection of personal data, and the freedom to conduct a business while in the other, the right to privacy in a defamation context and right to property sit. Regarding the methodology, the two courts followed a very similar balancing method. They assess the alleged interference, whether it is provided by law, the existence of a legitimate aim or public interest objective, and, finally, examine necessity. In order to determine what is necessary, both the courts reduce conflicts between two fundamental rights, e.g., freedom of expression and the right to privacy or the right to property to utilitarian comparisons of relative weights or interests on the case by case basis and thus ignores the justification-protective function of rights.[122] Particularly, the defamation cases, such as Delfi, Tamiz, Phil and Glawischnig, show that it is up to the courts to decide what the context-specific interests of freedom of expression and right to privacy are, and consequently what are the limits of these fundamental rights in each case. Depending on the nature of the defamatory content and the size or reach of the online intermediary, the limitations on the exercise of right to receive information changes. Similar problems can be observed in the CJEU rulings in the Youtube/Cyando and Poland v Parliament/Council cases. In both cases, proportionality of the monitoring obligation is assessed based on, among others, the provision of *sufficiently substantiated* information regarding the infringement to the online intermediary.[123] However, the vagueness of sufficient information again led to the arbitrary scope of restrictions. Unfortunately, these cannot be coherent with human rights because the deep values and considerations of these rights are seen as fundamental to human life and therefore, they provide minimum rules and obligations regardless of the context they arise or of their status in the community.[124]

40 Moreover, even if the balancing exercise is justified, almost all the recent rulings seem to overlook the interests or weights of right to privacy and protection of personal data of internet users on this hypnotical scale. Permanent blanket monitoring of all online content and the possibility of false positive results of automated filtering systems, which is subject to the review of moderators who are not targeted by the content generator at the first place is indeed limiting on the right to privacy.

118 Jürgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (William Rehg tr, MIT Press 1996); Basak Cali, 'Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions' (2 January 2007) <https://papers.ssrn.com/abstract=2406348> accessed 6 July 2022; Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?' (2009) 7 International Journal of Constitutional Law 468.

119 Cali (n 118); B van der Sloot, 'The Practical and Theoretical Problems with "Balancing": Delfi , Coty and the Redundancy of the Human Rights Framework' (2016) 23 Maastricht Journal of European and Comparative Law <https://dare.uva.nl/search?identifier=eb7afd99-1e35-4000-a0f4-ece8178e0ab3> accessed 6 July 2022.

120 Tsakyrakis (n 118); Olivier De Schutter and Françoise Tulkens, 'The European Court of Human Rights as a Pragmatic Institution' (6 June 2014) <https://papers.ssrn.com/abstract=2446909> accessed 6 July 2022.

121 Tsakyrakis (n 118).

122 ibid.

123 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 91.

124 Cali (n 118).

IV. Interim Conclusion

41 This article shows that, at the beginning of the last decade, the CJEU adopted a broad interpretation of the concept of *general monitoring*. Accordingly, the imposition of any obligation requiring an online intermediary to monitor all information of all service users to filter infringements falls within the scope of the prohibition as it constitutes an excessive burden on the fundamental rights of online intermediaries as well as of internet users.[125] However, in the recent cases, the CJEU has recognised the difficulties for the targeting specific infringement from particular users due to fast-paced information flow of the internet realm, and acknowledged the fact that any preventive measure against illegal content cannot be effective without prior monitoring of all information flowing through the service.[126]

42 Perhaps, this shift from banning monitoring of all information to allowing the same practices for specific infringements can be explained by assessing the validity of the reasons behind the adaptation of the prohibition on the general monitoring obligation in the ECD at the beginning of this millennium.[127] Given the advancement in technology and the rapid economic growth of online intermediaries in recent years, the reasons for the lack of technical capacity and the desire not to deter a developing industry seem to have lost their validity in the eyes of the CJEU. Furthermore, the risk of creating actual knowledge and awareness by monitoring all the content including illegal but not notified ones has also been refused by the CJEU in the YouTube/Cyando case.[128] On the other hand, the risk of over-blocking and the unfairness of imposing obligation upon those mere intermediaries seem to be only valid reasons behind the CJEU's interpretation of Article 15(1) of the ECD. In relation to these concerns, both the European Courts seem to limit the scope of proactive measures against manifestly illegal content that would not require the online intermediary to conduct any legal assessment and only allow its imposition on financially and technically resourceful intermediaries that have influence over the curation of content instead of merely hosting them.[129] Lastly, in any circumstance, intermediaries must implement effective redress mechanisms and safeguards for legitimate personal data processing for internet users.[130]

43 Overall, as per the CJEU's case-law, the permissible monitoring obligations must: (i) be targeted to online content[131] which has been previously identified as illegal by a court[132] or which is manifestly illegal for a reasonable person[133], (ii) not require an additional independent legal assessment to identify,[134] (iii) be effective[135], reasonable[136] and propriate in accordance with the technical, operational and financial capabilities of the intermediary,[137] and with the impact of illegal content[138], for instance anyone of the GAFAM platforms[139], (iv) be carried out on the legitimate basis for the processing of personal data[140], and (v) be supplemented with an appropriate redress mechanism granted to internet users[141].

125 *L'Oréal SA and Others v eBay International AG and Others* (n 17); *Scarlet Extended v SABAM* (n 21); *SABAM v Netlog NV* (n 22); *McFadden v Sony Music* (n 28).; For the explanation of the related judgements, please see Section C, p 18 et seq.

126 *Eva Glawischnig-Piesczek* (n 24) 36; *Peterson/Elsevier v Youtube/Cyando*, Opinion of the AG Saugmandsgaard ØE (55) 221; *Peterson/Elsevier v Youtube/Cyando* (33); Republic of Poland v. European Parliament and Council of the European Union (n 56).

127 For the detailed explanation, please see Chapter B, Section II, p 5 et seq.

128 *Peterson/Elsevier v Youtube/Cyando* (33), para 109.

129 Reda, Selinger and Servatius (n 38).

130 *Republic of Poland v. European Parliament and Council of the European Union* (n 56) para 94.

131 *Delfi AS v. Estonia* (n 79); *Eva Glawischnig-Piesczek* (n 24); *Peterson/Elsevier v Youtube/Cyando* (33).

132 Reda, Selinger and Servatius (n 38); Frosio and Mendis (n 94).

133 Opinion of the AG Saugmandsgaard ØE in case C-401/19 (n 60).

134 Peterson/Elsevier v Youtube/Cyando (33); *Eva Glawischnig-Piesczek* (n 24).

135 *L'Oréal SA and Others v eBay International AG and Others* (n 17) para 136,141; *Eva Glawischnig-Piesczek* (n 24) para 46; *UPC Telekabel Wien GmbH v Constantin Film* (n 41) para 64

136 *L'Oréal SA and Others v eBay International AG and Others* (n 17) para 141,144; *UPC Telekabel Wien GmbH v Constantin Film* (n 41) paras 53,59.

137 *L'Oréal SA and Others v eBay International AG and Others* (n 17) para 141; *UPC Telekabel Wien GmbH v Constantin Film* (n 41), *Peterson/Elsevier v Youtube/Cyando*, Opinion of AG Saugmandsgaard ØE (42).

138 Delfi AS v Estonia 113, 115, 117, 128 and 145.

139 GAFAM is a common abbreviation used to refer to big tech giants, Google, Amazon, Facebook, Apple and Microsoft.

140 *SABAM v Netlog NV* (n 62); *Scarlet Extended v SABAM* (n 62).

141 *UPC Telekabel Wien GmbH v Constantin Film* (n 41)

44 It must be noted that Senftleben and Angelopoulos (2021) refused this general conclusion as they believe that the standards for the prohibition on general monitoring must be "specific in respect of both the protected subject matter and potential infringers".[142] First, they argued that the Glawischnig-Piesczek judgement is incompatible with the CJEU's rulings in the SABAM, McFadden, and L'Oréal cases because the infringements in intellectual property law depend not only on the specific use of work but also on the identity of the specific group of users.[143] Furthermore, Senftleben and Angelopoulos (2021) also pointed out that while it is often sufficient to identify the protected work that is fixed after the first publication in copyright issues, defamation cases, by contrast, depend on the nature of uploaded content and the use of specific defamatory elements in specific contexts.[144] Due to these substantial differences, the standards of general monitoring will be shaped based on "the nature and scope of the legal position, in respect of which the imposition of duties of care, including the introduction of content moderation duties, is requested".[145] While this is a plausible argument, considering the horizontal nature of the ECD, and both AG Saugmandsgaard-ØE's interpretation of manifestly illegal content in Poland v Parliament and Council case with the explicit reference to AG Spunzar's interpretation in Glawischnig-Piesczek case,[146] this article accepts the horizontal effect of the CJEU's interpretation of the scope of *specific monitoring* in line with Reda et al (2020), and Van Eecke (2011), and it argues that monitoring obligation for specific infringement is permissible regardless of the nature of infringement as long as the identification of illegal content can be carried out without any legal assessment of intermediaries and the effective redress mechanisms are implemented.[147]

C. Interplay Between the Prohibition on General Monitoring Obligation and the Evolving EU Legislations.

45 This chapter will analyse the role of general monitoring within the new online intermediary liability regime introduced under the new EU legislations by comparing the implementation of the prohibition with the CJEU's interpretation. The aim is to reveal the inconsistencies between these legislations and the CJEU's interpretation.

I. Audiovisual Media Services Directive

46 In 2018, the EU amended the AVMSD[148] to introduce new requirements for VSP provider, a recently defined subset of hosting service provider.[149] According to Article 28b, member states must ensure that VSP providers adopt "appropriate, practicable and proportionate" measures to protect minors from online content which may impair their physical, mental or moral development and the general public from the dissemination of content containing hate speech and incitement to violence, provocation to commit terrorist offence, child sexual abuse material and racism and xenophobia.[150] The AVMSD further provides a non-exhaustive list of measures that are deemed appropriate by EU legislators including, among others, the notice and take down systems based on user's reporting[151] but also allow Member States to impose more detailed and stricter measures

142 Christina Angelopoulos and Martin Senftleben, 'An Endless Odyssey? Content Moderation Without General Content Monitoring Obligations' (22 June 2021) <https://papers.ssrn.com/abstract=3871916> accessed 9 July 2022.

143 Martin Senftleben and Christina Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3717022 <https://papers.ssrn.com/abstract=3717022> accessed 21 May 2021."plainCitation":"Martin Senftleben and Christina Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (Social Science Research Network 2020

144 Angelopoulos and Senftleben (n 142).

145 ibid.

146 *Peterson/Elsevier v Youtube/Cyando*, Opinion of AG Saugmandsgaard ØE (42), para 221; Opinion of the AG Saugmandsgaard ØE in case C-401/19 (n 60) para 113.

147 Reda, Selinger and Servatius (n 38) 19,20; Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market Law Review 1487 <http://kluwerlawonline.com/journalarticle/Common+Market+Law+Review/48.5/COLA2011058> accessed 23 August 2021.

148 The AVMSD.

149 For detailed definition please see Chapter IV, Section A, Part i, p 31 et seq.

150 The AVMSD Article 28b(1),(2).

151 Ibid Art 28b(3).

on VSPs.[152] However, these measures shall not lead to ex-ante control measures or upload-filtering of content, which do not comply with Article 15 ECD.[153]

47 It becomes evident that the EU lawmakers consider the balance test requirement for the determination of appropriate, practicable and proportionate measures in line with the CJEU's case-law.[154] But, it is not clear as to what measures could be stricter than a notice and takedown procedure in the context of the available technology[155] but do not constitute ex-ante content moderation measures, which are clearly considered a violation of Article 15 of the ECD. Moreover, this prohibition of *ex-ante control measures* and *upload-filters* fails to reconcile the YouTube/Cynado, Glawishking and Poland v Parliament/Council rulings as well as the ECtHR's case-law, which allow the imposition of monitoring obligation to prevent *manifestly* illegal content.[156]

II. Regulation on Preventing Dissemination of Terrorist Content Online

48 The Regulation on Preventing Dissemination of Terrorist Content Online enacted in May 2021 imposes obligations on hosting service providers to remove terrorist content within an hour upon receipt of a notification from a competent authority.[157] Hosting service providers must take specific measures to protect their services from being misused for the dissemination of terrorist content if the competent authority finds the service is exposed to terrorist content on basis of certain factors, such as having received two or more removal orders from a competent authority within the past twelve (12) months. In line with the settled balancing test of the CJEU, the Regulation also grants freedom to hosting service providers on their choice of specific measures on condition that these measures must be effective in mitigating the risk, proportionate with the technical, financial, and operational capabilities, the number of users of the hosting service provider and the amount of content they provide.[158] The competent authorities also have power to require additional specific measures if they find the hosting service provider's measures are insufficient to address the risks.[159] Nevertheless, the imposition of any requirement leading a general obligation to monitor or actively seek facts or circumstances indicating illegal activity under Article 15(1) ECD or to use of automated tools by hosting providers are prohibited.[160]

49 Once again, the prohibition on general monitoring appears as the borderline for statutory specific measures. However, the whole system established under the Regulation including the obligation to remove notified terrorist content and to take specific measures for the protection of the service, seems to give no other option to hosting providers

152 Ibid Art 28b(6).

153 Ibid Art 28b(3),(6).

154 Commission Staff Working of 25 May 2016, Impact Assessment of AVMSD Proposal, SWD(2016) 168.

155 In the automated content moderation, two techniques are mainly adopted by VSPs, i.e. the matching and classification technique. In the matching, filtering system automatically review newly uploaded audio-visual content against a large table of existing fingerprints of previously removed harmful content which is generated based on either whole audio-visual file or specific elements or features of such content such as certain colours, corners in images, hertz-frequency of sound etc. For instance, YouTube's CSAI Match, Microsoft PhotoID and Facebook's PDQ and TMK+PDQF are examples of the filtering systems based on this technique systems and used for the detection of child sexual exploitation, terrorist propaganda, and graphic violence. The classification technique based on Machine Learning or Deep Neural Network solutions and are used for object detection, scene understanding, and semantic segmentation, or advanced video understanding. Object detection and semantic segmentation can identify certain objects such as weapons, faces, body parts, and text within images and their location within an image through processing regions of an image or video and associating it with predefined features of harmful content such as nudity, violence, hate speech etc. For more information, please see; Analisa Tamayo Keef and Lior Ben-Kereth, 'Introducing Rights Manager' (*Facebook for media*, 12 April 2016) <https://perma.cc/YB5H-BEM5> accessed 23 June 2021; Tony Wang, 'Recognizing Firearms from Images and Videos in Real-Time with Deep Learning and Computer Vision' [2019] *Medium* <https://medium.com/@tont/recognizing-firearms-from-images-and-videos-in-real-time-with-deep-learning-and-computer-vision-661498f45278> accessed 23 June 2021; 'Use of AI in Online Content Moderation' (Cambrige Consultants 2019) <https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/online-content-moderation>; Gorwa, Binns and Katzenbach (n 65).

156 For legal analysis of these case-laws, please see Chapter II, Section B, C, p 9 et seq.

157 As per Article 12 of the Regulation on Preventing Dissemination of Terrorist Content Online, competent authorities will be designated by each member states.

158 Ibid Art5(1), Recital 22.

159 Ibid Art 6.

160 Ibid Art 8.

but to take certain proactive measures in practice. First, as the obligation to take specific measures is triggered by the receipt of more than two removal orders, without any preventive measures, the previously removed terrorist content can be easily re-uploaded and cause the competent authorities to issue additional third removal order which eventually trigger the requirement to take so-called specific measures. Moreover, Article 5(2)(a) classifies "appropriate technical and operational measures or capacities, such as appropriate staffing or technical means to identify and expeditiously remove or disable access to terrorist content" as a permissible specific measure which clearly requires *de facto* monitoring of uploaded content in order to identify terrorist content. Given that Article 7(3)(b) also requires providers to publish information about measures taken to address the *reappearance* of previously removed content annually, it becomes apparent that hosting providers are expected to take preventive measure at some degree, for instance against the pre-identified terrorist content.[161]

50 To a certain extent, the suspension of users or accounts that are identified as terrorist content uploader can be considered a preventive measure. However, the privacy concerns over the loss of online anonymity[162] and the availability of technologies that provide anonymity[163] would hamper the effectiveness of these suspensions. Therefore, considering the requirement for specific measures to be *effective, appropriate and proportionate* in accordance with a hosting provider's size, technical and economic capacity, and the number of its users,[164] it becomes evident that major hosting service providers enabling access to user content in large scales do not have any other option to effectively mitigate the dissemination of terrorist content but to implement the filtering measure for pre-identified terrorist content. Indeed, this understanding would comply not only with both the EU legislators' recent statements concerning the proactive measures against manifestly illegal content[165] but also with the CJEU's interpretation of Article 15(1) ECD.[166] In fact, all necessary safeguards for fundamental rights stipulated by the CJEU have already been considered under the Terrorist Content Regulation such as the proportionality test, human oversight, and verification in the use of automated tools against over-blocking and the introduction of complaint and redress mechanisms.[167] However, if the CJEU's interpretation is accepted and the hosting providers can be forced to take *technical and operational measures* to identify and expeditiously remove pre-identified terrorist content under Article 5(2)(a), this Regulation would be incompatible with the prohibition of ex-ante control measures as provided for under the AVMSD.

III. The Directive on Copyright in the Digital Single Market

51 The obligations stipulated under Article 17(4) of the Copyright Directive were the subject of one of the most influential CJEU rulings, Poland v Parliament/Council. According to Article 17(4), online content-sharing service providers ("OCSSP")[168] which have not obtained an authorization from the rightholders must demonstrate that they have: (i) made best efforts to ensure the unavailability of specific copyright-protected works for which the relevant rightholders must have provided the OCSSP with the relevant and necessary information and (ii) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to remove the content infringing the notified works and made best offers to prevent their future uploads.[169] The assessment of "best efforts" is made in accordance with "high industry standards of professional diligence" and the principle of proportionality with regard to the number of elements such as the type,

161 Aleksandra Kuczerawy, 'Proposed Regulation on Preventing the Dissemination of Terrorist Content Online' (For Center for Democracy and Technology 2018) <https://cdt.org/insights/research-paper-from-leuven-university-proposed-regulation-on-preventing-the-dissemination-of-terrorist-content-online/> accessed 17 August 2021.

162 Rachel Melis, 'Anonymity Versus Privacy in a Control Society' (2019) 2 Journal of Critical Library and Information Studies <https://journals.litwinbooks.com/index.php/jclis/article/view/75> accessed 17 August 2021.

163 Thais Sardá and others, 'Understanding Online Anonymity' (2019) 41 Media, Culture & Society 557.

164 Regulation on Preventing Dissemination of Terrorist Content Online, Recital 24.

165 European Parliament, 'Resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed (2020) 0274, para 27; Commission, Recommendation on measures to effectively tackle illegal content online.

166 Please see Chapter II, Section D 'Interim Conclusion', p 22 et seq.

167 Terrorist Content Regulation Art 5, 10.

168 The Directive on Copyright in the Digital Single Market, Article 2(6) defines online content-sharing service provider as "*a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes*".

169 Ibid Art 17(4).

the audience and the size of the service, the evolving state of the art to avoid the availability of different types of content and the cost of such means for the services.[170] In fact, Article 17(6) exempts new OCSSPs from the "best effort" requirement that have been active in the EU for less than 3 years, have less than 5 million monthly unique visitors and have an annual turnover of less than 10 million euros. Lastly, Article 17(8) explicitly states that the application of best effort requirements under Article 17 shall not lead to any general monitoring obligation.[171]

52 The EC's Guidance on Article 17 recognises the content recognition technologies as a method "commonly used today to manage the use of copyright protected content, at least by the major online content-sharing service providers and as regards certain types of content" and note that these technologies can be considered as the market standards to filter and block *manifestly infringing* content for large OSSPs.[172] In the Poland v Parliament/Council case, the CJEU confirmed this position by explicitly announcing that the requirement for use of automated recognition and filtering technologies under the best effort obligations, do not amount to general monitoring obligations that could hamper the providers.[173] Basically, both the EC and CJEU agreed that upload filters can be compatible with the prohibition as long as the scope of filtering measures is limited to specific infringement identified by courts or rightholders and which is specific enough to be detected by automated tools.[174] In addition, they noted that certain safeguards must be implemented for fundamental rights in particularly freedom of expression and right to remedy.[175]

170 Ibid Art 17(5), Recital 65.

171 Ibid Art 17(8).

172 Commission 'Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market' COM (2021) 288 Final, ('Guidance on Article 17') pages 12,22.

173 *Republic of Poland v. European Parliament and Council of the European Union* (n 56).

174 Guidance on Article 17, p 16; Case C-401/19, *Republic of Poland v European Parliament and Council of the European Union* [2019], Opinion of AG Saugmandsgaard ØE paras 200-201.

175 Guidance on Article 17, p. 22; The Directive on Copyright in the Digital Single Market Article 17(9), Recital 70; *Republic of Poland v European Parliament and Council of the European Union* [2019], Opinion of AG Saugmandsgaard ØE 98 et seq.

D. The Implementation of General Monitoring Prohibition on Video-Sharing Platforms

53 This last chapter elaborates how this discrepancy concerning the notion of general monitoring under the EU legislations will affect VSPs in practice. However, in order to conduct such legal analysis, first an explanation needs to be made of why VSPs fall within the scope of these legislations.

I. Understanding Video-Sharing Platforms

1. Definition

54 VSP services are defined under Article 1(aa) of the AVMSD. Accordingly, any information society service satisfying the following three conditions is VSP service: (i) the principal purpose of the service or of a dissociable section thereof, or an essential functionality of the service is devoted to providing programmes, user-generated videos ("UGV"), created and uploaded by a service user, or both, to the general public, for which the service provider does not have editorial responsibility, in order to inform, entertain or educate; (ii) the service is made available by means of electronic communication networks and (iii) the organisation of these content is determined by the provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing.[176]

55 The assessment of whether video-sharing is "principal purpose" of the service or "dissociable section" thereof simply refers to hosting service providers that do not have any features or services other than video sharing, or the home page of which is devoted to shared videos or have a section listed in the navigation of a website or accessible from a link or icon on an app home screen that provides video-sharing or upload.[177] Considering these parameters, YouTube, TikTok, and all adult VSPs become VSP providers due to principal purpose of services, while

176 The AVMSD, Art 1(aa).

177 Yi Shen Chan, Sam Wood and Stephen Adshead, 'Understanding Video-Sharing Platforms Under UK Jurisdiction' (Plum Consulting 2019) <https://plumconsulting.co.uk/understanding-video-sharing-platforms-under-uk-jurisdiction/> accessed 21 May 2021.; EU Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service' under the Audiovisual Media Services Directive (n 138).

Vimeo[178], Instagram's IGTV[179] which is mainly and Facebook's Watch Section[180] can be identified as VSPs whose dissociable section of principal service is video sharing.

56 If this assessment cannot be made, then it should be assessed whether the provision of UGV or programmes is an "essential functionality" of the service of an online intermediary. As per Recital 5 of the Directive 2018/1808, a service could have the "essential functionality" of the provision of videos if "the audiovisual content is not merely ancillary to, or does not constitute a minor part of" the activities of that service.[181] For the essential functionality test, the EC has determined four main indicators under its Guidelines.[182] Although these guidelines are not legally binding, and do not provide uniformity of interpretation, because of their relevance, this article takes into account for the determination of the scope of the AVMSD.

57 As per the Guidelines, the essential functionality requires that audiovisual content has discretely core value on the main service. This should focus more on the architecture and operation method of the online intermediary to determine whether the video-sharing feature constitutes a stand-alone function on the service.[183] Secondly, the quantitative and qualitative relevance of audiovisual content for the service such as the amount, use and reach of audiovisual content needs to be reviewed collectively.[184] Third, whether the online platform gains revenue through its video-sharing features by example ads placement, pay-to-access system, or processing of users data for various marketing/ commercial purposes in exchange of views.[185] Lastly, whether the service promotes the user's engagement with shared video is assessed.[186] These indicators must be considered under an overall analysis of the service and the absence of one or more of them does not automatically exclude the service from being a VSP. The AVMSD applies to the intermediary if the results of a sufficient number of indicators support the conclusion that the provision of audiovisual content is not merely ancillary or a minor part of, the activities of that intermediary's service. In line with this conclusion, Snapchat[187], Reddit[188] and Twitter[189] can be identified as VSP providers as the video-sharing functionality of their platforms has become an essential function of their social networking services.[190]

58 The last important element is the absence of editorial responsibility. It separates VSPs providers from being "media service providers" who have legal obligation to comply with certain requirements in relation to commercial communication, audiovisual advertising, sponsorship and product placement under the AVMSD. According to Article 1(1)(c), editorial responsibility refers to the exercise of effective control over both the selection of the programmes and the organisation either in a chronological schedule or in a catalogue.[191] Given that the definition of VSP service acknowledges the organisational control over the content, the distinctive factor becomes

178 Vimeo's main service is pivoted into software provision for video production and storage and does not monetise video-sharing activities.

179 Instagram was first launched as photo-sharing social network, however in recent years, it embedded video-sharing function on its app and website. Although it's principle purpose of service might be considered as the provision of UGV to the general public, its initial photo-sharing function still constitutes as principle element of the service.

180 Chan, Wood and Adshead (n 164).

181 The AVMSD Recital 5.

182 Guidelines on the practical application of the essential functionality criterion of the definition of a 'video-sharing platform service', (n 156).

183 Ibid p 6.

184 Ibid p 7.

185 Ibid pp 7-8.

186 Ibid pp 8-9.

187 Tiffany Peón, 'A Guide to Snapchat for People Who Don't Get Snapchat' *The New York Times* (7 February 2018) <https://www.nytimes.com/2018/02/07/smarter-living/snapchat-guide.html> accessed 22 August 2021. While its principal purpose of the service is to provide a camera and messaging application, the video-sharing function has become more dominant in recent years.

188 Christian Stafford, 'What Is Reddit? - Definition from WhatIs.Com' <https://searchcio.techtarget.com/definition/Reddit> accessed 22 August 2021.

189 'How to Go Live on Twitter with Twitter Live Stream Feeds' <https://help.twitter.com/en/using-twitter/twitter-live> accessed 22 August 2021; 'How to Share and Watch Videos on Twitter' <https://help.twitter.com/en/using-twitter/twitter-videos> accessed 22 August 2021.

190 Joan Barata, 'Regulating Content Moderation in Europe beyond the AVMSD' (*Media@LSE*, 25 February 2020) <https://blogs.lse.ac.uk/medialse/2020/02/25/regulating-content-moderation-in-europe-beyond-the-avmsd/> accessed 15 June 2021.

191 AVSM Directive Art 1(c).

the ability to decide and select which content will be available on the service. Therefore, this sole power over the selection of the content distinguishes VSP providers from other audio-visual content providers such as publishers whose website includes videos regarding news or subscription-based video-on-demand services, or broadcasters providing content online on their website as well as online platforms.

2. Legal Framework

59 The previous commentary on the definition of VSP service under Article 1(aa) AVMSD reveals that nearly all of today's popular social networks fall within the scope of Article 28b of AVMSD.[192] Furthermore, the UGV hosted by VSPs are broadly defined as an individual set of moving images with or without sound created by an internet user and uploaded to a VSP by that user or any other user which could cover most of today's online content.[193] As VSPs host their user's information in form of, audiovisual content and transmit it to other users through electronic means, without actively selecting the content, they become a subset of hosting service providers under the ECD.[194] Therefore, as a result of being a hosting service provider, VSPs also fall within the scope of the Terrorist Content Regulation.[195]

60 Moreover, the OCSSP definition under Article 2(6) the Copyright Directive, with the emphasis on the function to store and give the public access to large amount of copyright-protected works which are organised by the OCSSP for profit-making purposes and the thresholds set forth by Article 17[196] are clearly designed to include major VSPs.[197] Overall, it can be concluded that the commercially large-scale VSPs are obliged to implement necessary measures against certain types of illegal content online in accordance with the AVMSD, the Terrorist Content and the Copyright Directive.

II. To What Extend the Prohibition of General Monitoring Should Be Applied on Video-Sharing Platforms under the EU Legislations.

61 It is evident that there is a lack of a uniform application of general monitoring prohibition within the EU intermediary liability regime. Whereas the AVMSD qualifies ex-ante control measures and upload-filters as prohibited general monitoring regardless of the nature of the content and the Terrorist Content Regulation prohibits obligation to use automated tools against terrorist content[198], the Copyright Directive, in line with the CJEU's interpretation, obliges VSPs to implement automated filtering measures against specific copyright infringements. In practice, these different approaches regarding content moderation measures might cause VSPs which host both video, image and textual content like Instagram or Twitter to face difficulties depending on whether manifestly illegal potential content is posted by video, or within a still image or as a written article.[199]

62 Firstly, while both the AVMSD and the Terrorist Content Regulation aim to tackle with the dissemination of the terrorist content, the required measures differ significantly under each legislation. According to AVMSD, VSPs cannot be forced to implement upload-filters, but on the other hand, the Terrorist Content Regulation expects them to prevent the recurrence of previously removed terrorist content. This

192 Barata (n 177); Francisco Javier Cabrera Blázquez and others, *The Legal Framework for Video-Sharing Platforms* (European Audiovisual Observatory 2018).

193 Ibid Art 1(b)(ba), Directive 2018/1808, Recital 6.

194 Jan Oster, *European and International Media Law* (Cambridge University Press 2016) <https://www.cambridge.org/core/books/european-and-international-media-law/11DB5E88696AE095F61FE885E190B762>.; The E-Commerce Directive Recital 18; Joined Cases C-682/18 and C-683/18, Peterson/Elsevier v Youtube/Cyando (n 54) para 117, the CJEU acknowledge that activities of VSP providers fall within the scope of Article 14 of the ECD.

195 The Terrorist Content Regulation, Article 1.

196 For the detailed explanation of these thresholds, please see Chapter III, Section C, p 29 et seq.

197 João Quintais, 'The New Copyright in the Digital Single Market Directive: A Critical Look' (2019) 2020 European Intellectual Property Review <https://papers.ssrn.com/abstract=3424770> accessed 23 August 2021; Karina Grisse, 'After the Storm—Examining the Final Version of Article 17 of the New Directive (EU) 2019/790' (2019) 14 Journal of Intellectual Property Law & Practice 887; Christophe Geiger and Bernd Justin Jütte, 'Towards a Virtuous Legal Framework for Content Moderation by Digital Platforms in the EU? The Commission's Guidance on Article 17 CDSM Directive in the Light of the YouTube/Cyando Judgement and the AG's Opinion in C-401/19' <https://papers.ssrn.com/abstract=3889049> accessed 10 August 2021.

198 This is the result of the interpretation made under this paper, please see Chapter III, Section B, p 26 et seq.

199 This was the issue in the Case C-18/18, Eva Glawischnig-Piesczek v Facebook (n 48).

means VSPs cannot be required to take measures to "identify and expeditiously remove" pre-identified terrorist content under Article 5(2)(a) the Terrorist Content Regulation, as it contradicts with the AVMSD. However, without implementing ex-ante monitoring to tackle previously removed terrorist content and by solely relying on reactive measures, there will be a loop of constant uploads and one-hour removals of the same terrorist content.

63 If the prohibition of general monitoring under the Terrorist Content Regulation is read in compliance with the AVMSD, then the specific measure under Article 5 would not go beyond being the supplementary list to the non-exhaustive list of appropriate measures under Article 28b of the AVMSD. Furthermore, there is nothing to stop national courts from issuing an injunction on VSPs to prevent pre-identified terrorist content on its service. This will eventually lead to VPSs with thousands of daily uploads to implement an automated filtering system to comply with such injunction even if it cannot be required under the Terrorist Content Regulation. Given that the CJEU identified automated recognition and filtering tools as an effective measure against dissemination of illegal content in the Poland v Parliament/Council judgement, the prohibition on requirement for the use of automated tools under the Terrorist Content Regulation perhaps becomes an empty shell in practice at least for large service providers as they do not have any other option but to implement automated systems other than employing thousands of human moderators.

64 Secondly, there is an imbalance between rights and interests under the current legislative framework. The interests at stake for the prevention of reappearance of content containing non-consensual sexual videos, child sexual abuse, provocation to commit a terrorist or extremist offence which are pre-identified by judicial authorities as illegal are considerably higher than the interest of copyright holders protected under Article 17 of the Copyright Directive.[200] In fact, today, the automatic duplicate-detection systems are the most commonly deployed systems to filter out duplicates of known, specific terrorist or child exploitation images, audio, or videos in practice, and they even provide more successful results then human moderators.[201] On the other hand, despite the recent developments in the content recognition technologies, empirical studies show that these systems still perform poorly for the detection of infringements that contain the same, previously notified copyright-protected work.[202] Considering the balance test conducted by both European Courts, it is evident that the monitoring obligations against these manifestly illegal content would constitute a more proportionate limitation on the exercise of the freedom of expression and VPS's freedom to conduct a business. Therefore, the AVMSD's interpretation of general monitoring which covers upload-filters against child sexual abuse and provocation to terrorism and extremism seriously hamper the EU's aim to create a safe digital single market.[203]

65 On the other hand, this article does not disregard the concerns over the risk of excessive restriction of fundamental rights posed by any monitoring obligation requiring an independent assessment of VPSs or national administrative authorities. In addition to risks explained under the case-law review above, as per Balkin (2014), by imposing general monitoring obligation, governments can acquire the power to impose "collateral censorship" on free speech online through the hands of the VSPs.[204] Moreover, it is evident that monitoring of all user information to detect not only manifestly illegal but also other types of illegal content, which require legal assessment, would preclude individuals from sharing and discussing their ideas online and eventually harm their intellectual privacy.[205]

200 Giancarlo Frosio and Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2020) Forthcoming European Law Journal <https://papers.ssrn.com/abstract=3747756> accessed 1 August 2021.

201 Olivia Solon, 'Facebook, Twitter, Google and Microsoft Team up to Tackle Extremist Content' *the Guardian* (6 December 2016) <http://www.theguardian.com/technology/2016/dec/05/facebook-twitter-google-microsoft-terrorist-extremist-content> accessed 16 August 2021; Tracy Jan and Elizabeth Dwoskin, 'A White Man Called Her Kids the N-Word. Facebook Stopped Her from Sharing It.' *Washington Post* (31 July 2017) <https://www.washingtonpost.com/business/economy/for-facebook-erasing-hate-speech-proves-a-daunting-challenge/2017/07/31/922d9bc6-6e3b-11e7-9c15-177740635e83_story.html> accessed 16 August 2021. For further information on automated filtering systems which are currently deployed by VSPs, please see fn 128.

202 Joanne E Gray and Nicolas P Suzor, 'Playing with Machines: Using Machine Learning to Understand Automated Copyright Enforcement at Scale' (2020) 7 Big Data & Society 2053951720919963; Daniel Seng, 'Copyrighting Copywrongs: An Empirical Analysis of Errors with Automated Dmca Takedown Notices' (2021) 37 Santa Clara High Technology Law Journal 119.

203 Montagnani (n 7); Ullrich (n 8).

204 Jack M Balkin, 'OLD-SCHOOL/NEW-SCHOOL SPEECH REGULATION' (2014) 127 Harvard Law Review 2296, 2311.

205 Neil Richards, 'A Theory of Intellectual Privacy', *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age* (Oxford Uni-

Unfortunately, it seems like these considerations are overlooked under the balancing exercise of the European human rights adjudicators. Whereas the monitoring obligation should be accepted as a direct interference with the freedom of expression, the right to privacy of internet users and the proportionality test as per Article 52 of the Charter needs to be applied in this context, we have witnessed mere utilitarian comparison of fundamental rights without considering principled hierarchy of interests. As rightly pointed out by van der Sloot (1998), the case law review under Chapter B, Section III of this paper presents minor interests, "such as not being called a rascal or the copyright protection of a commercial business," are promoted to fundamental rights discourse under the balancing exercise.[206] The special protection to certain principles and interests which are deemed essential not only to human life but also to modern day democratic societies, such as the right to receive and impart information on VSPs seems to be forgotten in the interpretation of general monitoring obligations by both the CJEU and the EU legislators.

66 Lastly, imposing specific monitoring obligations against defamatory content might be very problematic in practice. While the copyrighted works can be detected by automatic recognition tools regardless of the format of content, such as video, text, audio, automatic recognition of defamatory content may not always be easily done. For instance, if the defamatory content in Glawischnig-Piesczek case would have been re-uploaded as a video to Facebook where a random person reads the text of the original defamatory content in a different but commonly use language, would this video still qualify as *equivalent content* to original as the message remains essentially unaltered? Or what if this video does not include any audio but just shows series of cardboards where the original messages are written? Or should we expect VSPs to prevent occurrence of such video if it was a part of reporting activities of an amateur journalist?

67 In light of these considerations, it becomes evident that one horizontally applicable prohibition not only creates legal uncertainty for VSPs but also fails to address interests of internet users in the online realm. Therefore, at the current situation, the evolving content/sector-specific EU legislations may include provisions which clearly distinguish the default prohibition on general monitoring obligations from the context-specific measures and which are tailored to address each specific type of illegality in a limited scope and under conditions that overwhelmingly safeguard the interest of individuals in exercising their freedom of expression and right to privacy.[207]

E. Conclusion

68 All in all, this article made three distinctive conclusions. First, by analysing the CJEU's case-law, it notes that the proactive monitoring and filtering obligations targeted to a specific kind of illegality are permitted for, at least, financially and technically resourceful online content hosting and sharing services as long as safeguards for the right to effective remedy and right to protection of personal data and privacy are guaranteed.[208] This exercise reveals that the main concerns behind the prohibition are the negative impacts arising from the imposition of obligation on online intermediaries to carry out an independent assessment of the nature of content and being liable of this assessment. This will cause an excessive burden on online intermediaries which are, to a certain extent, still considered as being passive players or *mere conduits* of content stored or transmitted through their services by third parties and result them to over-remove the legitimate user content. However, the CJEU's adaptation of balancing exercise is found overlooking the special protections for individual and communal interests in the right to privacy and freedom of expression and information in an online environment. Particularly, the possible chilling effect on internet users arising from ex-ante monitoring practices seem not to be assessed in detail by the CJEU.

69 Secondly, under the recent EU legislations, there is a legal uncertainty on which types of obligations to monitor online content in order to prevent the dissemination of illegal content, are prohibited. This is the result of the conflicting interpretations on the scope of the prohibited general monitoring by the EU legislators and the CJEU. Thirdly, it has been noted that the broad definition of VSPs leads almost all the major online intermediaries to legal uncertainty regarding their content moderation practices and thus turning the Article 15(1) of the ECD in an empty shell. As this causes a detrimental impact on the rule of law, this article acknowledges the need for a clear distinction for VSPs between vertically applicable measures arising content or sector specific regulations and the prohibition on blanket monitoring obligations.

70 As for the future, this article foresees the potential

versity Press, Incorporated 2015) <http://ebookcentral.proquest.com/lib/ed/detail.action?docID=1910138> accessed 12 April 2021.

206 van der Sloot (n 119).

207 Sartor and Loreggia (n 9).

208 Please see Chapter II, Section D, p 22 et seq.

violations of the fundamental European values by monitoring obligations and thus questions the need for *ex-ante monitoring* to prevent occurrence of illegal content or illegal activities online. The 21st century world is the dynamic convergence and symbiosis of both the physical and cyber worlds where almost every day digital and physical actions become more intertwined. As the line between real and digital is blurring day by day, perhaps, it is time to reevaluate our legal methodology to regulate this new world. Imposing *ex-ante* monitoring obligation on VSPs for all the information hosted on their services to prevent the occurrence of violations summons the dystopic future depicted in the movie *The Minority Report* in which the police use technology to catch criminals before a crime is committed.[209] As the law does not refuse people from thinking about copying copyrighted works for personal use or having libellous thoughts of another individual, this should also not be the duty for VSPs with respect to online activities of their users. Thus, it is up to us to find an alternative solution that can suppress the impact of online illegal activities without restricting the fundamental rights of individuals.

209 Steven Spielberg, *Minority Report* (Twentieth Century Fox, Dreamworks Pictures, Cruise/Wagner Productions 2002).

Great expectations: the Facebook case and subsequent legislative approaches to regulate large online platforms and digital markets

by **Karin Jackwerth***

Abstract: In recent years, the accumulation and entrenchment of power by a few large firms in the digital markets sector and the complementary decrease in the level of competition has become visible around the world. This could likely result in negative consequences for potential competitors, individuals and businesses that interact with these firms. In order to address this challenge, several jurisdictions have initiated the development of legislative tools to regulate these large firms. The first regulation of this type has been enforced by the German legislator and could therefore serve as a reference for other jurisdictions. In advance of practical experience, this paper will conduct a theoretical analysis of potential structural and data-related issues arising from this regulation. It will deduce that the regulation successfully addresses data-related concerns which have previously been confronted in the so-called Facebook case. The paper will also identify shortcomings in structural aspects, which will be confronted with a comparison to the UK approach for a similar regulatory tool. The results of the comparison will be summarised in a list of recommendations with the aims to improve the German regulation and to serve as guidance for similar approaches in other jurisdictions.

Keywords: Digital markets; competition law; data protection; Facebook case; Digital Markets Act; Germany; United Kingdom; EU

Recommended citation: Karin Jackwerth, Great expectations: the Facebook case and subsequent legislative approaches to regulate large online platforms and digital markets, 13 (2022) JIPITEC 200 para 1.

A. Introduction

1 In recent years, the accumulation and entrenchment of power by a few large firms in the digital markets sector and the complementary decrease in the level of competition has become visible around the world. Market dominance in itself is not unlawful,[1] but in the absence of significant competition, there is an increasing risk that the firms will abuse their power over businesses and individuals that interact with the digital markets. In addition, the entrenchment of this power is likely to create barriers for new entrants and to reduce the incentive for innovation and maintenance of quality by the large firms.[2] Furthermore, multi-sided platforms,[3] that offer access

* LL.B. English and German Law Graduate at University College London.

1 Jason Furman and others, 'Unlocking Digital Competition: Report of the Digital Competition Expert Panel' (13.03.2019), 6; Marija Stojanovic, 'Can Competition Law Protect Consumers in Cases of a Dominant Company Breach of Data Protection Rules?' (2020) 16 European Competition Journal 531, 532.

2 Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16 European Competition Journal 628, 658f; CMA, 'Online Platforms and Digital Advertising: Market Study Final Report' (B6-113/15, 01.07.2020) ("Market Study"), paras 6.5-6.14.

3 On Multi-sided platforms one party sets up relations to parties in different markets and enables interaction between those parties, in Mark-Oliver Mackenrodt and Klaus Wiedemann, 'Zur kartellrechtlichen Bewertung der Datenverarbeitung durch Facebook und ihrer normativen Kohärenz mit dem Datenschutzrecht und dem Datenschuldrecht'

to their services without monetary payment and instead make their profits with targeted advertising, may unilaterally increase the prices for the advertisers in the absence of competitors with comparable outreach and targeting quality. This increase in prices would potentially be passed on to consumers.[4] In most cases, the users of these platforms "pay" with their attention or personal data,[5] thereby adding an economic value to the generally non-rival personal data and making its collection an important factor in the digital markets.[6] Therefore, the lack of competition in these markets has an impact on the way this data is collected, processed and made available to the users,[7] which can lead to infringements of the users' data protection rights as part of their fundamental rights.[8] In short, the current developments in digital markets pose risks to competition, consumer rights as well as data protection rights.

2 Regulators around the world are starting to react to these issues with more proactive steps to promote competition before damage to the markets and their participants could become irreversible.[9] Several countries have conducted and published marked studies,[10] initiated court proceedings against large online platforms,[11] or began drafting legislation to regulate the digital markets efficiently.[12]

3 While most such legislation is still in drafting stage, the German legislator has introduced a new regulatory tool in section 19a of the German Act against Restraints of Competition ("GWB"**)**.[13] Its development has been significantly influenced by the administrative order of the German Federal Cartel Office ("Bundeskartellamt") against Facebook on the basis of traditional competition law,[14] the first case to take the academic debate forward and apply data protection principles in a competition law case.[15]

(2021) 65 ZUM 89, 91. For a collection of further definitions see Bundeskartellamt, 'Arbeitspapier – Marktmacht von Plattformen und Netzwerken' (09.06.2016), 8ff <www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Think-Tank-Bericht.html> unless otherwise stated, all URLs were last accessed 07.08.2022.

4 Market Study (n 2), paras 6.15-6.23.

5 On the costs for seemingly free services see Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 UCLA L. Rev. 606.

6 Francisco Costa-Cabral and Orla Lynskey, 'Family Ties: The Intersection between Data Protection and Competition in EU Law' (2017) 54 CML Rev 11, 12; Jan Krämer and others, 'Making Data Portability More Effective for the Digital Economy' (*CERRE*, 15.06.2020), 51 <https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/>.

7 For a critical evaluation of the evidence on six adverse effects on data privacy see Aline Blankertz, 'How Competition Impacts Data Privacy – And Why Competition Authorities Should Care' (*Stiftung neue Verantwortung*, September 2020) <www.stiftung-nv.de/de/publikation/how-competition-impacts-data-privacy>.

8 Costa-Cabral (n 6), 12. In Germany, rights on personal data are constitutionally protected by art 2(1) in connection with art 1(1) of the German Basic Law; they are a core part of human dignity, Volker Boehme-Neßler, 'Privacy: A Matter of Democracy. Why Democracy Needs Privacy and Data Protection' (2016) 6 International Data Privacy Law 222, 223.

9 Filippo Lancieri and Patricia Morita Sakowski, 'Competition in Digital Markets: A Review of Expert Reports' (2020) Stigler Center Working Paper Series No. 303, 84 <www.chicagobooth.edu/-/media/research/stigler/pdfs/workingpapers/303competitionindigitalmarketslawreview.pdf>.

10 See Autorité de la concurrence (France), 'Opinion 18-A-03 on Data Processing in the Online Advertising Sector' (06.03.2018) <www.autoritedelaconcurrence.fr/en/opinion/data-processing-online-advertising-sector>; ACCC (Australia), 'Digital Platforms Inquiry - Final Report' (26.07.2019) <www.accc.gov.au/publications/digital-platforms-inquiry-final-report>; Konkurrensverket (Sweden), 'Market Study of Digital Platforms' (01.06.2021) <https://www.konkurrensverket.se/en/news/market-study-of-digital-platforms/>.

11 See Department of Justice (USA), 'Justice Department Sues Monopolist Google For Violating Antitrust Laws' (21.10.2020) <www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>; FTC (USA), 'FTC Sues Facebook for Illegal Monopolization' (09.12.2020) <www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization>.

12 See European Commission, Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector (Digital Markets Act) COM(2020) 842 final ("DMA Proposal"); Japan Fair Trade Commission, 'Study Group on Improvement of Trading Environment surrounding Digital Platforms' (12.12.2018) Interim Discussion Paper 7 <www.jftc.go.jp/en/policy_enforcement/survey/index_files/190220.2.pdf>.

13 Gesetz gegen Wettbewerbsbeschränkungen, available in English at <www.gesetze-im-internet.de/englisch_gwb/>.

14 Bundeskartellamt, administrative order as of 06.02.2019, B6-22/16 ("Administrative Order").

15 The EU approach is characterised by strict separation of competition and data protection law, see Case C-238/05 *Asnef-Equifax* [2006] ECLI:EU:C:2006:734; Google/Double-

This approach, however, is currently pending a ruling by the Court of Justice of the European Union ("CJEU"). Given this context, this discussion will focus in particular on the concerns arising from handling data-related matters under the new regulation.

4 This discussion will show that the new German regulation provides a good first step towards regulating large online platforms and digital markets but that improvements are necessary. The regulation successfully addresses the data-related concerns which have previously been confronted in the Facebook case. But several structural aspects need to be amended before this regulation can serve as template for other jurisdictions.

5 Part of these structural aspects will be outlined in the subsequent chapter following an account of the Facebook proceedings and section 19a GWB. The shortcomings of another structural aspect, the section 19a(1) GWB designation process, will then be discussed in chapter C, followed by an analysis of potential issues arising from data-related concerns. Chapter D will then compare the German regulation with a similar UK framework under development, in order to gather and evaluate possible improvements to the German regulation. Chapter E will analyse the extent to which the Digital Markets Act ("DMA"), an EU regulation expected to be adopted soon, is compatible with the existing German legal framework including section 19a(1) GWB and will then compare the approach taken in the DMA with the German and UK approaches. The discussion will conclude with recommendations for the German regulation in light of the abovementioned issues and comparison with the UK framework.

B. Regulating digital markets in Germany: from the Facebook case to the GWB amendment

I. The Facebook case

6 On 6 February 2019, the Bundeskartellamt enacted an administrative order against three entities of the Facebook Group ("Facebook"), subsequently renamed as Meta. It held that Facebook abused its market dominance as prohibited under section 19(1) GWB. The abuse was established in an infringement of the principles in Articles 6 and 9(2) of the General Data Protection Regulation ("GDPR")[16]: Facebook's policy to merge data collected from its users via several applications with the personal profiles on the users' Facebook accounts was held to constitute unlawful data processing due to a lack of valid consent.[17]

7 On appeal, the Higher Regional Court Düsseldorf ("OLG") granted Facebook the requested interim relief under summary proceedings, basing its decision on competition-related issues.[18] Upon appeal by the Bundeskartellamt, the Federal Court of Justice ("BGH") overruled the OLG decision.[19] In particular, it relied on a different statutory basis for finding abuse of market dominance, citing constitutional and competition law considerations instead of GDPR principles.[20]

8 The case has since advanced to the main proceedings. The first OLG hearing closed with the announcement of a preliminary reference to the CJEU to clarify whether the Bundeskartellamt can rule on GDPR violations and, if so, whether Facebook violated the GDPR provisions.[21]

II. Outline of Section 19a GWB

9 Following the proceedings by the Bundeskartellamt, the German legislator initiated an amendment to the GWB to increase its effectiveness in regulating

click (Case No COMP/M.4731) Commission Decision [2008] OJ C184/10; Facebook/WhatsApp (Case No COMP/M.7217) Commission Decision [2014] OJ C417/02.

16 Regulation of the European Parliament and of the Council (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

17 Administrative Order (n 14), paras 494ff.

18 OLG Düsseldorf, judgment as of 26.08.2019, VI Kart 1/19 (V) ("OLG-Facebook-decision").

19 BGH, judgment as of 23.06.2020, KVR 69/19, available in English at <https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/BGH-KVR-69-19.html>.

20 Blankertz (n 7), 16; Mackenrodt (n 3), 90; Stephan Manuel Nagel and Stefan Horn, 'Die Facebook-Entscheidung des BGH – ein neuer Kompass für die Missbrauchskontrolle?' (2021) ZWeR 78, 112-114.

21 OLG Düsseldorf, order for reference as of 24.03.2021, Kart 2/19 (V). See also OLG, 'Facebook gegen Bundeskartellamt: Vorlagebeschluss beim EuGH' (press release no. 11/2021, 23.04.2021) <https://www.olg-duesseldorf.nrw.de/behoerde/presse/archiv/Pressemitteilungen_aus_2021/20210423_PM_Facebook-Beschluss/index.php>.

digital markets.[22] At the heart of this amendment is Section 19a GWB, which grants the Bundeskartellamt the power to prohibit certain conduct of large online platforms in a two-step mechanism.

10 In a first step, the Bundeskartellamt designates a company as having "paramount significance for competition across markets" ("PSC") by considering the factors in Section 19a(1) GWB. This designation is valid for five years, during which the Bundeskartellamt can take the second step of enforcing any of the prohibitions listed in Section 19a(2) GWB to support competition. Two of these prohibitions can be seen as protruding into data protection law.

11 Section 19a(2)(1)(4) GWB grants the Bundeskartellamt the power to prohibit a firm from making access to its services conditional on either (i) a user's consent to data merging (similar to Facebook's conduct described above)[23]; or (ii) a business' consent to data processing for purposes other than providing its services. This prohibition builds on the concept in Article 6 GDPR but, unlike in the Facebook case, the Bundeskartellamt will not have to refer to the GDPR when seeking to enforce this prohibition.

12 Section 19a(2)(1)(5) GWB enables the Bundeskartellamt to prohibit actions constraining interoperability and data portability if these actions hinder competition. A business is deemed to constrain interoperability if it hinders different systems from working together as seamlessly as possible. It is deemed to constrain data portability if it hinders the retrieval of digitally stored personal data by data subjects wishing to transfer this data to another business.[24] This prohibition overlaps notably with the right to data portability in Article 20 GDPR. Together with Section 19a(2)(1)(4) GWB, this prohibition can be seen to empower the Bundeskartellamt to address data issues that are similarly dealt with by the GDPR.

13 The remaining paragraphs will outline four structural aspects of Section 19a GWB that are subject to criticism but whose detailed analysis is beyond the scope of this discussion.

14 The disconnection from the GDPR in the two prohibitions addressed above might lead to the development of deviating interpretations on data-related aspects in German competition law and EU data protection law, as the last instance for proceedings based on the GDPR is the CJEU but for the GWB it is the BGH. This is criticised because it could impede harmonised enforcement and thus weaken legal certainty within the EU.[25]

15 Furthermore, there are two ways by which Section 19a GWB aims to increase the protection of competition by speeding up regulatory interventions.[26] Neither is without criticism.

16 First, the regulation cuts down on the time that appeals might take: instead of giving the parties two instances for appeal (OLG and BGH), orders under Section 19a GWB can only be appealed at the BGH.[27] However, this loss of an additional instance for appeal might be held to unduly reduce legal protection for the firms.[28]

17 Second, the legislator shifted the burden of proof so that, in case of enforcement, designated firms must show why they are legitimate in carrying out actions that are otherwise prohibited under Section 19a(2) GWB.[29] This additional burden of proof is criticised because some of the prohibited actions are not perceived to be harmful to competition under traditional competition law.[30]

22 GWB-Digitalisierungsgesetz (BGBl. I p. 2, 18.01.2021) ("GWB Digitisation Act").

23 The Facebook case is mentioned in the Government Draft of the GWB Digitisation Act (Bundestag printed matter 19/23492, 19.10.2020) ("Government Draft"), 76.

24 Commission 'Competition Law 4.0', *A New Competition Framework for the Digital Economy* (Federal Ministry for Economic Affairs and Energy, 2019), 39.

25 Torsten Körber, 'Die Digitalisierung der Missbrauchsaufsicht durch das „GWB-Digitalisierungsgesetz" im Spannungsfeld von moderater Anpassung und Überregulierung' (2020), 75 <https://ssrn.com/abstract=3543719>.

26 Resolution Recommendation and Report on the GWB Digitisation Act (Bundestag printed matter 19/25868, 13.11.2020) ("Resolution Recommendation"), 119ff. This acceleration is deemed necessary since for example it is unforeseeable when the Facebook case will be definitively decided, Rupprecht Podszun, 'Die 10. Novelle des Gesetzes gegen Wettbewerbsbeschränkungen (GWB): Stellungnahme für den Ausschuss für Wirtschaft und Energie des Deutschen Bundestags' (expert opinion, Deutscher Bundestag 2020), 7f.

27 S 73(5) GWB.

28 Sebastian Louven, '§ 19a GWB kommt – Was ändert sich beim Rechtsschutz?' (*Louven.Legal*, 14.01.2021) <https://louven.legal/2021/01/14/%C2%A7-19a-gwb-kommt-was-aendert-sich-beim-rechtsschutz/>.

29 S 19a(2)(3) GWB; Government Draft (n 23), 77f.

30 In favour see Verbraucherzentrale Bundesverband e.V., 'Fairen Wettbewerb in digitalen Märkten sicherstellen' (expert opinion, Deutscher Bundestag 2020), 14; against see Körber (n 25), 56-60.

18 Lastly, the justification of the extended powers in Section 19a GWB is called into question. Under the *ex post* approach of Section 19 GWB the Bundeskartellamt can only act upon a suspicion that a firm had abused its market dominance. In contrast, the *ex ante* approach of the new Section 19a GWB allows the Bundeskartellamt to act pre-emptively even without such suspicion. Some of the newly introduced obligations may require large online platforms to substantially revise their business strategy. Due to these drastic consequences, this regulation requires strong justification. This justification may be found under competition law principles, which provide that, if the market cannot regulate itself through competition, the state can interfere by imposing special responsibilities on entities in sufficiently powerful market positions. These responsibilities include a refrain from exploiting users and from further distorting competition. Insofar as any digital market cannot regulate itself, the state is therefore justified in imposing such responsibilities, in the form of additional obligations under Section 19a GWB, on entities that it designates as being in such powerful positions.[31] However, some argue that more observation is still required before it can be established that digital markets cannot regulate themselves, so as to justify interference.[32] Regardless, the advantages of the new regulation in preventing exploitation of businesses and private users constitute a sufficient basis to consider an *ex ante* approach necessary.[33]

C. Is the regulation of digital markets in Germany under Section 19a GWB justified?

19 The administrative order against Facebook has sparked a discussion in Germany on how large online platforms should be regulated. It brought to attention the issues of applying traditional competition law to data-related conduct of multi-sided platforms. Together with two expert reports that recommended cautious steps towards stronger regulation,[34] the legislator concluded from this order that a new legal instrument, tailored to the needs of the digital markets, was necessary: Section 19a GWB.[35]

20 This chapter will first consider if the designation process is sufficiently limited to powerful online platforms. It then will turn to the issues encountered in the Facebook case regarding data-related enforcement: the legitimacy of applying the new powers in GDPR-related areas, and the justification for the overlapping applicability of competition and data protection authorities. It will defend the new regulation against these GDPR-related concerns, but acknowledge that the designation process risks being over-inclusive.

I. Risk of over-inclusive designation under section 19a(1) GWB

21 The scope of application of Section 19a GWB is determined as follows:

> *"(1) The Bundeskartellamt may issue a decision declaring that an undertaking which is active to a significant extent on markets within the meaning of Section 18(3a) is of paramount significance for competition across markets. In determining the paramount significance of an undertaking for competition across markets, account shall be taken in particular of:*
>
> *1. its dominant position on one or several market(s),*
>
> *2. (...)"*[36]

31 Cf Commission 'Competition Law 4.0' (n 24), 48; Körber (n 25), 51-52.

32 Cf Körber (n 25), 46f, 81. See also Christine S. Wilson and Keith Klovers, 'The Growing Nostalgia for Past Regulatory Misadventures and the Risk of Repeating these Mistakes with Big Tech' (2020) 8 Journal of Antitrust Enforcement 10, comparing strong regulation of big tech companies to controversial historic US railroad and airline regulations.

33 Cf Laurine Signoret, 'Code of Competitive Conduct: A New Way to Supplement EU Competition Law in Addressing Abuses of Market Power by Digital Giants' (2020) 16 European Competition Journal 221, 230; Damien Geradin, 'What Is a Digital Gatekeeper? Which Platforms Should be Captured by the EC Proposal for a Digital Market Act?' (2021), 4-7 <https://papers.ssrn.com/abstract=3788152>.

34 Heike Schweitzer and others, *Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen: Gutachten für das Bundesministerium für Wirtschaft und Energie* (1st edn, Nomos Verlag 2018), 192f, an executive summary is available in English at <www.bmwi.de/Redaktion/DE/Downloads/Studien/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen-zusammenfassung-englisch.pdf?__blob=publicationFile&v=3>; Commission 'Competition Law 4.0' (n 24), 46ff.

35 Anne C. Witt, 'Excessive Data Collection as a Form of Anticompetitive Conduct: The German Facebook Case' (2021), The Antitrust Bulletin, 21 <https://doi.org/10.1177/0003603X21997028>.

36 Section 19a of the Act against Restraints of Competition, available in English at <www.gesetze-im-internet.de/englisch_gwb/>.

22 This scope plays an important role. The designation must not be over-inclusive to ensure that the *ex ante* regulation is justified under competition law principles by limiting it to powerful platforms. The designation also must not be under-inclusive as it might otherwise not tackle issues in the digital market effectively. This section will explain how this regulation was intended to have a narrow scope but that vague formulations and insufficient definitions resulted in an over-inclusive regulation.

23 As a starting point, the designation is unlikely to be over-inclusive because the legislator had intended to specify a narrow scope, and because this scope is accepted by the Bundeskartellamt. According to the official explanations, the regulation addresses only a small group of firms with a strategic position on digital markets.[37] These mainly include the largest US American tech companies (Google, Apple, Facebook, Amazon and Microsoft).[38] An extension to large Chinese platforms or possibly to future European businesses, as hinted by the president of the Bundeskartellamt,[39] would also not risk a significant expansion of scope. This intention to specify a narrow scope is demonstrated in the following two aspects.

24 The enforcement structure of Section 19a GWB helps avoiding over-inclusiveness: unlike Section 19 GWB, which can also be enforced in civil courts, the enforcement of Section 19a GWB is reserved for the Bundeskartellamt.[40] Together with the limitation of courts available for appeals to the BGH, this leaves only two state entities with the competencies to interpret Section 19a GWB. Therefore, it is unlikely in practice that the scope of designation under Section 19a(1) GWB will be interpreted substantially broader than anticipated.

25 Moreover, the new powers avoid over-inclusiveness through passage of time. A company which the Bundeskartellamt designated under section 19a GWB might lose market power and eventually fall outside the scope of this regulation. To avoid that those companies remain subject to additional prohibitions, the designation is limited to a time period of five years.[41]

26 However, vague formulations in the new regulation risk it to be applied over-inclusively and thereby undermine the intention of creating a narrow section. This can be observed in three instances.

27 First, the new term PSC risks being over-inclusive because its defining factors might be interpreted more broadly than anticipated. The specification of these factors in section 19a(1)(2) GWB and thereby also of the scope of the new term is left to the Bundeskartellamt.[42] This provides the Bundeskartellamt with powers to broaden the scope of application. Even if the Bundeskartellamt does not decide to designate additional companies, the lack of precedents for the application of PSC complicates the self-assessment process for companies in determining if they might satisfy the designation requirements.[43] This uncertainty risks placing undue pressure on companies that are not intended to be designated.

28 On a separate note, it is unconvincing that the use of this vague term would help to avoid under-inclusiveness. Some argue that the broad terminology supports the removal of enforcement barriers; if too many detailed obligatory requirements had to be satisfied, large online platforms with ample resources to spend on legal counsel could appeal on narrow technical points in an attempt to prolong court proceedings on the applicability of Section 19a GWB.[44] With this strategy, these firms could potentially even avoid enforcement. However, the broader scope of application, which would be necessary to avoid under-inclusiveness on this basis, weakens the legitimacy of the new regulation and, at least theoretically, risks the regulation being struck down as disproportionate intrusion into the companies' fundamental rights.[45]

37 Government Draft (n 23), 61.

38 Torsten J. Gerpott and Tobias Mikolas, 'Zugang zu Daten großer Online-Plattformbetreiber nach der 10. GWB-Novelle' (2021) CR 137, para 1; Witt (n 35), 1.

39 Klaus Janke, 'Wir können jetzt früher einschreiten' *HORIZONT* (Frankfurt (Main), 11.02.2021), <www.bundeskartellamt.de/SharedDocs/Publikation/DE/Interviews/2021/210211_HORIZONT.html>.

40 S 19a(1)(1), (2)(1) GWB; Gabriela von Wallenberg, '10. GWB-Novelle – Ordnungsrahmen zur Digitalisierung der Wirtschaft' (2020) 53 ZRP 238, 239.

41 S 19a(1)(3) GWB; Resolution Recommendation (n 26), 112.

42 Monopolkommission, 'Policy Brief: 10. GWB-Novelle – Herausforderungen auf digitalen und regionalen Märkten begegnen!' (2020), vol 4, 3.

43 Körber (n 25), 51. For the same reason the Commission 'Competition Law 4.0' recommended the retention of the market dominance requirement instead of introducing a new legal concept, see Commission 'Competition Law 4.0' (n 24), 50.

44 Deutscher Bundestag, 'Wortprotokoll der 95. Sitzung' (protocol no. 19/95, 2020), 10.

45 Companies are covered in particular by arts 2(1), 12, 14 of the German Basic Law.

29 Second, the regulation creates another risk for over-inclusiveness by introducing the "dominant position on one or more markets" as one of five equal factors instead of making it an obligatory requirement for the designation. Since not all factors have to be considered in every investigation, this structure relieves the Bundeskartellamt from determining the relevant market, a difficult task in digital markets.[46] It is probable that the Bundeskartellamt will make use of this chance to avoid a potential source of error and accelerate the investigation procedure.[47] Although this strategy initially seems to support the aim of avoiding under-inclusiveness by providing the addressed companies with one less reason for appeal, courts generally do not strike down orders in competition law over controversial market definitions. For example, the summary proceedings on the Facebook case did not address the Bundeskartellamt's determination of the relevant market.[48] To the contrary, if the market dominance test was introduced as obligatory requirement, the regulation would express more clearly that the term PSC constitutes a stronger position than the market dominance requirement in Section 19 GWB.[49] Currently this relation cannot be clearly deduced from the wording of the regulation. This is another aspect that makes the regulation appear over-inclusive.

30 Third, by using a reference to another section that is not limited to digital markets, the regulation risks being more over-inclusive. According to the official explanation, the reference of Section 19a(1)(1) GWB to "markets within the meaning of Section 18(3a)" also covers analogue multi-sided markets, such as shopping centres with markets regarding the shops and regarding their customers, or private television broadcasters with the market of the advertising providers and the market of the subscribers.[50] The non-exhaustive list of factors also does not cater explicitly to digital markets.[51] Therefore, this oversight extends the scope of the new regulation beyond digital markets.

31 To conclude, official publications regarding the new regulation and the inclusion of some aspects display the intention of the legislator to introduce Section 19a GWB with a very narrow scope. If the regulation was always acted upon within this limited scope, it would strike a balance between over- and under-inclusiveness. However, the wording of this regulation is overly broad in the abovementioned parts so that it creates a foundation for over-inclusive application. Therefore, this designation process needs clarification.

II. Risk of over-autonomous actions by the Bundeskartellamt

32 The Bundeskartellamt is not empowered to enforce data protection law, as this is the purpose of the national data protection authorities within the EU. In order to subject companies that are active throughout the EU only to one investigation per data protection issue, the GDPR introduced the one-stop-shop mechanism to determine which one of the data protection authorities in the EU is competent to enforce a specific matter.[52] However, the new Section 19a GWB awarded the Bundeskartellamt powers to enforce prohibitions connected to data processing and data portability, which are also regulated under the GDPR. By applying these new powers, the Bundeskartellamt may act autonomously in the sphere of data protection law. Whilst the Bundeskartellamt could thereby provide valuable support to the data protection authorities in enforcing some GDPR principles more efficiently, these powers risk undermining the one-stop-shop mechanism. This section will argue that the Bundeskartellamt cannot rely on any existing exceptions to the one-stop-shop mechanism to justify its new powers. However, it will also show that the Bundeskartellamt does not need to comply with the one-stop-shop mechanism because it merely enforces data protection related matters supplementary to the enforcement of competition law.

33 To begin with, the new powers of the Bundeskartellamt are useful for compensating the time delay observed in data protection enforcement. Under the one-

46 Romina Polley, 'Paradigmenwechsel in der deutschen Missbrauchsaufsicht – Der Referentenentwurf zur 10. GWB-Novelle' (2020) 8 NZKart 113, 116. For problems of distinguishing digital markets see also Ralf Dewenter and others, 'Abgrenzung zweiseitiger Märkte am Beispiel von Internetsuchmaschinen' (2014) 2 NZKart 387; Commission 'Competition Law 4.0' (n 24), 27ff.

47 Cf Körber (n 25), 51.

48 OLG-Facebook-decision (n 18). For another example see LG Berlin, judgment as of 19.02.2016, 92 O 5/14 Kart (Google Snippets).

49 Government Draft (n 23), 73f; Körber (n 25), 51.

50 Government Draft of the Ninth GWB Amendment (Bundestag printed matter 18/10207, 07.11.2016), 49; Körber (n 25), 49.

51 Körber (n 25), 50; Sebastian Louven, '§ 19a GWB: Welche Unternehmen sind betroffen?' (*Louven.Legal*, 01.11.2020) <https://louven.legal/2020/11/01/%C2%A7-19a-gwb-welche-unternehmen-sind-betroffen/>.

52 Recital 127 of the GDPR.

stop-shop mechanism, the only competent data protection authority for cases with cross-border processing of personal data is the authority in the jurisdiction with the main establishment of the respective firm in the EU, called the lead supervisory authority ("LSA").[53] As most large online platforms have their main establishment in Ireland,[54] the Irish Data Protection Commission ("IDPC") is the LSA for most situations addressed by Section 19a GWB. While the IDPC has initiated several investigations against large online platforms,[55] these investigations highlight an inherent flaw of the GDPR in practice: time delay. The first complaints have been submitted as soon as the GDPR entered into force, but almost three years later the IDPC is still far from reaching most decisions.[56] This delay has sparked criticism.[57] Therefore, help from the Bundeskartellamt could be beneficial for the enforcement of data protection.

34 However, the powers of the Bundeskartellamt would not be justified if they necessitated a breach of the one-stop-shop mechanism. This mechanism is important to improve compliance with the principle of sincere cooperation (Article 4(3) TEU) in comparison to the former Data Protection Directive ("DPD"),[58] because, unlike competition law, the GDPR is only enforced by national authorities and not directly at EU level.[59] Nevertheless, some strategies have been developed to avoid this mechanism, the three most relevant of which are set out below.

35 One exception to this mechanism has been established by the French data protection authority CNIL in a case against Google.[60] It argued that, in line with the guidelines by the European Data Protection Board ("EDPB") for identifying LSA,[61] Google did not have a place of central administration in the EU because the Irish headquarters had no autonomous decision-making powers. Therefore, all EU data protection authorities were competent. However, this argumentation seems to rely on the wording of the first GDPR proposal.[62] This wording has since been changed to reflect that it is sufficient for a place of central administration to have the power to make autonomous decisions regarding the implementation of data collection, not necessarily its purposes.[63] Therefore, the CNIL-interpretation is not persuasive.

53 Art 56(1), (6) GDPR.

54 Mandy Hrube, 'EuGH: Schlussanträge des Generalanwalts zur Zuständigkeit von Datenschutzbehörden bei grenzüberschreitender Datenverarbeitung' (2021) CR R25.

55 IDPC, 'Data Protection Commission Opens Statutory Inquiry into Facebook' (17.12.2018) <www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-facebook>; IDPC, 'Data Protection Commission Opens Statutory Inquiry into Google Ireland Limited' (22.05.2019) <www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited>.

56 An open letter by the platform noyb describes that the first two out of six steps of the investigation took the IDPC almost two years and therefore expects a decision to take years, 'Open Letter on "Confidential" Dealings in Facebook Case' (noyb, 25.05.2020), 4 <https://noyb.eu/en/open-letter>. The exceptions are two decisions against Twitter and WhatsApp respectively, see IDPC, "Data Protection Commission Announces Decision in Twitter Inquiry" (15.12.2020) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-twitter-inquiry>; IDPC, "Data Protection Commission Announces Decision in WhatsApp Inquiry" (02.09.2021) <https://www.dataprotection.ie/index.php/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry>.

57 Catherine Stupp, 'Dutch Lawsuit Seeks Quicker Resolution in Google Case; Consumers and Privacy Groups are Frustrated with Lengthy GDPR Process' *Wall Street Journal* (New York, N.Y., 07.01.2021); Kelvin Chan, 'EU Ruling on Data Privacy Leaves Facebook Exposed' *Toronto Star* (Toronto, 14.01.2021).

58 Directive of the European Parliament and of the Council 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/0031. Shortcomings on its compliance with article 4(3) TEU are evident in Case C-230/14 *Weltimmo* [2015] ECLI:EU:C:2015:639 and Case C-210/16 *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388.

59 Alberto Miglio, 'The competence of supervisory authorities and the 'one-stop-shop' mechanism' (2020) 28 EU Law Live, Weekend Edition 10, 10-11.

60 CNIL (Commission Nationale de l'Informatique et des Libertés), Délibération de la formation restreinte n° SAN – 2019-001 du 21.01.2019 prononçant une sanction pécuniaire à l'encontre de la société Google LLC, a press release is available in English at <www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>. See also Lokke Moerel, 'CNIL's decision fining Google violates one-stop-shop' (2019) <https://papers.ssrn.com/abstract=3337478>.

61 Article 29 Data Protection Working Party, 'Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority' (WP 244 rev.01, 05.04.2017), as endorsed by the EDPB in its first plenary meeting (EDPB, 'Endorsement 1/2018' (25.05.2018)), 5.

62 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2012] COM(2012) 11 final, art 4(13).

63 Moerel (n 60), 10-11.

36 Further alternatives have been set out in the opinion by advocate general Bobek,[64] and have recently been accepted by the CJEU in its decision.[65] In particular, he set out two approaches on how supervisory authorities other than the LSA could be authorised to handle cases against large online platforms or oblige the LSA to handle them in a certain manner. Both approaches require the LSA to have failed acting promptly in its investigations.[66] Due to the time delay issue of the IDPC, a German data protection authority could apply these approaches to handle cases against large online platforms. However, there are no indications for the development of a cooperation structure of this authority with the Bundeskartellamt.

37 This outline shows that all three strategies lack authority to justify the Bundeskartellamt's new powers. Therefore, the Bundeskartellamt cannot directly enforce data protection law without undermining the one-stop-shop mechanism.

38 Instead, the Bundeskartellamt can address data-related concerns and thus replace otherwise delayed actions with supplementary data protection enforcement. The Bundeskartellamt is not prohibited from handling a competition law case despite data protection concerns; in some decisions, competition authorities have to regulate aspects that are also covered by data protection laws in order to efficiently enforce compliance with competition law.[67] The remaining paragraphs will set out the legal foundation for this reasoning in two points.

39 First, the new powers only extend to supplementary enforcement of data-related aspects because the two GDPR-related prohibitions under Section 19a(2)(1)(4)-(5) GWB are based on competition law. Regarding data processing, only data that is relevant for competition and that results in anti-competitive effects on new market entrants or other businesses is taken into account. The interoperability- and data portability-related prohibition is explicitly limited to conduct that hinders competition. Furthermore, data portability itself may improve competition law through positive effects on innovation,[68] which often leads to competitive advantages.[69] It might therefore support smaller companies and increase competition.

40 Second, competition and data protection law have similar goals, irrespective of different methods and situations they can be applied to,[70] so that mutual enforcement supports each other's objectives. Two of these goals are highlighted below.

41 One common goal is consumer welfare. The main objective of data protection is to counteract power imbalances between organisations and individuals.[71] It protects personal data as a fundamental right of the weaker individuals.[72] Data protection law therefore pursues the goal of consumer welfare.[73] Competition law's main objective is maintaining competition on the market by interfering when companies abuse their market dominance.[74] The reason for maintaining competition, in turn, is the facilitation of low prices, high quality and innovation to benefit the consumers. Accordingly, competition law essentially strives for consumer welfare as well,[75]

64 Case C-645/19 *Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit*, Opinion of AG Bobek (13.01.2021).

65 Case C-645/19 *Facebook Ireland Limited, Facebook Inc., Facebook Belgium BVBA v Gegevensbeschermingsautoriteit* [2021] ECLI:EU:C:2021:483.

66 Ibid para 115-122.

67 Costa-Cabral (n 6), 23; cf Sebastian Louven, 'When Privacy Meets Competition' (*Louven.Legal*, 01.10.2020) <https://louven.legal/2020/10/01/when-privacy-meets-competition/>. See also Wolfgang Kerber, 'Updating Competition Policy for the Digital Economy? An Analysis of Recent Reports in Germany, UK, EU, and Australia' (2019), 41 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469624>; Boris Paal, 'Marktmacht im Daten(schutz)recht' (2020) ZWeR 215.

68 Krämer (n 6), 10, 64.

69 Prodromos Chatzoglou and Dimitrios Chatzoudes, 'The Role of Innovation in Building Competitive Advantages: An Empirical Investigation' (2018) 21 European Journal of Innovation Management 44, 56.

70 See Costa-Cabral (n 6), 17-18.

71 Administrative Order (n 14), para 530.

72 Costa-Cabral (n 6), 17.

73 Nela Grothe, *Datenmacht in der kartellrechtlichen Missbrauchskontrolle* (1st edn, Nomos Verlag 2019), 31.

74 Ibid 88.

75 Cf Miriam Buiten, 'Datenschutzverletzungen als Kartellrechtsverstöße', in Elena Beyer and others (ed), 'Privatrecht 2050 - Blick in die digitale Zukunft' (1st edn, Nomos Verlag 2020), 335. See also David A. Balto and Matthew C. Lane, 'Monopolizing Water in a Tsunami: Finding Sensible Antitrust Rules for Big Data' (2016) 12, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2753249>; Margrethe Vestager, 'Competition is a Consumer Issue' (13.05.2016) <https://wayback.archive-it.org/12090/20191129205633/https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-consumer-issue_en>; Richard Whish and David Bailey, *Competition law* (9th edn, Oxford University Press 2018), 19.

potentially as the main goal that interacts with other goals.[76]

42 Another goal common to both competition law and data protection law is promoting and upholding the internal market.[77] Regarding data protection, this goal has manifested in the replacement of the DPD with the GDPR that increases EU-wide harmonisation in its capacity as a Regulation. And competition law supports the internal market by preventing trade barriers between Member States.[78]

43 On this basis, it can be deduced that the main goals of competition and data protection law are substantially the same. This finding substantiates the expectation that both authorities complement each other's actions when either of them regulates a matter.[79] Accordingly, they do not act over-autonomously when applying principles from the other sphere of law for supplementary enforcement.

44 Therefore, the new powers granted to the Bundeskartellamt are not in conflict with the one-stop-shop mechanism. Their reach into the sphere of data protection law is justified because they are centred in competition law and merely allow the Bundeskartellamt to enforce these principles as supplementary effects. As such, the new regulation does not risk leading to over-autonomous actions by the Bundeskartellamt in the sphere of data protection law.

III. Risk of overlapping application of competition and data protection law

45 As established above, the Bundeskartellamt has been awarded competencies that can enforce data protection-related aspects as supplementary effects. These new powers result in the applicability of both competition and data protection law to the same matters. This might pose a risk for the potentially affected companies as overlapping applicability may weaken legal certainty when the authorities take different approaches and apply different interpretations to similar matters.[80] This would make it increasingly difficult for companies to avoid administrative orders via specific changes of conduct. However, the following two arguments will successfully refute this risk.

46 The risk of overlapping application is limited to a very small number of instances. As outlined above, the designation process in Section 19a(1) GWB is intended to ensure that only very few platforms with particularly powerful positions in the digital markets can be faced with the prohibitions in Section 19a(2) GWB. Therefore, only these few companies can be subject to overlapping applicability. The number of instances that may fall under both regulations is further limited because only two of the seven available prohibitions, from Section 19(2)(1)(4)-(5) GWB, are sufficiently connected to data protection.

47 This risk is further reduced by sufficient cooperation between the two authorities. So far, the only type of cooperation set out in law between the two authorities is the exchange of information.[81] Nevertheless, cooperation between the competition and data protection authorities is likely to arise in practice even without legal obligation. For example, in the Facebook case the Bundeskartellamt has been cooperating with German data protection authorities, in particular with the Federal Commissioner for Data Protection and Freedom of Information ("BfDI"), throughout its investigation.[82] The BfDI subsequently also publicly approved the Bundeskartellamt's

76 Ariel Ezrachi, 'EU Competition Law Goals and The Digital Economy' (2018) <https://papers.ssrn.com/abstract=3191766>; Ceara Tonna-Barthet and Louis O'Carroll, 'Procedural Justice in the Age of Tech Giants – Justifying the EU Commission's Approach to Competition Law Enforcement' (2020) 16 European Competition Journal 264, 268-271.

77 Hans-Georg Kamann and Dominik Miller, 'Kartellrecht und Datenschutzrecht – Verhältnis einer „Hass-Liebe"?' (2016) 4 NZKart 405, 407-408.

78 Costa-Cabral (n 6), 19.

79 Inge Graef and others, 'Limits and Enablers of Data Sharing: An Analytical Framework for EU Competition, Data Protection and Consumer Law' (TILEC Discussion Paper 2019-024, Digital Clearinghouse 2019), 20.

80 Monopolkommission, *Hauptgutachten. Wettbewerb 2018 – XXII. Hauptgutachten der Monopolkommission gemäß § 44 Abs. 1 Satz 1 GWB* (Nomos Verlag 2018), para 683, a summary is available in English at <www.monopolkommission.de/en/press-releases/219-biennial-report-xxii-competition-2018.html>; Torsten Körber, 'Die Facebook-Entscheidung des Bundeskartellamtes – Machtmissbrauch durch Verletzung des Datenschutzrechts?' (2019) 7 NZKart 187, 194. See also EDPS, 'Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content' (14.03.2017); Christian Schwedler, 'Schutz von Nutzerdaten durch Missbrauchskontrolle – das Bundeskartellamt als Datenschutzbehörde', in Torsten Körber and Ulrich Immenga (eds), *Innovation im Kartellrecht - Innovation des Kartellrechts* (Nomos Verlag 2020), 66-67 regarding the potentially conflicting Facebook decision.

81 S 50f(1) GWB.

82 Administrative Order (n 14), para 555.

administrative order.[83] As the new powers in Section 19a GWB have removed all doubts on the fact that the competencies of the two authorities overlap, it is even more likely that voluntary cooperation will arise between these authorities to coordinate their approaches and decisions. Therefore, any remaining risk of overlapping application is highly unlikely to manifest in practice.

48 In conclusion, the risk that the overlapping applicability of data protection law and the new competition law powers may result in overlapping application is limited to an insignificant number of cases. The cooperation that is expected to take place in practice decreases this risk even further.

D. Comparison with the UK approach to regulate large online platforms and digital markets

49 Given the abovementioned shortcomings of the GWB amendment, a comparison with a similar piece of upcoming legislation, the UK approach to regulate digital markets, will help to discover improvements for the German regulation. Both regulations grant the empowered authorities similarly broad competencies, despite the fact that the new German regulation is located within competition law whereas the UK aims to create a new regulatory unit for which it can define new powers. The broad powers for the Bundeskartellamt came about because the German regulation inherited none of the traditional competition law requirements. Therefore, these two approaches are directly comparable, irrespective of the debate on whether competition law is the right sphere of law to address the issues on digital markets.[84]

50 After a short introduction to the UK approach, the issues identified regarding the new German regulation will be addressed from the perspective of the UK proposal. This will display some advantages of the UK approach over the German system and give suggestions on how the German regulation could benefit from these insights.

I. The UK approach

51 While the exact structure of the envisaged regulatory regime is pending legislative action, a high-level overview can be deduced from the Advice of the Digital Markets Taskforce,[85] in line with the latest government statement.[86] The new regulatory regime, the Digital Markets Unit ("DMU"), is established within the framework of the Competition and Markets Authority ("CMA"),[87] but it will remain unconnected to the powers of the CMA.[88] This regulation will create an *ex ante* system, so that the DMU can impose additional obligations on large online platforms in advance of any verifiable abuses of market dominance.

52 In particular, the DMU will be empowered to establish and enforce rules for large online platforms whose activities provide them with strategic market status ("SMS firms") in two steps.[89] First the DMU will designate a company as SMS firm for a fixed period of time,[90] taking into account several factors.[91] Then the DMU will establish an enforceable code of conduct tailored to the SMS firm.[92] It will also address the roots of the strategic status and market power of SMS firms by imposing on them effective and proportionate pro-competitive interventions ("PCIs"), consisting of a broad range of remedies with the aim of promoting competition.[93]

83 BfDI, 'Landmark Decision on Facebook by the Bundeskartellamt' (21.02.2019) <https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/EN/2019/06_BundeskartellamtzuFacebook.html;jsessionid=7270302A187803EE431468D9A459410D.intranet222>.

84 On this debate see Sebastian Louven, 'Braucht es mehr materielles Kartellrecht für digitale Plattformen?' (2019) ZWeR 154, 187-191.

85 CMA, 'A new pro-competition regime for digital markets: Advice of the Digital Markets Taskforce' (CMA 135, 08.12.2020) ("Taskforce Advice").

86 Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy (UK), 'A new pro-competition regime for digital markets' (CP 489, 20.07.2021).

87 CMA, 'New Watchdog to Boost Online Competition Launches' (07.04.2021) <www.gov.uk/government/news/new-watchdog-to-boost-online-competition-launches--3>.

88 Taskforce Advice (n 85), para 7.3.

89 Ibid para 4.33.

90 Ibid para 4.28.

91 Ibid paras 4.7-4.24.

92 Ibid paras 4.35-4.37.

93 Ibid paras 4.60-4.81.

II. Which parts of the UK approach could improve the German regulation?

53 The evaluation of risks stemming from Section 19a GWB shows that some improvements are necessary to increase its legitimacy. This section will outline aspects from the UK structures which address the issues identified in the German designation process. It will also display how the implementation of further aspects of the UK approach might enhance the available prohibition structure and the cooperation between the authorities.

1. Comparison of the designation processes

54 According to the Digital Markets Taskforce, the test to designate firms as having SMS in the digital markets should be the following:

> *a firm only has SMS if "the firm has substantial, entrenched market power in at least one digital activity".*[94]

55 This section will consider this SMS test in three parts and deduce three aspects that would be beneficial to be included in the German regulation in order to avoid over-inclusiveness.

56 The first part is an assessment of whether the firm has *substantial* market power in at least one digital activity. The next two paragraphs show that this approach is one step closer to avoiding over-inclusiveness than the German regulation and should thus serve as inspiration for the German legislator. But simply mirroring this approach would be insufficient to substantially improve the German law.

57 The aspect that would be beneficial for the German legislation is the obligatory requirement to assess the market power because it narrows the scope of application more than an optional factor. The market power assessment could be made compulsory in the German regulation either by adopting the UK requirement on substantial market power, or by giving the market power factor more weight than other factors.[95] However, it would be even more beneficial for the German regulation to take this test another step further and diminish the scope of application through the implementation of a requirement for market dominance in at least one digital market.[96] As the online platforms that are expected to fall under this regulation will all satisfy this test in one digital market or another, this step would not result in under-inclusiveness. Instead, it would further tackle over-inclusiveness and put at ease companies that the legislator does not intend to target.

58 The aspect that should not be considered for the German regulation is the fact that the SMS test does not require significant market power across markets but that substantial market power in one specific activity suffices.[97] While it can be presumed that power across markets will nevertheless play a role in designating SMS firms, this formulation could potentially lead to over-inclusiveness and is therefore not advisable for the German system.

59 The second part, the requirement of *entrenched* market power, aims to exclude firms with only temporary market power to avoid stalling innovation. This requirement would also be beneficial to the German system. It would tackle the risk of over-inclusiveness by avoiding the designation of firms whose market power is only a temporary phenomenon without sufficient adverse effects on the digital markets to justify the additional obligations.

60 As a third part, the test sets out that the market power has to relate to a "digital activity", explicitly referring to digital as opposed to analogue markets. In the current German legislation, the wording in Section 19a(1)(1) GWB also includes multi-sided platforms that are active only on non-digital markets. Thus, it is advisable for the German legislator to add the word "digital" in order to reduce the risk of over-inclusiveness.

61 The above considerations regarding the three parts of the SMS test set out three requirements that should be implemented in the German designation process in order to reduce the scope of the regulation. The current legislation risks being over-inclusive.

2. Comparison of the scope of autonomous actions by the authorities

62 In post-Brexit UK, the proposed regulation does not risk acting over-autonomously by way of working around the one-stop-shop mechanism because the UK is not directly bound by the EU GDPR anymore.

94 Taskforce Advice (n 85), paras 4.9-4.22.

95 Cf Daniela Seeliger, 'Öffentliche Anhörung zum Entwurf eines Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 (GWB)' (expert opinion, Deutscher Bundestag 2020), 2.

96 Polley (n 46), 117; Körber (n 25), 78.

97 Taskforce Advice (n 85), para 4.7ff.

While the UK will presumably remain connected to the GDPR rules to some extent by way of an adopted adequacy agreement,[98] this does not interfere with the UK legislator's ability to assign additional competencies to different supervisory authorities. The UK can therefore decide independently to curtail the powers of other national authorities like the Information Commissioner's Office ("ICO") by granting some of their powers to the new DMU. This section will show that the proposed scope of PCIs that are available to the DMU also does not risk over-autonomous actions by the DMU. Furthermore, this section demonstrates that this structure for prohibitions is beneficial for the German system because it is expected to be more effective in regulating digital markets.

63 The PCIs available to the DMU are extensive: aside from prohibitions connected to competition, they comprise data-related prohibitions, including interoperability and defaults intervention, and obligations to provide access to data and to separate collected data.[99] They are proposed to be set out in non-binding guidance to create a fully flexible system to enforce any change short of ownership separation.[100] Their scope is limited by requiring them to be targeted, effective and proportionate to the adverse effect on competition or consumers.[101] In so far as this proportionality test is conducted thoroughly and the data protection-related PCIs are agreed upon in cooperation with the ICO,[102] these broad powers are sufficiently justified to regulate the digital markets.

64 This particularly flexible structure of PCIs is beneficial for the German regulation. Although the suggested PCIs are roughly in line with the German prohibitions, the UK approach is better suited to adapt to new challenges in the digital markets that need to be regulated in the future. However, in order to uphold the legitimacy of the extended powers within the competition law framework, the German system would have to introduce an additional requirement of sufficient connection between the prohibition and competition law.

65 This section showed that the UK approach provides no basis for indications that it might include over-autonomous actions. Furthermore, the German legislator should consider introducing a more flexible prohibition system along the lines of the PCIs in the UK.

3. Comparison of the risks resulting from overlapping application

66 According to the UK proposal, the DMU will be awarded competencies that overlap with those of the following authorities: CMA, ICO, the Office of Communications ("Ofcom") and the Financial Conduct Authority ("FCA").[103] This establishes a risk of overlapping application on similar matters by the DMU and either of these authorities, which might manifest in weakened legal certainty in case the authorities apply different interpretations. However, the Digital Markets Taskforce sets out a comprehensive structure for cooperation between the abovementioned authorities that is likely to create an effective basis to avoid issues of overlapping applicability. The following paragraphs will describe separate aspects of this structure and consider which of these aspects would benefit the German regulation.

67 Firstly, these authorities will be able to share information among them if this information is relevant for their duties.[104] This part is already established in Germany in Section 50f(1) GWB and does not need amending.

68 Furthermore, Ofcom and the FCA are supposed to receive joint powers with the DMU in relation to SMS firms, in which case the DMU should always take the lead.[105] While cooperation under the new regulation between the Bundeskartellamt and telecommunications or financial supervisory authorities has not been discussed at this stage, it might be helpful for future cases. Either way, the decision to make the authority that enforces the *ex ante* regulation the primary authority should be carried over to the German legislation for any matter in which Section 19a GWB will be involved. This would help to avoid situations with unclear decision-making hierarchies.

98 Draft Commission implementing decision pursuant Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom [2021].

99 Taskforce Advice (n 85), para 4.68.

100 Taskforce Advice (n 85), para 4.67. This approach rather aims to offer an alternative to breaking up monopolies, see Greg Ip, 'In Britain, a Middle Way for Reining in Big Tech; Government-Appointed Panel Seeks to Bolster Competition without Invasive Regulation' *Wall Street Journal* (New York, N.Y., 13.03.2019).

101 Taskforce Advice (n 85), para 4.76.

102 Ibid para 4.77.

103 Cf ibid para 6.3.

104 Ibid paras 6.8-6.11.

105 Taskforce Advice (n 85), paras 6.12-6.15.

69 Overlapping powers with the CMA on competition-related conduct by SMS firms also will not be an issue in practice: the location of the DMU within the CMA structure will presumably generate internal arrangements to avoid double investigations with the aim of managing shared resources efficiently. As the new Section 19a GWB is enforced by the Bundeskartellamt itself as German competition authority, this situation does not have to be catered for in Germany.

70 Moreover, the Taskforce suggests that the DMU should always consult with the ICO on compatibility of its planned PCIs with data protection laws.[106] While such consultation is practised without legal foundation in Germany, the German regulation would benefit from mirroring the UK approach on this account and introducing an obligation to consult with data protection authorities before deciding data protection-related matters.

71 The relationship between DMU and ICO is also specified by the proposed competencies for the DMU to refer discovered breaches of data protection laws onto the ICO.[107] These competencies would be useful to increase data protection enforcement without exceeding the limit of supplementary enforcement. However, implementation in Germany is limited by the one-stop-shop mechanism of the GDPR, so that only cases without EU-wide cross border issues or with the LSA located in Germany could potentially be referred on to the German data protection authorities by the Bundeskartellamt. Therefore, this aspect would not improve the German cooperation structure.

72 In short, the Taskforce established a strong cooperation structure which is tailored to the legal environment of the UK and can be expected to succeed in avoiding risks resulting from overlapping applicability. Therefore, although the German regulation would benefit from mirroring the UK structure completely, only two parts can and should be implemented in Germany: making the Bundeskartellamt the primary authority on cases regulating digital markets and introducing a consultation requirement with the relevant data protection authorities for data-related decisions.

E. Comparison with the Digital Markets Act in the EU

73 The application of the GWB amendment through the DMA will be limited in scope by new European legislation and is expected to be adopted soon. In order to assess the consequences that the DMA will have on the functioning of Section 19a GWB, this chapter will first analyse its compatibility with the German approach in the areas of competition law and data protection law as well as the enforcement of the new regulations against large online platforms. Following this will be a comparison of the DMA to the German and UK approaches on the basis of the findings in the previous comparison.

I. The Digital Markets Act

74 The DMA has initially been inspired by the first steps taken in the UK towards a new legislation directed specifically at large online platforms and services but has undergone extensive change since then.[108] While the first proposal was only published on 15 December 2020,[109] the DMA has by now been unanimously adopted by the Council of the EU in the third and final reading, with only the adoption by the European Parliament outstanding.[110] This adoption relates to the latest version of the DMA published on 11 July 2022 with significant changes to the initial proposal.[111] For clarification, this version will be referred to in this discussion as "DMA" and the initial proposal as of 15 December 2020 as "DMA proposal".

75 Once adopted, this regulation will provide the Commission with additional powers in dealing with

106 Ibid para 4.77.

107 Ibid para 5.7.

108 This inspiration is indicated in the following expert study by demonstrating the similarities of the UK approach with the 'New Competition Tool' (NCT) which has now been partly incorporated into the DMA: Heike Schweitzer, 'The New Competition Tool: Its institutional set up and procedural design' (2020) <https://op.europa.eu/en/publication-detail/-/publication/1851d6bb-14d8-11eb-b57e-01aa75ed71a1>; see also Maik Wolf, in *Münchener Kommentar zum Wettbewerbsrecht* (4th edn, CH Beck 2022), section 19a para 97.

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

110 Council of the European Union, 'Voting result [on the] Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' 2020/0374 (COD), ST 11507 2022 INIT, 18.07.2022.

111 Council of the European Union, 'Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' 2020/0374 (COD), PE 17 2022 INIT, 11.07.2022.

the most influential providers of core platform services, the so-called gatekeepers, and their commercial relations with businesses and consumers on digital markets.[112] Its structure is similar to that of the German and UK approaches in so far as it also consists of two steps. First, the Commission will designate undertakings for gatekeepers in accordance with qualitative and quantitative factors set out in Article 3 of the DMA. Subsequently, these gatekeepers will be subject to the obligations listed in Articles 5–7 DMA. These obligations can be enforced by the Commission with fines of up to 10% of the undertakings' total worldwide turnover pursuant to a decision of non-compliance with these obligations and up to 20% of their turnover for repeated non-compliance.[113] Aside from various competition related obligations, the proposal also takes into account data protection in particular. This includes obligations to refrain from combining and cross-using personal data from end users collected via different services without consent in Article 5(2) (b) and (c) DMA and obligations for certain services for interoperability pursuant to Article 7 DMA.

II. Compatibility with European national frameworks

76 Due to the interlaced relationship of the German and European jurisdictions, the scope of application of the GWB amendment is dependent on its compatibility with the new DMA. The first chapter will address this compatibility and explain how Section 19a GWB will likely still be broadly applicable parallel to the DMA and beyond it, despite some inevitable restrictions and unresolved issues. The second chapter will determine the compatibility of the DMA with other legal fields touched by it, exemplified by the DMA's relationship with national data protection authorities. It will show a number of shortcomings in terms of the cooperation structure and consider their solutions in practice. The third chapter will argue that the success of the DMA itself is dependent on its enforcement in cooperation with national competent authorities ("NCAs"), which has not been extended as widely as it could have been in order to be more efficient.

1. Compatibility of the DMA with Section 19a GWB

77 The DMA has been developed in the form of a European regulation and will therefore be directly applicable in all Member States as per Article 288(2) (2) TFEU.[114] It follows that, once adopted, the DMA will enjoy primacy of application as the stricter law over the German legislation including section 19a GWB.[115] In order to determine the potential remaining impact of the GWB amendment on digital platforms after the enforcement of the DMA, it is therefore necessary to analyse its compatibility with the new EU legislation.

78 To start with, Article 1(5) DMA prohibits the enforcement of national legal obligations on gatekeepers that would exceed those available to the Commission under Articles 5-7 DMA "for the purpose of ensuring contestable and fair markets". As mentioned above, competition law is generally aimed at maintaining competition in the markets for the benefit of consumers.[116] This aim also lies at the heart of Section 19a GWB by way of imposing additional prohibitions on undertakings with PSC.[117] As Section 19a GWB has a similar purpose as the DMA, it would initially be blocked in its entirety by Article 1(5) DMA.

79 However, Article 1(6) DMA sets out three exceptions for national competition rules. One of these is Article 1(6)(b) DMA for national competition measures prohibiting unilateral conduct by gatekeepers insofar as they enforce obligations that go beyond those imposed under the DMA. In line with Recital 10 DMA, this exception is aimed at traditional competition law regulations prohibiting abusive conduct by way of individualised assessments. The Bundeskartellamt will thus at least remain competent to apply Section 19 GWB to undertakings irrespective of their status as gatekeeper under the DMA. Whether Section 19a GWB can be applied within the scope of this exception, however, is less straightforward. It would need to satisfy the following requirements: (i) Section 19a GWB has to be regarded a competition law rule, (ii) it needs to target unilateral conduct, and (iii) it has to impose further obligations on gatekeepers.

112 Cf. Jürgen Basedow, 'Das Rad neu erfunden: Zum Vorschlag für einen Digital Markets Act' (2021), 1 <https://papers.ssrn.com/abstract=3773711>.

113 Articles 29, 30 of the DMA.

114 Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C-115/47.

115 Rehbinder, in Ulrich Immenga and Ernst-Joachim Mestmäcker (eds), *Wettbewerbsrecht* (6th edn, CH Beck 2020), section 22 GWB para 18.

116 Grothe (n 73), Buiten (n 75).

117 Government Draft (n 23), 75; Wolf (n 108), section 19a para 1.

a) Competition law rule

80 It remains in dispute whether Section 19a GWB should be considered part of competition law or, instead, of the general regulatory law. Competition law is generally understood to protect existing competition from collusion and abusive conduct by way of prohibiting individual conduct. Regulatory law in turn aims to break up more or less closed networks in specific sectors to create a basis for competition through more intense proactive measures.[118] On the one hand, Section 19a could be located within regulatory law due to its *ex ante* approach; since this regulation does not always require proof of practices that distort competition but can be applied prior to any such consequences, it might not be sufficiently linked to the aim of safeguarding competition but be classified as proactive. In addition, the individual investigation of an undertaking only focusses on its PSC status irrespective of any actual misconduct as basis for prohibitions.[119] On the other hand, it can be argued that Section 19a GWB has the character of competition law since prohibitions will only be imposed on an individual basis at the discretion of the Bundeskartellamt, following thorough investigations into the conduct of an undertaking and its threat to competition.[120] This point is reinforced by the location of this section within the GWB in the chapter on market dominance and by its parallels to the market dominance test in Section 18 GWB, especially Section 18(3a) GWB, and to the detrimental effects listed in Section 19(2) GWB.[121] These parallels are also indicated in the Government Draft on the Tenth GWB amendment in determining that conduct prohibited under Section 19a(2) GWB may in some cases also be prohibited under Sections 19, 20 GWB.[122] In addition, Section 19a GWB is not confined to a specific sector but constitutes an extension to the tools available to combat market abuse.[123] Accordingly, while Section 19a GWB shows some traits of regulatory law, it can still be firmly placed within the competition law framework and satisfies this requirement under the exception in Article 1(6) DMA.

b) Unilateral conduct

81 That Section 19a GWB is aimed at prohibiting unilateral conduct is already evident in its structure; the Bundeskartellamt needs to investigate one undertaking at a time in order to declare it to have PSC and must subsequently be subject to the prohibitions in Section 19a(2) GWB. It therefore only addresses conduct demonstrated by the undertakings themselves as opposed to unlawful cooperation with other undertakings.

c) Imposing further obligations on gatekeepers

82 Section 19a GWB needs to impose obligations on the targeted gatekeepers that go beyond those imposed under the DMA. From the wording in Article 1(6)(b) DMA ("imposition of further obligations") it remains unclear whether a rule only falls under this exception if it provides for obligations that are not covered by the DMA or whether a rule can already apply under this exception if it merely imposes obligations that could be imposed by the Commission at a later point of time but have not yet been initiated against the respective gatekeeper under the DMA. The former interpretation would require a detailed comparison of the scope of prohibitions in Section 19a(2) GWB and Articles 5-7 DMA. Due to the broadly similar prohibitions available under both regulations, this would result in a very limited scope of application left for Section 19a GWB. However, Recital 10 of the DMA provides the crucial detail in the following phrase: "the application of [national competition] rules should not affect the obligations imposed on gatekeepers under this Regulation" (emphasis added). On this basis, the latter interpretation can be followed, permitting national competition law authorities to enforce any obligations against gatekeepers as long as they have not yet been imposed under the DMA.

118 Franz Jürgen Säcker, 'Das Verhältnis von Wettbewerbs- und Regulierungsrecht' (2015) EnWZ 531, 532.

119 Wissenschaftliche Dienste des Deutschen Bundestags, 'Die Anwendbarkeit von § 19a GWB im Lichte des europäischen Gesetzgebungsverfahrens zum „Digital Markets Act"' (07.01.2022) WD 7 - 3000 - 114/21; PE 6 - 3000 - 067/21, 13 <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwj4_vrB37T5AhXMCewKHcYnCh0QFnoECAMQAQ&url=https%3A%2F%2Fwww.bundestag.de%2Fresource%2Fblob%2F880748%2F856d83cb24c61822c508aa47f27e18e7%2FWD-7-114-21-PE-6-067-21-pdf-data.pdf&usg=AOvVaw0Gy0SADi2TIrAOjHBChH66>.

120 Wissenschaftliche Dienste des Deutschen Bundestags (n 119); Florian Haus and Anna-Lena Weusthof, 'The Digital Markets Act - a Gatekeeper's Nightmare?' (2021) WuW 318, 324f; Rupprecht Podszun, 'Competition in the digital economy: What next after the Digital Markets Act? Statement for the Economic Committee of the German Bundestag' (2022), 9 <https://ssrn.com/abstract=4096357>.

121 Haus and Weusthof (n 120), 324.

122 Government Draft (n 23), 78.

123 Wolf (n 108), section 19a para 97.

83 It follows therefore that Section 19a GWB is covered by the exception in Article 1(6)(b) DMA and can continue to be applied to gatekeepers both before the Commission imposes specific obligations on them and afterwards insofar as the obligations then go beyond those enforced by the Commission. Nevertheless, due to the ongoing dispute regarding the character of Section 19a GWB and the interpretation of Article 1(6)(b) DMA, the actual scope of application of the German regulation is not legally settled and therefore likely to be subject to court rulings in the future.[124]

84 However, even if future court rulings would curtail the scope of application of Section 19a GWB beyond the scope determined above, this norm would still remain relevant for three reasons. Firstly, the GWB already has and will continue to play an important role in collecting information and experience in the sphere of regulating large online platforms until the DMA will start applying.[125] Secondly, the scope of application of Section 19a GWB goes beyond that of the DMA with regard to the designation process. Aside from the potential gatekeepers in accordance with the DMA, Section 19a GWB may extend to (a) local companies, as it does not require any impact on the internal market, (b) companies that are active in the digital sphere but do not provide core platform services in line with the definition in article 2(2) DMA, and (c) companies below the indicative quantitative thresholds due to its sole reliance on flexible criteria.[126] Even though these extensions would not cover the main addressees of this regulation, they could still have an impact on companies in the periphery. Thirdly, Section 19a GWB would eventually rise in importance by way of its flexibility in a situation in the future where the inflexible requirements listed in Articles 5-7 DMA would be fully enforced.

85 On a separate note, this interpretation leads to the following question: what happens if the Commission decides to impose an obligation on a gatekeeper after a national authority has already imposed a similar obligation on the gatekeeper within its jurisdiction? Technically, this obligation should not be necessary anymore as the undertaking should have already complied with the obligation. But if the obligation has not yet been fulfilled, the undertaking might now face two potential sanctions. The topicality of this issue becomes apparent in the following example. Irrespective of the fact that the case was based on Section 19 GWB instead of Section 19a GWB, as both sections have been demonstrated to be covered by the exception in Article 1(6) DMA, a final court ruling against Meta, formerly Facebook, in the abovementioned Facebook case might impose obligations similar to those in Article 5(2)(b) DMA on this undertaking. If, following such a decision, the Commission decided to regulate Meta as gatekeeper with regard to the same issue, it would remain unclear on the basis of the DMA whether Meta would face additional sanctions.[127]

86 There is a fundamental principle in EU law, called *ne bis in idem*, which is enshrined in Article 50 of the Charter of Fundamental Rights[128] ("Charter") and protects everyone from repeated punishment for the same offence in criminal proceedings in the EU. The term "criminal" has been interpreted broadly and is recognized to also cover competition law proceedings.[129] On this basis, the enforcement of sanctions by the German court and the Commission in the above example could infringe Article 50 of the Charter if all conditions were satisfied. Until recently, the CJEU had applied a narrow scope of this principle in competition law by requiring not just the same offender and the same facts but also the same offence in order to find that duplicate proceedings infringed this principle. As an offence committed under two different legislations is almost always determined to be different, this principle would not have been of significance in situations similar to the above.[130] However, in two recent CJEU decisions, *bpost*[131] and *Nordzucker*,[132] the CJEU has established and confirmed a more lenient approach, demanding only the accordance of offender and facts, thus making this principle relevant for future DMA applications. It will nevertheless remain difficult to demonstrate that the duplicate proceedings cannot be justified: the first requirement for this justification, that duplicate proceedings are provided by law, can be justified due to the exception in Article 1(6) DMA that it applies without prejudice to national competition law. In order to refute the second

124 Wissenschaftliche Dienste des Deutschen Bundestags (n 119), 14f.

125 The German government laid down its intentions on this point in the Resolution Recommendation (n 26), 10.

126 Cf. Podszun (n 120), 10.

127 Basedow (n 112), 6-7.

128 Charter of Fundamental Rights of the European Union [2012] OJ C-326/02.

129 See Case C-501/11 *Schindler* [2013] ECLI:EU:C:2013:522.

130 Dimitrios Katsifis, 'Ne bis in idem and the DMA: the CJEU's judgments in bpost and Nordzucker – Part I' (The Platform Law Blog, 28.03.2022) <https://theplatformlaw.blog/2022/03/28/ne-bis-in-idem-and-the-dma-the-cjeus-judgments-in-bpost-and-nordzucker-part-i/>.

131 Case C-117/20 *bpost* [2022] ECLI:EU:C:2022:202.

132 Case C-151/20 *Nordzucker* [2022] ECLI:EU:C:2022:203.

requirement, that both proceedings must pursue complimentary instead of coincidental aims, the court would likely need to deviate in the specific case from the characterization of the DMA as regulatory instead of competition law.[133] And the basis to satisfy the third requirement of proportionality and coordination between both proceedings has recently been introduced in Article 38(1) DMA in the form of a new cooperation mechanism for national competition authorities.[134] This shows that the outcome of a case will particularly depend on the evaluation of the aims and extent of cooperation in the application of the DMA.

87 Due to these uncertainties regarding the new scope of the *ne bis in idem* principle, it is expected that the entry into force of the DMA will provide the courts with lots of new litigation. This is the case despite the fact that related issues have already been resolved within competition law regarding the relationship between the competencies of the Commission and NCAs.[135] Therefore, further legislative work would be beneficial to resolve the aforementioned issues.

88 That said, the current framework should be able to function in the majority of cases despite these issues, due to a crucial and broadly welcomed amendment to the DMA; unlike the initial DMA proposal, the new version of the DMA provides for a so-called high-level group in Article 40 DMA.[136] This group will consist of up to 30 representatives from a list of European bodies and networks in the areas of electronic communication regulation, data protection, competition, consumer protection and media regulation. It should meet regularly with the Commission in order to provide the Commission with advice on how to enforce the DMA in its areas of expertise with the aim to create a consistent regulatory approach. In particular, this group should report on any potential trans-regulatory issues between the EU and national level regulation pursuant to Article 40(6) DMA. If this group is sufficiently engaged with these processes, well-staffed and kept up-to-date on all levels, it could mitigate the issue described above by actively coordinating the investigations and workstreams which the authorities involved are working on. This is all the more likely as no authority should rationally have any interest in engaging in legal struggles with each other and thereby prolonging the imposition of prohibitions on gatekeepers. In addition, the abovementioned new Article 38(1) DMA sets out that the Commission and NCAs enforcing competition law are supposed to cooperate through the European Competition Network ("ECN") or alternative arrangements and have the power to exchange even confidential information. On this basis, the abovementioned issues should be very unlikely to occur in practice.

2. Compatibility of the DMA with national data protection authorities

89 The new competencies transferred to the Commission under the DMA touch on a number of different areas of law. These include, in particular, those areas of with bodies and networks are participating in the high-level group, as listed in the previous paragraph. This sub-chapter will discuss one of the issues arising from this overlap: the compatibility of the DMA with national data protection authorities.

90 These authorities derive their competencies from directly applicable EU law, as the GDPR is mainly enforced on a national level. Therefore, the competencies are not overruled by the application of the DMA. In addition, even separate national competencies would not likely be prohibited by Article 1(5) DMA, as data protection rules are not enforced "for the purpose of ensuring contestable and fair markets", and because they are not connected to any gatekeeper status. It is also unlikely that actions by data protection authorities would be caught under Article 1(7) DMA, which prohibits decisions that run counter those adopted under the DMA. This is because decisions to improve data protection usually benefit the increase of fairness on the market as well, as indicated by the number of data protection-related obligations in Articles 5-7 DMA. Therefore, similar tensions could arise as those described above regarding competition law, when the Commission imposes an obligation on a gatekeeper which has previously been enforced by a data protection authority.

91 Similar to the previous section, this issue might be resolved in practice through the new high-level group under Article 40 DMA, in addition to a high-level cooperation assurance for NCAs in Article 37 DMA. The legislators seem to have at

133 For example, this characterization is indicated in recital 10 DMA; see also Giorgio Monti, 'The Digital Markets Act – Institutional Design and Suggestions for Improvement' (2021), 14 <https://ssrn.com/abstract=3797730>.

134 Dimitrios Katsifis, 'Ne bis in idem and the DMA: the CJEU's judgments in bpost and Nordzucker – Part II' (*The Platform Law Blog*, 29.03.2022) <https://theplatformlaw.blog/2022/03/29/ne-bis-in-idem-and-the-dma-the-cjeus-judgments-in-bpost-and-nordzucker-part-ii/>.

135 Basedow (n 112), 7.

136 See for example Damien Geradin, 'The leaked "final" version of the Digital Markets Act: A summary in ten points' (*The Platform Law Blog*, 19.04.2022) <https://theplatformlaw.blog/2022/04/19/the-leaked-final-version-of-the-digital-markets-act-a-summary-in-ten-points/>.

least incorporated part of the recommendations published by the European Data Protection Supervisor ("EDPS") regarding the development of structured cooperation between the Commission and the relevant authorities.[137] Nevertheless, the implementation of these recommendations fell short of actual obligations for information exchange and consultations throughout investigations and assessments which would have created complementary roles.[138] Instead, the competencies of the new high-level group will be limited to the provision of advice and expertise to the Commission while the information collected within the powers in the DMA remains limited to be applied under this regulation only, as per Article 36(1) DMA. Thus, any cross-authority cooperation arrangements regarding information exchange are prohibited. This prohibition might likely lead to other authorities requiring extra resources to investigate the same matter, which could have been spent on other cases in the interest of the citizens. The prohibition on information exchange could even result in incoherent decisions on the basis of varying findings within the repeated investigation. Nevertheless, in practice it is likely that amicable coordination meetings by the high-level group will present a practical solution in such cases and should help the system run sufficiently and smoothly despite the creation of a theoretically difficult and legally uncertain situations regarding competencies and consequences.

3. Cooperation of the Commission with national competent authorities on enforcement

92 Irrespective of the abovementioned compatibility issues, the DMA will only be successful in improving the digital markets if it is able to enforce the vast number of obligations efficiently against all previously designated gatekeepers. The limitation of the designation to three years at a time in Article 4(2) DMA should make efficiency the priority in the enforcement system of the DMA. In light of this, the Commission has already announced that it will be hiring additional staff and organise them in teams around "thematic domains" for increased efficiency and expertise.[139] Nevertheless, given the size of the potential gatekeepers and the detailed investigations necessary for each designation and effective enforcement of each obligation, it is likely that the additional staff will not suffice.[140]

93 Against this backdrop, many voices have suggested the establishment of a cooperation framework with NCAs to help enforce this extensive new regulation, one of them being the Bundeskartellamt,[141] in agreement with the ECN.[142] But no such legal basis has been added to the DMA since. The only possibility for NCAs to get involved is by launching investigations on gatekeepers and their non-compliance with the obligations in Article 38(2), (7) DMA. But instead of acting upon the results of such an investigation, the NCAs are required to pass on the information to the Commission, losing all influence on the application of this information against the undertakings concerned. Therefore, it is viewed with scepticism if this mechanism will be applied by NCAs, as they would be expected to use their resources for own projects and investigations.[143]

94 The reasons for the legislator's refusal to include NCAs any further down the line include the increase of efficiency by way of organising the whole process in one hand without delays through information exchange and approval requirements,

137 EDPS, 'Opinion 2/2021 on the digital markets act' (10.02.2021), para 40.

138 Ibid para 41.

139 Thierry Breton, 'Sneak peek: how the Commission will enforce the DSA & DMA' (*LinkedIn*, 05.07.2022) <https://www.linkedin.com/pulse/sneak-peek-how-commission-enforce-dsa-dma-thierry-breton/>.

140 On the need for additional staff and expertise see an open letter signed by the Bureau Européen des Unions de Consommateurs (BEUC), the Federation of German Consumer Organisations and 16 others, 'Resources to ensure effective enforcement of the Digital Markets Act' (27.06.2022) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-068_open_civil_society_letter_-_resources_to_ensure_effective_enforcement_of_the_dma.pdf>.

141 Bundeskartellamt 'Digital Markets Act: Perspektiven des (inter)nationalen Wettbewerbsrechts' (07.10.2021), 37ff <https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Diskussions_Hintergrundpapier/AK_Kartellrecht_2021_Hintergrundpapier.html?nn=3590858>.

142 ECN, 'Joint paper of the heads of the national competition authorities of the European Union: How national competition agencies can strengthen the DMA' (22.06.2021) <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiE-aa8ubT5AhWLr6QKHTtuA_AQFnoECAIQAQ&url=https%3A%2F%2Fec.europa.eu%2Fcompetition%2Fecn%2FDMA_joint_EU_NCAs_paper_21.06.2021.pdf&usg=AOvVaw3MLbJg3Pkf2GsQyRHNdkZs>.

143 Alexandre de Streel and others, 'Making the Digital Markets Act more resilient and effective' (*CERRE*, 26.05.2022), 76 <https://cerre.eu/publications/european-parliament-digital-markets-act-dma-resilient-effective/>; Geradin (n 136).

and a costly cooperation network.[144] But due to the fact that the Commission will likely remain relatively understaffed, these efficiency losses through procedural delays would not be outweighed by efficiency gains from shared enforcement competencies. NCAs are also not intended to be involved in this process in order to avoid the development of an atmosphere of competition between the Commission and NCAs.[145] However, these issues could be better avoided through enhanced cooperation procedures. The exclusion of NCAs from this area of enforcement might even fuel competition as NCAs either have to be faster in their regulation of gatekeepers than the Commission or they have to be creative to find new ways for achieving their goals when getting impatient with the predictably busy Commission. The only reason that cannot be denied is the upholding of thorough harmonisation not just of the applicable set of rules, as set out in Article 1 DMA, but also of the process and decisions, especially since most gatekeepers are active within the whole EU.[146] Nevertheless, a lack of harmonisation could be reasonably mitigated by way of more tightly knit cooperation procedures. This has also been demonstrated by the functioning system of parallel enforcement between EU and NCAs in competition law.[147] It therefore would still be preferable for the legislators to include the NCAs in the enforcement framework.[148]

III. Comparison of the DMA with the German and UK approach

95 The following comparison, based on the topics and findings of the comparison between the German and UK approach, aims to further inform the German approach on possible improvements while also pointing out potential amendments that would be beneficial to the not yet adopted DMA. However, keeping in mind the different preconditions for national legislation compared to EU legislation, the DMA will not provide many recommendations for the German approach, as some potentially beneficial aspects cannot be carried over onto the national level and others would not fit into the flexible framework selected by the German legislator.

1. Comparison of the designation processes

96 Due to the similar two-step structure of all three approaches, the designation process in the DMA is directly comparable. Nevertheless, the EU legislation has developed a more complex method with several alternative designation paths. For the comparison, this process will be divided into the following three parts which are in turn considered below: (i) the three main requirements listed in Article 3(1) DMA, (ii) the three quantitative thresholds set out in Article 3(2) DMA and (iii) the list of elements in Article 3(8)(2) DMA.

97 Prior to that, it is worth noting that unlike the other approaches, the DMA expects undertakings to initially notify the Commission themselves in order to avoid a thorough market investigation. This requirement could increase efficiency, but would likely only be used by undertakings that are certain that their gatekeeper status is unavoidable. These undertakings in turn could probably be easily determined by the Commission anyway. Therefore, the efficiency gains from this initial requirement are limited and would not be sufficiently beneficial to be recommended to the other jurisdictions.

a) Main requirements, Article 3(1) DMA

98 The main requirements of Article 3(1) DMA require significant impact on internal markets, the provision of core platform service as important gateway for users and an entrenched and durable position. The internal market requirement is unique to the EU and therefore beyond consideration for other frameworks. Instead, the entrenchment requirement is similar to the UK approach and should likewise be recommended to the German approach to avoid stalling innovation by putting new and recently growing undertakings at risk of designation.

99 The requirement on the provision of an important core platform service is similar to the UK requirement insofar as it goes beyond the requirement of multi-sided platforms as applied in Section 19a GWB and thereby reasonably narrows the scope of this regulation to the intended type of undertaking. At the same time, the conclusive list of services covered

144 Cf. de Streel (n 143), 75.

145 Laura Kabelka, 'Umsetzung des DMA könnte in Deutschland zu Rechtsunsicherheit führen' (*EURACTIV.de*, 11.04.2022) <https://www.euractiv.de/section/innovation/news/umsetzung-des-dma-koennte-in-deutschland-zu-rechtsunsicherheit-fuehren/>.

146 Monti (n 133), 5, 17.

147 Cf. Justus Haucap and Heike Schweitzer, 'Revolutionen im deutschen und europäischen Wettbewerbsrecht' (2021) WRP 2021 issue 7, I <https://www.ruw.de/suche/pdf/wrp/wrp-07-2021-i-efa3cbbb1e3235af4f1c66f46b97100d.pdf>.

148 For additional arguments see Bundeskartellamt (n 141), ECN (n 142) with further references.

by the term "core platform service", set out in Article 2(2) DMA, avoids an issue faced by the UK definition on whether only digital platforms or any activities on digital markets are included.[149] Nevertheless, while the list comprehensively includes all services that appear significant for this framework at the current moment, it is an inflexible term potentially limiting the scope of this regulation in the future. Therefore, it would not be recommended for the German legislation to adopt a similar list in a binding manner in order to retain its flexibility. At the same time, this specific list does not particularly hinder the EU legislation from achieving its goals. It rather is an example of how the European legislator has decided to base the DMA structure with an emphasis on predictability, while both the UK and German approach are leaning more towards flexibility and time-resilience of their framework.[150]

b) Quantitative thresholds, Article 3(2) DMA

100 The quantitative thresholds of Article 3(2) DMA, which include annual turnover, number of active users and maintaining this number of users over the last three years, could be favourable compared to the German and UK approaches by providing the EU designation process with a level of objectivity and thereby increasing legal certainty and predictability. On the other hand, the fact that only satisfying the quantitative thresholds places the burden on the undertakings to show that they nevertheless do not satisfy the qualitative requirements under Article 3(5) DMA could be problematic because the size of an undertaking is not in itself informative of the importance of the respective core platform service on the market.[151] While the DMA proposal had provided for a rebuttal system which allowed undertakings to refute the presumption with reference to the list of elements which is now found in Article 3(8) DMA, this process has now been changed for the worse. According to Recital 23 DMA, designated undertakings may only rebut the Commission's presumption by taking into account elements directly linked to the quantitative criteria. These additional elements could still not help reliably determine the importance of the core platform service within the undertaking or the market. If applied in accordance with Recital 23, this approach will likely lead to over-inclusion.[152] Therefore, this approach is not beneficial even to the predictability-based EU framework and should not be considered in the German system.

c) List of elements, Article 3(8)(2) DMA

101 This list of elements from Article 3(8)(2) DMA is to be taken into consideration in a market investigation pursuant to Article 17 DMA, in case any of the quantitative thresholds are not satisfied. This includes, *inter alia*, elements on size, number of users, network effects, scale and scope effects, user lock-in, conglomerate corporate structure and other structural characteristics. There is a striking similarity to the German designation factors under Section 19a(1)(2)(2)-(5) GWB. Nevertheless, due to the fact that both of the other jurisdictions do not rely on quantitative criteria and are solely based on investigation procedures by the authorities instead of notification requirements, there is no need for additional elements of this type.

102 In short, the complex designation system with different routes could render the process more predictable in some ways but does not appear necessary or recommendable to national jurisdictions. In particular, this system would not provide other jurisdictions with additional benefits as it does not limit the application to the handful of largest online platforms, as was expected during the legislation process, but is intended to be extended to about 15 companies.[153]

149 While the recent CMA Market Study only covered digital platforms, the Taskforce Advice (n 85) in para 6 does not refer exclusively to platforms and therefore appears to propose the latter. This would considerably broaden the scope of applicability for the DMU powers since a rising number of businesses from different sectors is active in the digital markets. On this point, see Kiran Desai, 'The CMA's Report, Online Platforms and Digital Advertising, In Context' (2020) CoRe 210, 213-215.

150 Thomas Tombal, 'Ensuring contestability and fairness in digital markets through regulation: a comparative analysis of the EU, UK and US approaches' (2022), 32f <https://www.tandfonline.com/doi/full/10.1080/17441056.2022.2034331>.

151 Damien Geradin, 'One needed area of improvement for the Digital Markets Act: The designation of gatekeepers' (*The Platform Law Blog*, 10.01.2022) <https://theplatformlaw.blog/2022/01/10/one-needed-area-of-improvement-for-the-digital-markets-act-the-designation-of-gatekeepers/>.

152 Geradin (n 136).

153 Christina Caffarra and Fiona Scott Morton, 'The European Commission Digital Markets Act: A translation' (*Voxeu*, 05.01.2021) <https://voxeu.org/article/european-commission-digital-markets-act-translation>.

2. Comparison of the scope of autonomous actions by the authorities

103 The Commission generally does not risk acting over-autonomously as the European legislator can grant it the necessary competencies. In addition, unlike the non-binding list in the UK on types of conduct that may be prohibited at the DMU's discretion, the DMA leans towards the German approach by having established a pre-defined and inflexible list of prohibited conduct. The actions by the Commission against gatekeepers are therefore more predictable, not only for companies but also for other authorities. Accordingly, the DMA is in no risk of permitting over-autonomous actions but also could not be replicated in Germany due to the EU's characteristics.

3. Comparison of the risks resulting from overlapping application

104 Due to its similarity with the German and UK approach, the DMA also awards the Commission competencies that will create an overlap with other authorities. These authorities are identified in the list of components for the new high-level group in Article 40(2)(a)-(e) DMA. For example, this includes the European data protection authorities due to the abovementioned regulations in the data protection field like limitations to data collection or use and the new Article 7 DMA on inter-operability. In addition, the overlap extends to NCAs which would usually enforce EU regulations like the GDPR. This is exemplified in a remark that the Commission is now able to rule on certain data issues by itself in order to avoid a blockade through slow enforcement by the IDPC.[154] Although this possibility could be claimed as a positive outcome, these new powers generally undermine the competencies previously handed to NCAs and at the same time risks overlapping and contradictory decisions.

105 While this issue could practically be solved again by pointing to the high-level group in Article 40 DMA, the cooperation regulations outside the competition law field remain insufficient. This is particularly clear when compared to the rules in the UK which determine the DMU as main coordinator in its field while setting up structures for regulated cooperation with each involved agency. However, a coordination system as thorough as this one could not be implemented as easily on the EU level due to the need to coordinate authorities in 27 Member States. Thus, the high-level cooperation is a reasonable compromise. Nevertheless, the very limited basis for information exchange set out above would benefit particularly from an expansion, and obligatory consultation requirements would also be welcome for certain authorities, like the UK has established for the ICO. There might also be situations in which overlaps with other EU regulations cause incoherent decisions, in particular those regulations listed in Recital 12 DMA that are applicable per se without prejudice to the DMA. However, a detailed consideration of such overlaps goes beyond the scope of this discussion as it would not provide new insights for the improvement of the German legislation. In practice it remains likely that these possible overlaps will be solved amicably because all involved authorities are expected to pull in the same direction and should therefore be interested in thorough cooperation. Nevertheless, this paragraph has demonstrated that the DMA does not provide any suggestions on how to avoid overlapping applications in the German legislative framework.

F. Conclusion and summary of recommendations

106 The new Section 19a GWB succeeded in removing the doubts that have been raised in response to the Facebook case regarding the application of data-related principles in competition law. It dispelled risks arising from over-autonomous applicability and overlapping application by both spheres of law. However, the legitimacy of applying these new powers is drawn into question because the wording of the regulation does not sufficiently limit the scope of firms addressed by it.

107 In search of improvements for this new regulation, the comparison with the UK approach and the DMA currently under development resulted in the following list of recommendations that should be incorporated in the current German legislation in order to improve its effectiveness and legitimacy:

a) Designation requirements

108 The scope of designation should be limited in order to avoid over-inclusiveness by supplementing it with three strict requirements. The regulation should require the firms to have market dominance in at least one of the digital markets it is involved in. The entrenchment criteria proposed by the UK approach and incorporated in the DMA should be adopted. And the limitation of the scope of application to firms that are active on digital markets as opposed to non-digital markets should be formulated unambiguously.

154 Irish Council for Civil Liberties, 'Remarks by Johnny Ryan at the CRA "Disrupted Times" Conference in Brussels' (*ICCL*, 04.04.2022) <https://www.iccl.ie/2022/remarks-by-johnny-ryan-at-the-cra-disrupted-times-conference-in-brussels/>.

b) Types of prohibitions

109 The prohibitions that are enforceable against designated companies should be determined in a more flexible manner in order to improve the effectiveness of the legislation in regulating digital markets within the limits of autonomy available to the Bundeskartellamt. The new types of prohibitions available to the Bundeskartellamt should be set out and kept up to date in non-binding guidance, mirroring the UK approach on PCIs. The new structure should differ from the UK proposal only by introducing an additional requirement regarding a connection to competition law. This would also help Section 19a GWB in regaining a broader scope of application beyond the DMA after its entry into force.

c) Strong cooperation

110 The extent of cooperation between the involved authorities set out in the legislation should be extended by two requirements in order to avoid the risk of overlapping application which could result in weakened legal certainty. In investigations under Section 19a GWB by the Bundeskartellamt that also touch areas which are regulated by other authorities, the German legislator should make it compulsory for the Bundeskartellamt to consult with those authorities in advance of a decision. This is in line with the UK approach regarding cooperation with the ICO. The Bundeskartellamt should also be empowered to take the lead in deciding these cases while cooperating with other authorities.

111 Although it would be recommended for the German legislator to draft a new amendment soon to incorporate the abovementioned aspects, the political reality has to be accounted for. The proposed DMA, which will significantly reduce the scope of application of the new German legislation, as set out above, is expected to enter into force in the near future and possibly start applying in 2023.[155] Until then, the German regulation will primarily gather practical experience with the regulation in its current shape instead of drafting an amendment on the basis of theoretical discourse. To this end, the Bundeskartellamt has already initiated proceedings on the basis of the new regulation against Facebook and Oculus,[156] Amazon,[157] Google,[158] and Apple.[159]

112 Against this backdrop, instead of waiting for a new legislative amendment, the Bundeskartellamt and involved courts should implement some of the recommendations by way of interpreting the regulation accordingly in their decisions. In this way, the entrenchment, market dominance and digital market criteria should be read into the legislation in order to provisionally compensate the legitimacy issues. Regarding the scope of prohibitions, it is sufficient to interpret them reasonably broadly to fit upcoming cases. The proposed cooperation principles should be detailed as theoretically non-binding but practically obligatory guidance either in a judgment or in a publication by the authorities.

113 To conclude, whilst several aspects of the German regulation in Section 19a GWB need to be improved, the German legislator took an important step towards regulating digital markets more effectively by publishing the first regulation worldwide that directly targets large online platforms. This discussion explained that the German legislator succeeded in applying the lessons learned from the Facebook case regarding the limits of traditional competition law against data-related concerns. It further discussed some remaining issues of the regulation and recommended strategies for improvement. These recommendations may also serve as a starting point for other jurisdictions in drafting similar regulations, in addition to further inter-jurisdictional exchange

155 Natasha Lomas, 'EU's new rules for Big Tech will come into force in Spring 2023, says Vestager' (*TechCrunch*, 05.05.2022) <https://techcrunch.com/2022/05/05/digital-markets-act-enforcement-margrethe-vestager/>.

156 Bundeskartellamt, 'First Proceeding Based on New Rules for Digital Companies – Bundeskartellamt also Assesses New Section 19a GWB in its Facebook/Oculus Case' (28.01.2021) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/28_01_2021_Facebook_Oculus.html>.

157 Bundeskartellamt, 'Proceedings against Amazon based on new rules for large digital companies (Section 19a GWB)' (18.05.2021) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/18_05_2021_Amazon_19a.html>.

158 Bundeskartellamt, 'Proceeding against Google based on new rules for large digital players (Section 19a GWB) – Bundeskartellamt examines Google's significance for competition across markets and its data processing terms' (25.05.2021) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/25_05_2021_Google_19a.html>; Bundeskartellamt, 'Bundeskartellamt examines Google News Showcase' (04.06.2021) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/04_06_2021_Google_Showcase.html>.

159 Bundeskartellamt, 'Proceeding against Apple based on new rules for large digital companies (Section 19a(1) GWB) – Bundeskartellamt examines Apple's significance for competition across markets' (21.06.2021) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2021/21_06_2021_Apple.html>.

and the collection of practical experience. The discussion also established the continuing significance of Section 19a GWB after the entry into force of the DMA and the overall compatibility of this European approach by way of practical solutions based on a new coordination group. Insofar as the enforcement of the DMA will not be slowed down due to resource issues or extensive litigation, these two approaches have a good chance of making a real impact on the digital market. And maybe they will even succeed in creating another Brussels effect, following the GDPR, by "exporting" the idea of this type of regulation for large online platforms around the world. Overall, these developments promise to lead to an effective and legitimate legislative tool to regulate large online platforms that had plenty of time below the radar of regulators to accumulate and entrench their power in digital markets.

Open sourcing AI: intellectual property at the service of platform leadership

by **Carlos Muñoz Ferrandis and Marta Duque Lizarralde***

Abstract: Artificial Intelligence (AI) is one of the most strategic technologies of our century. Consequently, tech companies are adopting intellectual property strategies to protect their investment in the field, which encompasses copyright, patents, and trade secrets. While the number of AI-related patent applications is increasing, the number of open-source AI projects sponsored by major AI patent holders is also on the rise. This article explores the commercial and policy strategic reasons behind the growing adoption of open-source licensing in the AI space. More precisely, it assesses how IP rights are articulated around "openness" as a competitive factor in ecosystem competition, and how some players are using open-source licensing successfully to attract a critical mass of users and build an ecosystem around their AI platforms. Moreover, this article integrates the debate on the protectability of AI features by IP rights to assess the potential implications for open-source. Finally, it analyses the most used open-source licenses in AI projects and highlights existing and future challenges from an IP and contractual law perspective.

Keywords: AI; platforms; open-source; licenses; copyright; patents

Recommended citation: Carlos Muñoz Ferrandis and Marta Duque Lizarralde, Open sourcing AI: intellectual property at the service of platform leadership, 13 (2022) JIPITEC 224 para 1.

A. Introduction

1 Artificial Intelligence (AI) is transforming the world while "becoming one of the most strategic technologies of the 21st century".[1] Nevertheless, AI technology is nothing new. The concept of AI was first introduced as an academic discipline in 1956, subsequently suffering ups and downs until the current boom, caused by the growth in computing power, connectivity, and the greater availability of data.[2]

2 Although there is no universal definition of AI, it can be regarded as "a discipline of computer science that is aimed at developing machines and systems

* Carlos Muñoz Ferrandis was at the time of the paper's acceptance PhD Researcher at the Max Planck Institute for Innovation and Competition, and member of the Global Innovation Policy & Law Research Group (Alicante Univ.). Marta Duque Lizarralde is Doctoral Candidate and Research Associate at the Technische Universität München. Both authors have equally contributed to this paper. The views expressed herein are those of the authors alone and do not necessarily represent the views of their respective organizations.

1 All links last accessed on the 25th January 2022. European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, "Artificial Intelligence for Europe" (2018) 1 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN>.

2 Josef Drexl, Reto M. Hilty et al., 'Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective, Version 1.0' (2019) <https://ssrn.com/abstract=3465577>; WIPO, 'WIPO Technology Trends 2019' (2019) 58, 79 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf>.

that can carry out tasks considered to require human intelligence".[3] There are many ways to achieve AI, machine learning (ML) being one of them. ML is a subfield of AI that is "limited to predicting a future that looks mostly like the past".[4] It involves pattern recognising systems that "learn" by adjusting to previous data, in order to make predictions about new data.[5] Three main types of ML exist: supervised[6], unsupervised[7] and reinforcement.[8] Some well-known applications of AI are machine vision, object and speech recognition, and detection and language translation.[9]

3 Against this background, many companies have understood the need to protect their investments in the creation of AI systems by means of Intellectual Property Rights (IPRs). This may explain the drastic increase in AI-related patent applications in recent years. Statistics compiled by the World Intellectual Property Organisation (WIPO) show that although approximately 340,000 patent applications for AI-related inventions have been filed since the emergence of AI, more than half of these applications are from 2013 onwards.[10]

4 On the other side of the spectrum, there is a continuous increment in the number of open-source software (OSS) projects related to AI.[11] According to the OECD, since 2014 the number of OSS repositories related to AI has grown about three times more than the rest of OSS.[12] This is partly due to the roots of AI in academia, which has been at the origins of collaborative software development projects and tended to be reluctant to participate in projects with access restrictions due to IP.[13] Nowadays, however, some of the most relevant OSS AI projects are governed by large tech companies[14], such as Google and Facebook (now Meta) with their respective ML frameworks: TensorFlow[15] and PyTorch[16]. Despite owning the largest patent portfolios in the AI sector, these companies also share their source code and provide open-source licenses for their AI-related patents.[17]

3 WIPO (n 2).

4 Matt Taddy, ´The Technological Elements of Artificial Intelligence´ (2019) NBER Working Paper 24301 <https://www.nber.org/system/files/working_papers/w24301/w24301.pdf>.

5 Mohri Mehryar, Afshin Rostamizadeh, and Ameet Talwalkar, *Foundations of Machine Learning* (MIT Press, 2018) 1,2.

6 Anthony Man-Cho So, ´Technical Elements of Machine Learning for Intellectual Property Law´, in J.-A. Lee, K.-C. Liu, R. M. Hilty (eds.), *Artificial Intelligence & Intellectual Property* (Oxford University Press, 2020): In supervised learning the system is trained with labelled data and must be able to apply this knowledge to recognize the labels in a new dataset.

7 Mohri et al (n 5): In unsupervised learning the training data samples do not have any labels and the goal is to cover hidden structure underlying the data.

8 Anthony Man-Cho So (n 6): In reinforcement learning the system must achieve a certain goal and receives penalties or rewards for its performance, the goal being to maximise the total reward.

9 WIPO (n 2).

10 WIPO (n 2).

11 Open-source is a software collaborative innovation and development model based on the freedoms to access, run, study, re-distribute the used software and distribute derived one, while respecting the terms of the open-source license. For the purpose of this paper the definition proposed by the Open-source Initiative (OSI) is used, according to which each license must comply with the 10 OSI criteria. See <https://opensource.org/osd>.

12 Stefano Baruffaldi et.al. 'Identifying and measuring developments in artificial intelligence: Making the impossible possible' (Organisation for Economic Co-operation and Development, 2020) 32.

13 Ibrahim Haddad, *Open-source AI Projects, Insights, and Trends* (The Linux Foundation, 2018) 104; Danish Contractor et al., 'Behavioral Use Licensing for Responsible AI' (arXiv - Computer and Society, 2020) 1; assessing opposing views, see Knut Blind et.al. *The impact of Open-source Software and Hardware on technological independence, competitiveness and innovation in the EU economy* (European Commission, 2021) 306,307.

14 Tom Simonite, 'Despite Pledging Openness, Companies Rush to Patent AI Tech' (31 July 2018, WIRED) <https://www.wired.com/story/despite-pledging-openness-companies-rush-to-patent-ai-tech/>; WIPO (n 2). There are, however, some OSS AI projects which maintainers are research organisations (e.g., UC Berkeley) or OSS institutions (e.g., the Apache Software Foundation).

15 TensorFlow <https://github.com/tensorflow/tensorflow>.

16 Pytorch <https://github.com/pytorch/>.

17 Nathan Calvin, Jade Leung, 'Who owns artificial intelligence? A preliminary analysis of corporate intellectual property strategies and why they matter', (2020) 7,8 <https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-working-paper-Who-owns-AI-Apr2020.pdf>; Patrick Shafto, 'Why big tech companies are open-sourcing their AI systems' (2016, The Conversation) <https://theconversation.com/why-big-tech-companies-are-open-sourcingtheir-ai-

5 Patenting and open-source commercial strategies are not alien to each other in the ICT realm. Both are considered core innovation and competition factors in isolation. Having an efficient IP proprietary strategy allows companies a direct return on investment, to avoid free-riding, and to establish a competitive advantage.[18] Nevertheless, literature has recently highlighted the articulation of open-source as a strategic competitive move in contexts that depend on strong network effects, such as standardisation.[19] Interestingly, and in line with the aforementioned, the AI sector shows how the combination of patents and open licensing schemes towards hybrid IP strategies might have a strategic impact on the market.

6 This article aims to give insight into the objectives of tech companies when adopting open-source and proprietary strategies. It seeks to illustrate how OSS is contributing to the rapid development of AI technologies, but also to highlight the risks that stakeholders may face if they do not comprehend the licensing terms before contributing to AI open-source projects.

7 The structure of this article is as follows: Section B outlines how open-source licenses are used as strategic competitive elements in the quest to build ecosystems in the AI field. Then, Section C explores the IP rights involved in the protection of AI systems, before examining the most commonly used open-source licenses in AI projects according to the data collected from the scrutinised 60 open-source AI projects. The authors have taken an inductive approach, with the research criteria when selecting an open-source AI project for analysis being: (i) the open/public-access platform hosting the software (e.g., repositories such as GitHub); (ii) the platform's sponsors; (iii) the release under an OSS license; and (iv) the ecosystem around the OSS. The analysis of these data allows a better understanding of the rationale behind the use of a specific open-source license for an AI function, and to draw practical conclusions from it. In particular, the pervasiveness of permissive licenses over restrictive ones highlights the expected business strategies behind the choice of licenses such as Apache 2.0 or MIT; this will be explained in Section D.[20]

B. Open-source dynamics and their strategic impact in the AI space

8 Taking a strategic approach to OSS, IP assets might be conceived as attraction and control mechanisms. OSS licenses, especially permissive ones, are legal tools for software mass market adoption (B.I.), and play a core role in the development and market leadership of software platforms (B.II). Firms compete to capture the network effects derived from the adoption of OSS tools and/or platforms by trying to be the first in releasing specific OSS (B.III.). In addition, some companies use 'open' patent strategies complementary to OSS in order to leverage their IPRs as attractive instruments (B.IV.).

I. A non-traditional use of exclusivity rights

9 In general, open-source uses IP as a tool aimed at maximising the diffusion of innovation through licenses designed around the concept of distribution.[21] Hence, it represents a shift from a direct reward via licensing of IP to a focus on distribution and attraction as means to compete in markets. Companies commercially leveraging the potential of OSS might extract their return on investment at different points of the value chain (vertical approach)[22] and/or from adjacent connected markets (horizontal

systems-54437>.

18 See Alfonso Gambardella, ´The functions of patents in our societies: innovation, markets, and new firms´ (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789554>.

19 Jorge L. Contreras, 'Patent Pledges' (2015) 47(3) *Arizona State Law* Journal 546; Eli Greenbaum, 'Puzzles of the Zero-Rate Royalty' (2016) 27(1) *Fordham Intellectual Property, Media and Entertainment Law Journal* 13; Liza Vertinsky, 'The Hidden Costs of Free Patents' (2017) *78(6) Ohio State Law Journal.*

20 For the sake of clarity, informational purposes, and transparency the list of all the assessed OSS AI projects is attached in Annex A. It is thus expected to inform the reader on the AI specific licensed feature, the chosen OSS license, and the stakeholder behind the project.

21 Steven Weber, ´The Success of Open-source Groups´ (2005) *Harvard University Press* 1,86; Van Lindberg, 'OSS and FRAND: Complementary Models for Innovation and Development' (2019) *20 The Columbia Science and Technology Law Review* 254.

22 For instance, OSS business models might be based on dual licensing or open core, where aside from the OSS a commercial version is offered, either with a license enabling more flexibility to the user than the OSS one (dual licensing, e.g., MySQL); or technically optimized to better perform on an enterprise environment by adding extra closed software features (open core. e.g., MongoDB). Moreover, a classic example is one of RedHat's business models monetizing open-source by means of support, educational, and security services related to the OSS feature.

approach).[23] For instance, by open sourcing TensorFlow (an ML framework), Google enables developers to access ML capabilities and consequently generates demand for cloud computing and data centre provision.[24]

10 Companies relying on traditional IP strategies generally enforce their right to exclude others to protect their inventions from imitators or free riders, or/and to secure a direct return on investment from the monetisation of the IPR. Contrarily, open-source licenses implement both dissuasive and passive exclusion. With dissuasive exclusion, those licensees not complying with the terms of the license will lose the benefit of using the software.[25] Passive exclusion neutralises licensees' enforcement rights by compelling them not to enforce certain IPRs infringed within the OSS project. This can be done by means of reciprocity, non-assertion, and retaliation clauses.

11 Open-source licenses are *de facto mass-market licenses*[26], which means that the licensees are presented with a given set of standard and non-negotiable terms.[27] This is known as frictionless distribution[28], as the users only have the option of joining the contract, contrary to other existing licensing practices where the terms of the agreement are negotiated by the parties.[29] Moreover, actions such as using, reproducing or distributing the software are sufficiently indicative of the acceptance of the terms of the licenses.[30]

12 Due to the aforementioned characteristics, open-source licenses might reduce transaction costs, since both the licensor and the licensee are not forced to engage in a lengthy negotiation process. Besides, these licenses might promote faster adoption and a wider scope of innovation due to network effects, conversely to what happens in a static situation where the allocation of IPRs depends on individual negotiations, e.g., Linux. However, potential costs derived from OSS quality, licensing compliance and enforcement should not be overlooked.

II. Sided markets and ecosystem creation

13 From a market competition perspective, open-source can be a double-edged innovation tool. On the one hand, it may facilitate a broader access to technology, making its use easier and promoting participation. On the other hand, firms involved in the innovation process usually compete in terms of achieving network effects and market tipping[31], since this can have a positive indirect effect on adjacent component markets from which they seek to extract revenues.[32] In words of Blind et al. "Open-source has a multi-faceted role for competition."[33]

23 A 'modern' or not so explored angle of OSS business models are the ones targeting platform and market control by means of (not so) 'open' source strategies, such as Google's Android, analysed below.

24 Blind et al. (n 13) 89.

25 David McGowan, 'Legal Implications of Open-source Software' (2001) *241 Illinois Law* 34.

26 Steven Weber (n 21) 212.

27 Van Lindberg (n 21) 254.

28 Greg R. Vetter, 'Open-source Licensing and Scattering Opportunism in Software Standards' (2007) *48(1) Boston College Law Review* 247,248.

29 According to Weber, the open-source licenses are contrary to the adversarial legal dynamic in which each one tries to obtain the most advantageous terms for its side. Steven Weber (n 21) 179.

30 Some open-source licenses are more explicit than others regarding which actions trigger "acceptance", see Eclipse Public License v2 <https://opensource.org/licenses/EPL-2.0>; GPL v3 Section 9 <https://opensource.org/licenses/GPL-3.0>; Apache 2.0 Definition of the term "License" <https://opensource.org/licenses/Apache-2.0 >; from a literature standpoint, see Andrew M. S. St. Laurent, *Understanding Open-source and Free Software Licensing* (O'Reilly, 2004) Chap. 6; Lawrence Rosen, *Open-source Licensing Software Freedom and Intellectual Property Law* (Prentice Hall, 2004) 54,55; Andrés Guadamuz, 'The License/Contract Dichotomy in Open Licenses: A Comparative Analysis' (2009) *30(2) University of La Verne Law Review* 8; Van Lindberg, 'OSS and FRAND: Complementary Models for Innovation and Development' (2019) 20 *The Columbia Science and Technology Law Review* (n 21) 255,256.

31 Weber holds that free software counters opportunistic behaviours by reducing barriers to entry and avoiding potential lock-in. Steven Weber (n 21) 221. However, lock-in may also appear in open-source settings, despite competitors benefiting from low barriers to entry and the freedom to fork.

32 Michal S. Gal, Daniel L. Rubinfeld, 'The Hidden Costs of Free Goods: Implications for Antitrust Enforcement' (2016) *80(3) Antitrust Law Journal* 523,535; Stephen M. Maurer, Suzanne Scotchmer, 'Open-source Software: The New Intellectual Property Paradigm' (2006) *NBER Working Paper* 12148.

33 Blind et al. (n 13) 337: " *OSS is not an obstacle, but rather a facilitator for companies to enter competitive markets also based on AI. However, the large platform providers challenging competition policies and authorities also make use of OSS contributions for the development of software they use for developing their platform*

14 A firm might seek to invest in an OSS project in order to benefit from it in other markets where network externalities are decisive.[34] For instance, one of the incentives for stakeholders to compete in the Market A with an OSS product may be to exclude competitors relying on proprietary business models. The latter strategy will allow them to gain an advantage in Markets B and C where they also compete by offering proprietary components vis-à-vis the same participants from Market A.[35]

15 Namely, in order to compete in the mobile operating system market, Google chose to first develop and control the formation of a de facto standard, Android, by means of an industry consortium, the Open Handset Alliance, and with an "open" approach towards the technology.[36] Google then developed an ecosystem around Android in which it leaves some parts open for development from tier developers, and closes other parts that are developed and periodically released with new versions by Google. With Android, Google embraces openness as a means to an end, but not as an end in itself.[37] The end goal is to create an ecosystem around the platform, using the latter as an element of attraction for developers as well as hardware manufacturers. A similar strategy is being pursued today by open-source ML platforms.[38]

III. The race-for-release

16 The "release early and release often" dynamic stemming from the Linux development project has become a 'maxim' in the highly competitive and fast-growing ICT field. As a result of it, some companies compete fiercely by means of OSS products[39], aiming to attract a critical mass of users, composed of customers and developers, to consolidate an ecosystem around the released OSS tool.[40] By launching a product promptly the company seeks to benefit from the "first-mover advantages"[41], especially if it has considerable financial power to invest in terms of marketing policy and strategy.[42] Conversely, the introduction of a new OSS tool may be a response to a competitor's first move, or to its strong influence in a given market.[43] Moreover, a company can decide to release OSS to avoid potential competitors' attempts to patent a technology which is fundamental for the market.

17 Examples of the "race for release" can be found within markets related to autonomous vehicles. Clear illustrations are the open-source releases of

architectures and ecosystems. Consequently, open-source has a multi-faceted role for competition. Therefore, it is recommended to explicitly consider open-source in the further discussion and development of competition policies in general and platform policies in particular."

34 Elad Harison, *Intellectual Property Rights, Innovation and Software Technologies: The Economics of Monopoly Rights and Knowledge Disclosure* (Edward Elgar Publishing, 2008) 106; Josh Lerner, Jean Tirole, 'The Scope of Open-source Licensing' (2002) NBER Working Paper <https://www.nber.org/papers/w9363>.

35 However, this is just an over-simplified scenario focused on price as an essential competition parameter. The market can be more or less price-sensitive, and thus other parameters such as quality might play a relevant role. See Ramon Casadeus-Masanell, Pankaj Ghemawat, 'Dynamic Mixed Duopoly: A Model Motivated by Linux vs. Windows' (2006) 52(7) *Management Science* 1072.

36 Ron Amadeo, 'Google's iron grip on Android: Controlling open-source by any means necessary' (2018, arsTECHNICA) <https://arstechnica.com/gadgets/2018/07/googles-iron-grip-on-android-controlling-open-source-by-any-means-necessary/>; Michele Herman, 'Sensible Open-source Licenses For Standards Development Organizations' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3717031>.

37 Alan Cunningham, 'Open-source, Standardization, and Innovation' in Noam Shemtov, Ian Walden (eds.) *Free and Open-source Software: Policy, Law, and Practice* (Oxford University Press, 2013) 366.

38 Ibrahim Haddad (n 13) 36.

39 Sandeep Krishnamurthy, 'An Analysis of Open-source Business Models', in Joseph Feller, Brian Fitzgerald, Scott Hissam and Karim Lakhani (eds.) *Making Sense of the Bazaar: Perspectives on Open-source and Free Software* (Workshop 2001) 17,18.

40 Stephen M. Maurer, Suzanne Scotchmer, (n 32); Josh Lerner, Jean Tirole, (n 34): *"IBM released half-a-million lines of its Cloudscape program, a simple database that resides inside a software application instead of as a full-fledged database program, to the Apache Software Foundation. Hewlett-Packard released its Spectrum Object Model-Linker to the open-source community to help the Linux community write software to connect Linux with Hewlett Packard's RISC computer architecture. This strategy is to give away the razor (the released code) to sell more razor blades (the related consulting services that IBM and Hewlett Packard hope to provide)".*

41 In markets relying on network effects, companies seeking to be the first to launch a product/service want to capture and consolidate them to be able to lock-in demand and render more difficult market entry for potential competitors.

42 Steven Weber (n 21).

43 Stephen M. Maurer, Suzanne Scotchmer (n 32).

Uber[44] and Lyft.[45] While one might think that some of these companies are active only in certain specific ridesharing markets, the reality is that the released OSS tools may also be useful for them in other markets[46], such as ML tools applications and related markets.[47]

IV. Hybrid strategies

18 The predominant strategy of the leading AI companies is to simultaneously accumulate patents and heavily invest in the OSS community.[48] The debate on the need for AI-related patents can be assimilated with the debate on software patents. On the one hand, some national and regional strategies seek to reinforce the protection of IPRs and to ensure the patentability of AI-related inventions in order to foster research and investment.[49] They argue that AI-related patents encourage innovation and diffusion of AI technology via the disclosure of the technology in exchange of its protection.[50] On the other hand, others claim that patents on fundamental AI techniques with broad applications discourage innovation because the privatisation of the basic elements of AI can be used to exclude third parties from competition.[51] They fear that the increase of AI-related patents could lead to an unsustainable level of litigation, which is claimed to be extremely costly, might discourage innovation and hamper the growth of the AI sector.[52]

19 While AI-related patents are barely litigated so far[53], the IP strategy of the patent holders cannot be described as purely defensive. AI-related patents are being used to gain influence in other spheres, as seen in the patent sharing agreement concluded between Google and Tencent, which "is paving the way for Google's entry into the Chinese market".[54] Furthermore, as most of the AI-related patents granted are very recent, not enough time has passed as to assess the level of litigation in this area, which will only become visible when more AI applications and products are commercialised. Once this stage is reached, some believe that the number of AI patent lawsuits may increase.[55] Another view considers that patent holders may be hesitant to enter into disputes since the qualification of AI core inventions as patentable subject matter is still uncertain and this could lead to the invalidation of some of their patents in court.[56] Furthermore, AI related patents may be difficult to enforce due to the technical complexity of the inventions in question.[57]

20 Nevertheless, it is far from accurate to assert that the existence of AI-related patents will have a negative impact on the market and lead to further restrictions on AI's openness. Some companies engage in heavy R&D investments because of their trust on the IPR

44 Kyle Wiggers, 'Uber open-sources Manifold, a visual tool for debugging AI models' (202,Venturebeat) <https://venturebeat.com/2020/01/07/uber-open-sources-manifold-a-visual-tool-for-debugging-ai-models/>.

45 Kyle Wiggers, 'Lyft releases Flyte, a platform for maintaining AI workflows' (2020, Venturebeat) <https://venturebeat.com/2020/01/07/lyft-releases-flyte-a-platform-for-maintaining-ai-workflows/>.

46 Thomas R. Eisenmann, Geoffrey Parker, Marshall Van Alstyne, 'Opening Platforms: How, When and Why?' in Annabelle Gawer (ed.), *Platforms, Markets and Innovation* (Edward Elgar Publishing, 2011) 16,17.

47 Jesús Rodríguez, 'Uber Has Been Quietly Assembling One of the Most Impressive Open-source Deep Learning Stacks in the Market' (2020) Datasource.ai < https://www.datasource.ai/en/data-science-articles/uber-has-been-quietly-assembling-one-of-the-most-impressive-open-source-deep-learning-stacks-in-the-market> .

48 Nathan Calvin and Jade Leung (n 17) 2.

49 *Ibid;* See China, the USPTO, the EPO and the Singapore Patent Office; Rogier Creemers, Graham Webster, Paul Tsai, Paul Triolo, Elsa Kania, 'Translation State Council Notice on the Issuance of the Next Generation Artificial Intelligence Development Plan' (2017) https://d1y8sb8igg2f8e.cloudfront.net/documents/translation-fulltext-8.1.17.pdf >.

50 Nick Bostrom, 'Strategic Implications of Openness in AI Development' (2017) Global Policy 2; IPO, 'Artificial Intelligence A worldwide overview of AI patents and patenting by the UK AI sector'(2019) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf>.

51 Raphael Zing, 'Foundational Patents in Artificial Intelligence' in J.-A. Lee, K.-C. Liu, R. M. Hilty (n 6) 74,98.

52 Nathan Calvin and Jade Leung, (n 17) 4,5; Tom Simonite (n 14).

53 WIPO (n 2) 111,117: less than 1% of the 340,000 AI-related patent families have faced litigation so far.

54 Nathan Calvin and Jade Leung (n 17) 4.

55 WIPO (n 2) 141.

56 Patent Strategy, 'Machine yearning: AI and patents' (2019, ManagingIP) <https://www.managingip.com/pdfsmip/Machine-yearning-AI-and-patents.pdf>.

57 See Tabrez Ebrahim, 'Artificial Intelligence Inventions & Patent Disclosure' (2020) *125(1) Penn State Law Review* 149,220.

system and the possibility to obtain an adequate reward. Thus, a system lacking patents could discourage further R&D investments, leading to less innovation and negatively impacting the market in the mid- to long-term.[58]

21 Regarding the articulation of patent portfolios and OSS platform investment, it should be emphasised that when large tech companies use this hybrid strategy[59], the aim in the short run might be to gain traction by means of an "open" AI platform. In the long run, however, they seek to standardise and commoditise the technology, and ultimately to control essential software layers, and by extension their markets.[60]

22 In the software sector, for example, the major patent holders, IBM and Microsoft, instead of enforcing their IPR, have adopted policies to license them on a royalty free (RF) basis to users, provided the latter grant parallel access to their own IPR.[61] In this way, these companies managed to create and consolidate large "IP-neutralised" areas.[62] Defensive patent strategies and open-source dynamics might well complement each other to achieve market tipping and innovation control in a given market or software layers. Either in proprietary-based or open-source, IPRs are used as dissuasive instruments securing a non-assertion zone in which the sponsor could both avoid costly litigation and gain access to others' patents through a reciprocal 'patent pledge'.[63] The pledge may have a narrow scope devoted to a specific market use, to enable the sponsor a considerable margin of manoeuvre exploiting their patents for different uses and markets.

23 Previous experiences have shown that the use of OSS in some emerging technologies brings positive effects.[64] For small players having access at zero cost to the code and patented technology of the largest players can be a great opportunity and at the same time a significant risk, since RF access does not mean unconditional access.[65] In view of this, even if a high degree of openness in AI is desirable, and OSS can help to achieve this aim, contributors of AI OSS platforms should be aware of the licensing terms before committing to such projects.

C. IPR protection of AI features: implications for open-source licenses

24 Open-source licenses are characterised as conditional copyright licenses. That is, they grant all copyrights subject to the compliance with certain conditions for their exercise.[66] If these licenses apply to something that is not protected by copyright or related rights, they will not be triggered.[67] In addition, some open-source licenses contain patent grants and defensive termination provisions, so clarification is likewise needed as to which elements of AI systems may also be protected by patents.

I. Copyright

25 The software code and its preparatory design material are considered literary works protectable by copyright in the US and the EU. It follows that the copyright holder has the exclusive rights to

58 See Alfonso Gambardella (n 18).

59 Blind et al,(n 13) 38.

60 E.g., IBM's strategy with the x86 OS. See John C. Koenig, 'Seven Open-source Business Strategies for Competitive Advantage' (2006) *IT Manager's Journal* 5.

61 Anne Layne-Farrar, David S. Evans, 'Software Patents and Open-source: The Battle Over Intellectual Property Rights' (2004) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=533442>

62 *Ibid;* Ronald J. Mann, 'Do Patents Facilitate Financing in the Software Industry?' (2006) 83(4) *Texas Law Review* 1005,1007.

63 On common characteristics of patent pledges and their functioning see Jorge L. Contreras, 'Patent Pledges' (2015) 47(3) *Arizona State Law* Journal 546; Eli Greenbaum, 'Puzzles of the Zero-Rate Royalty' (2016) 27(1) *Fordham Intellectual Property, Media and Entertainment Law Journal* 13; Liza Vertinsky, 'The Hidden Costs of Free Patents' (2017) *78(6) Ohio State Law Journal.*

64 Bill Briggs, Stefan Kircher, Mike Bechtel, ´Open for business, How open-source software is turbocharging digital transformation´ (2019, Deloitte Insights) <https://www2.deloitte.com/us/en/insights/industry/technology/how-open-source-software-is-turbocharging-digital-transformation.html>; Eseosa Ehioghae and Sunday Idowu, ´Open-source Software in Emerging Technologies for Economic Growth´(2021) 7(27) ITEGAM-JETIA, *Manaus* 63,69.

65 See Jianan Wang and Xiaobao Peng, 'A Study of Patent Open-Source Strategies Based on Open Innovation: The Case of Tesla' (2020) <https://www.scirp.org/html/31-1763645_101900.htm>.

66 Heather Meeker, *Open-source for Business: A Practical Guide to Open-source Software Licensing´* (Last Mile Publishing, 2020) 77,88.

67 Begoña Gonzalez Otero, 'Machine Learning Models under the copyright microscope: is EU Copyright fit for purpose?' (2021) *GRUR International* 1043,1055.

authorise or prohibit the reproduction, translation, adaptation, arrangement, and any other alteration of the software, as well as its distribution.[68] It must be emphasised that copyright only protects the form in which the underlying ideas and principles of the software are expressed, i.e., its code, but its functional aspects are not covered.[69]

26 The algorithms composing AI systems are not by themselves protectable by copyright. However, these training algorithms are encoded in a programming language and embedded in software.[70] This software code, if meets the originality requirement, is copyrightable.[71] Under the same condition, the code provided in ML frameworks for training the models may also be protected.[72] As for the protection of ML models, Gonzalez Otero argues that even if they are expressed in coded form, and therefore can be qualified as computer programs, they may not meet the originality requirement.[73] In the same vein, it has also been pointed out that while simple linear ML models do not meet the requirements for protection under sui generis database right, it is debatable whether complex, dynamic ML models would be eligible for such protection.[74] Some have also proposed to introduce a new sui generis right for ML models.[75] Further research is needed on this subject and on how lack of IP for models would affect investment in their creation.[76] Finally, those parts of the overall AI application that are provided in the form of code may also be protected by copyright.[77]

27 A hot topic today is what IPRs protect training datasets. Many training datasets include data that although publicly accessible and freely available, are protected by copyright or related rights.[78] In addition, some training datasets may be susceptible to copyright or sui generis database rights protection.[79] Even when raw data and datasets are not protected by IPR, companies often restrict access to them through contractual restrictions or technical protection measures, creating de facto control.[80]

II. Patents

28 *AI-related inventions* can be divided between *AI-core* and *AI-applied* inventions. AI-core inventions are those characterised by mathematical or statistical-information-processing technology that improves the performance of the AI itself. Some examples are the algorithms composing the AI system, or improved ML methods.[81] AI-applied inventions are those resulted from applying AI-core inventions to individual technical fields. For instance, a ML

68 Art. 4 Directive 2009/24/EC (Software Directive); 17 U.S.C. §§ 101-103.

69 Art. 4 WIPO Copyright Treaty1996; Art. 1 Software Directive; and 17 U.S.C. §§ 101. See *SAS Institute v World Programming Ltd*, CJEU (2012) C-406/10, ECLI:EU:C:2012:259.

70 Stefano Baruffaldi, et.al. (n 12) 26. Peter R Slowinski ´Rethinking Software Protection´, in J.-A. Lee, K.-C. Liu, R. M. Hilty (n 6) 341,361.

71 Peter R Slowinski (n 70); Katarina Foss-Solbrekk, ´Three routes to protecting AI systems and their algorithms under IP law: The good, the bad and the ugly´ (2021) *16(3) Journal of Intellectual Property Law & Practice,* 246, 258.

72 Peter R Slowinski (n 70) 354.

73 Begoña Gonzalez Otero (n 67).

74 Josef Drexl, Reto M. Hilty et.al. ´Artificial Intelligence and Intellectual Property Law Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate´ (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3822924>.

75 Intellectual Property Owners Association Artificial Intelligence and Emerging Technologies Committee, ´Sui Generis Right for Trained AI Models´ (2020) <https://ipo.org/wp-content/uploads/2020/11/SG-model-rights-committee-paper-pub.pdf>.

76 Blind et al.(n 13) 340.

77 Peter R Slowinski (n 70) 356.

78 Benjamin Sobel 'A Taxonomy of Training Data: Disentangling the Mismatched Rights, Remedies, and Rationales for Restricting Machine Learning' in Reto Hilty, Jyh-An Lee, Kung-Chung Liu (n 6).

79 Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions, 'Towards A Common European Data Space', COM(2018) 232 final [2018] 6.

80 Josef Drexl, 'Designing Competitive Markets for Industrial Data – Between Propertisation and Access' (2017) *8 JIPITEC*, para 6,12; Catarina Arnaut, Marta Pont, Elizabeth Scaria, Arnaud Berghmans, Sophie Leconte, 'Study on data sharing between companies in Europe' (2018) <https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en>.

81 Japan Patent Office, 'Recent Trends in AI-related Inventions – Report´ (2020) <https://www.jpo.go.jp/e/system/patent/gaiyo/ai/document/ai_shutsugan_chosa/report-2020.pdf>; Kimberley Bayliss, ´Drafting AI patent applications for success at the EPO – eligibility and claim formulation´ (iam, 2021) <https://www.iam-media.com/patents/ai-epo-patent-drafting-eligibility-claim-formulation-hlk-co-published>.

model can be applied to image recognition, speech recognition, diagnosis, or prediction.[82]

29 When examining AI-related inventions, the European Patent Office (EPO) applies the two-hurdle approach of computer-implemented inventions (CII).[83] According to the patent-eligibility requirement, the invention cannot be *excluded subject matter*. To be patentable, AI-related inventions must be described and claimed in the context of an operation in a technical system, or in control of a technical process.[84] Subsequently, the EPO will analyse, as in any patent application, whether the AI-related invention meets the requirements of novelty, inventive step and industrial application.[85] Regarding the inventive step, the EPO will only consider the features of the technical character of the invention.[86]

30 In the US, AI-related inventions must pass the "two-part test" implemented by the Supreme Court in *Alice v. CLS Bank*.[87] Following to the ruling, claims must be directed to a "process, machine, manufacture or composition of matter"[88], but not to an abstract idea such as an algorithm or method of calculation.[89] Nevertheless, as the Court clarified, even if the claims are directed to an abstract idea, the invention may be patentable if it comprises an "inventive concept", meaning that "the implementation of the idea is not generic, conventional or obvious".[90]

31 AI in general and ML in particular are based on algorithms and computer models, which are of an abstract mathematical nature.[91] They are therefore excluded from patentability when claimed as such.[92] The same applies to some parameters, such as the weights, biases and evaluation mechanisms used in the training of the system. However, when all these features are applied in a specific technical use, they can be protected as elements of a broader invention, but only for that specific application.[93]

III. Trade secrets

32 The ideas or principles underlying the software, the programming language, the algorithms, models, and the aforementioned parameters can be protected by TS[94] if they are secret, have commercial value because of it, and the person lawfully in control of the information has taken reasonable steps to preserve their secrecy.[95] Nonetheless, since it is generally considered difficult to reverse engineer AI systems, maintaining the secrecy of AI innovation could prevent collaboration and integration among

82 *Ibid.*

83 The term "computer implemented inventions" covers claims which involve "*computers, computer networks or other programmable apparatus, whereby at least one feature is realised by means of a program.*". EPO Guidelines for Examination (2021) <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iv_3_9.htm>.

84 EPO, 'Guidelines for Examination, Mathematical methods' (2018) <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3.htm>.

85 Art. 52.1 European Patent Convention (EPC).

86 EPO, 'Guidelines for Examination, Artificial Intelligence and machine learning' (2018) <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm>.

87 US Supreme Court, *Alice Corp. v. ClS Bank International*, 573 U.S. 208 (2014).

88 35 U.S.C. Code §101.

89 Supreme Court: Assoc. for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576 (2013); US District Court Northern D. Illinois E.D.: Neochloris, Inc. v. Emerson Process Mgmt. LLP, 140 F. Supp. 3d 763 (2015), wherein one claim recited "*an artificial neural network module*" and the Court found that "*it is not even clear [from the specification or claim itself] what [that term] refers to besides a [generalized] central processing unit – a basic computer's brain*".

90 USPTO, 'Patent Subject Matter Eligibility [R-10.2019]' (2019) <https://www.uspto.gov/web/offices/pac/mpep/s2106.html>; James H. Ortega, 'Clarifying the Distinction Between the "Inventive Concept" and "Patentability" Requirements When Determining Patent-Eligible Subject Matter'(21 October, 2016, C&C Insights) <https://cclaw.com/2016/10/21/clarifying-distinction-inventive-concept-patentability-requirements-determining-patent-eligible-subject-matter/>.

91 EPO (n 86).

92 Art. 52.2(c) and 3 EPC.

93 Peter R Slowinski (n 70) 355; Josef Drexl, Reto M. Hilty et al. (n 74), Katarina Foss-Solbrekk (n 71).

94 Andrew Rapacke, 'Using Trade Secret Protection for AI IP' (2018) Rapacke Law Group <https://arapackelaw.com/trade-secrets/trade-secret-ai-ip/>; Jessica M. Meyers, 'Artificial Intelligence and Trade Secrets' (2019, American Bar Associacion) <https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/january-february/artificial-intelligence-trade-secrets-webinar/>.

95 According to Art. 2.1 Directive 2016/943 (Trade Secrets Directive), "trade secret" means information which meets all of these requirements; Josef Drexl, Reto M. Hilty et al (n 74); Peter R Slowinski (n 70) 356.

AI developers.[96] Conversely to reciprocal open-source licenses, permissive open-source licenses might work well with the use of non-disclosure agreements related to TS and know-how of the AI system.[97]

IV. Impact on the enforceability of OS licenses

33 There is no clear-cut answer for IPR protection of AI features. These might be subject to different interpretations, coming from the substance of the object of protection. Without IP rights the question arises whether the object of the license is missing. If potential implementers had to undertake the assessment of copyrightability and patentability of open-source AI features, they would incur an additional cost. Not all implementers would be willing, or have the legal expertise and financial resources, to do so. Also, the implementation of an IP clearance system in OS repositories carried out by the sponsor could have the effect of discouraging contributions to these repositories, as it is a large cost as well. The scenario is challenging. However, before embarking on a possible solution, the first step in this debate is to determine whether some AI features, such as ML models and datasets, are indeed protectable or not, given their wide availability under OSS licenses.

34 From the IPR holders' perspective, the enforceability of their IP rights is crucial. Traditionally the enforcement of OSS licenses has been conducted under the so-called "community enforcement", in which a warning letter or a report notifying the non-compliance is reportedly sufficient for overcoming the problem.[98] Nevertheless, even if voluntary compliance remains predominant, commercial litigation around OSS is not alien in the field. Consequently, IPR holders may also enforce their rights by claiming IPR infringement[99] and/or[100] contractual breach[101], depending both on the jurisdiction and the facts at the origin of the claim.[102] It is worth noting that unfair competition laws might also be a pertinent instrument in some instances.[103]

35 Until now, this article has explored the strategic use of open-source licenses as core competitive factors, and the implications of the IPR protection of AI features for open-source licensing. The next step is

96 EPO, 'Patenting Artificial Intelligence Conference summary' (2018) <https://e-courses.epo.org/pluginfile.php/23523/mod_resource/content/2/Summary%20Artificial%20Intelligence%20Conference.pdf >; Katarina Foss-Solbrekk (n 73).

97 Blind et al. (n 13) 191,192, see fig 6.5. For instance, permissive licenses might provide the IPR holder with an opportunity to offer a custom proprietary premium license attached to the OS core feature where sensitive information for the use of the OS core AI feature is disclosed.

98 Eben Moglen, 'Enforcing the GNU GPL' (2001, GNU Operating System) <https://www.gnu.org/philosophy/enforcing-gpl.html>.

99 Several judicial decisions have already pointed towards this option. Among them see, in the EU, *Welte v. Sitecom Deutschland GmbH*, Munich District Court *(Landgericht München)* Case No. 21 O 6123/04 (19 May 2004). In the US, see Court of Appeals for the Federal Circuit *Jacobsen v. Katzer*, inc. 535 F.3d 1373, 1379 (Fed. Cir. 2008); *Free Software Foundation v. Cisco*, Distict Court Sth. D. New York (11 December 2008), the case ended with a settlement. < https://www.fsf.org/news/2008-12-cisco-suit>.

100 Regarding accumulation of IPR infringement and breach of contract claims, not every jurisdiction accepts accumulating both contractual and IPR infringement claims. In the US, see *Artifex Software, Inc. v. Hancom, Inc.,* Case No. 16-cv-06982-JSC, (N.D. Cal. 2017). Contrarywise, in France, civil liability law is based on the principle of non-cumulation of criminal and contractual liability. Thus, an IPR holder will have always to claim either breach of contract or IPR infringement, but not both; See also Heather Meeker, 'Open-source and the Age of Enforcement' (2012) *4(2) Hastings Science and Technology Law Journal* 275,276.

101 In the EU, see *Entre'Ouvert v Orange & Orange Business Services* Paris Court of Appeal, Pôle 5 Ch. 2, 19th March 2021, nº19/17493, where the Court held that: *"lorsque le fait générateur d'une atteinte à un droit de propriété intellectuelle résulte d'un manquement contractuel, le titulaire du droit ayant consenti par contrat à son utilisation sous certaines réserves, alors seule une action en responsabilité contractuelle est recevable (...)".*

102 The conundrum relies on discerning whether IP law or contract law applies when enforcing an open-source license. Notwithstanding the latter, from a holistic approach, see CJEU C-666/18 *IT Development SAS v Free Mobile SAS* (2020) ECLI 1099. In this case, the CJEU held that regardless of the national applicable legal framework, an IPR holder will always be able to benefit from the warranties stemming from the provisions of the Directive 2004/48/CE (IPR Enforcement Directive).

103 The *Entre'Ouvert v Orange & Orange Business* case involved a breach of the GPLv2, the Court held that the licensee had taken an unfair competitive advantage stemming from the use of the software without complying with the licensing conditions imposed by the GPLv2, leading the company to be selected in a public procurement process before the French public administration (i.e., "parasitisme"). See *Entre'Ouvert v Orange & Orange Business Services* (n 96). Also, on the enforcement of unfair competition law by OS distributors see Till Jaeger, 'Enforcement of the GNU GPL in Germany and Europe', (2010) *1 JIPITEC* 35.

to examine which open-source licenses are the most widely used in the AI space, and why. The choice of an open-source license might define a company's IPR strategy.

D. Open-source dynamics: a legal approach

I. Most used open-source licenses for AI: rationale and legal assessment

36 Open-source strategies play a key role in the development and control of AI ecosystems.[104] To gain a better understanding of these dynamics in AI settings, the authors scrutinised 60 OSS AI projects and their licenses (see Annex I).[105] The main points of assessment were the predominant licensing terms; whether the project has a sponsor or has been *community-driven* from the beginning; and the existence of platform strategies in terms of ecosystem creation.[106] 42 projects have been released individually by a firm; 8 have been jointly released by a partnership of several firms/institutions; 8 from consortia or OSS organisations (Apache Foundation); and 2 by research centres.

37 While 56 of the 60 analysed OSS AI projects use permissive open-source licenses (42 chose Apache 2.0; 8 MIT, 3 selected BSD 2-clause and 3 BSD 3-clause), only 4 AI OSS projects use restrictive licenses.[107]

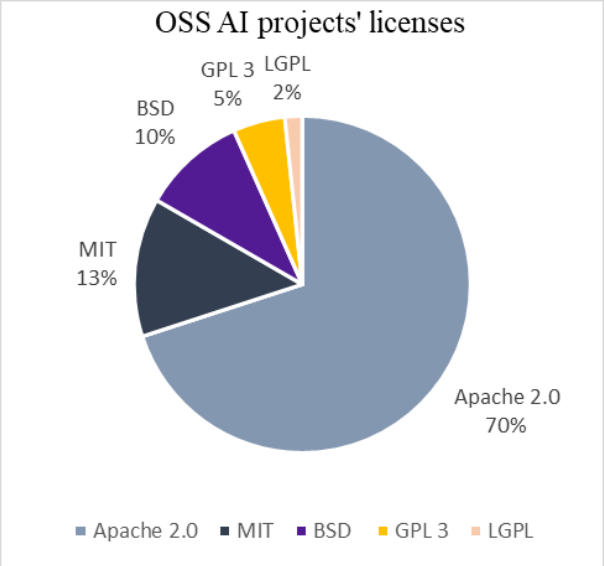

Figure 1 – Most used OSS licenses in 60 analysed AI projects

38 Our finding goes in line with a recent report sponsored by the European Commission, in which a survey of 441 respondents places permissive open-source licenses as the most used strategy for "*the protection*" of organisations' know how.[108]

39 The authors believe that the preference for permissive licenses in AI projects seems to be mainly due to three strategic business factors. The first one is the possibility for software to be sublicensed under different terms and to be incorporated into proprietary applications. This possibility of combining permissive licenses with restrictive licenses, and even with proprietary ones, provides the necessary flexibility for adopting hybrid licensing models[109], which are present in AI markets. For instance, in the field of ML and data analytics, companies such as H20.ai[110]or TIBCO[111], use open-source licenses tailored for commercial purposes, like MIT or Apache 2.0.[112]

104 Ibrahim Haddad (n 13) 8, 104; Gartner, ´Magic Quadrant for Machine Learning and Deep Learning Platforms´(2020). <https://www.gartner.com/doc/reprints?id=11Y4BB6P-M&ct=200110&st=sb.html&status=200>.

105 For project selection criteria, see section A. Taking a technical approach, although we focused on 'AI software tools' as a general framework including a non-exhaustive list of core technical features (libraries, ML frameworks, programming languages, etc), we specially focus afterwards on the platforms offering an AI toolkit or framework.

106 For this paper, an ecosystem is a network of interconnected systems, in this case interconnected software features, each of them potentially representing a product/service market.

107 3: GPLv3; 1: Lesser GPL (2.1).

108 Blind et al. (n 13) 192, fig 6.5.

109 For OS licenses' compatibility, see Heather Meeker (n 66); Thomas F. Gordon, 'Report on Problem Scope and Definition about OSS License Compatibility' (2009) Quality Platform for Open-source Software <https://www.osscc.net/pdf/QualipsoA1D113.pdf>.

110 See H20.ai <https://www.h2o.ai>.

111 See TIBCO <https://www.tibco.com>.

112 Even so-called restrictive open-source licenses might in given circumstances allow combination with other licenses. For instance, in the case of KNIME's platform, the OSS license GPLv3 integrates an additional exception that allows the use of an Application Programming Interface (API) to add proprietary extensions. Henceforth, the fact that GPL-family licenses integrate 'copyleft' clauses do not

40 The second business factor is based on the complexity of GNU General Public License (GPL-style) licenses and the lack of harmonisation on the interpretation of some specific terms and their scope.[113] This makes the license an ambiguous set of legal terms which might be seen as a deterrent for firms willing to release their software under an open-source license.[114] Although GPL-style licenses have been used on a marginal and strategic vein with the advent of commercial OSS, the increasing frictions between big cloud service providers and smaller companies (SMEs) on the use of open-sourced software has reinvigorated its use.[115]

41 The third factor is that permissive licenses are designed to ensure mass adoption of a technology, as implementers feel more confident if they are allowed to build any kind of project, open-source or not, on top of the licensed code. Therefore, permissive licenses are a pertinent option when sponsors aim for their software tool to become a de facto standard in a given market, and subsequently build an ecosystem around it. As for the use of a permissive license to build an ecosystem, the best examples are the ML frameworks[116], such as TensorFlow[117] and Paddle Paddle sponsored by Google and Baidu respectively under the Apache.2.0 license, or Pytorch, sponsored by Facebook and licensed under BSD-3.[118] Some of these actors, like Google and Facebook, are proving to be very successful with such a strategy. For example, from the projects analysed, several are compatible with both TensorFlow and PyTorch—e.g., features built on top. More tellingly, there are some specific projects that seek interoperability between tools and frameworks to train models[119], such as ONNX, as well as to use models trained in diverse ML frameworks, such as Neuropod.[120] In addition to this, it should be noted that some companies in the hardware market are also building AI-related microprocessors that aim to be compatible with these current predominant ML frameworks.[121]

literally imply that subsequent commercial strategies are foreclosed. It will depend on the affected software module, on the license and on the interpretation of its scope. See KNIME's open-source record <https://www.knime.com/knime-open-source-story>.

113 On contractual interpretation of OS licenses and their terms/clauses see also Andrés Guadamuz (n 30); and, Eli Greenbaum, 'Open-source Interpretation' (2021) *12(1) Journal of Open Law, Technology, & Society*.

114 The latter statement might also be true for permissive licenses in some cases, although these are simpler and more user-friendly than GPL-family ones.

115 More tellingly, the trend for SMEs nowadays in cloud infrastructure markets is steering towards the adoption of restrictive open-source licenses and a new type of open software license called 'source available' license. See Heather Meaker, 'Elastic License 2.0 and the Evolution of Open-source Licensing' (2021, COSS.community) <https://www.coss.community/coss/elastic-license-2-0-and-the-evolution-of-open-source-licensing-3jb3>.

116 We provide a definition which might also serve as justification for us to refer to these frameworks as 'platforms': Caffe2, 'Caffe2 and PyTorch join forces to create a Research + Production platform PyTorch 1.0' (2018) Caffe2: *"In practice, any deep learning framework is a stack of multiple libraries and technologies operating at different abstraction layers (from data reading and visualization to high-performant compute kernels)."* <https://caffe2.ai/blog/2018/05/02/Caffe2_PyTorch_1_0.html>

117 TensorFlow DL framework is licensed under an Apache 2.0 license, it has received more than 41,000 commits from 1,600 distinct contributors, and over 68,000 forks have been made (copy of the code for further modification). See Stefano Baruffaldi et al. (n 12) 26.

118 Ibrahim Haddad (n 13) 98: *"Most AI platforms are the results of years of investment and talent acquisition, and the open-source spinoff is a consequence of wanting to build an ecosystem versus a desire to collaborate with others on constructing a platform."*

119 See Open Neural Network Exchange (ONNX) "*a common set of operators - the building blocks of machine learning and deep learning models - and a common file format to enable AI developers to use models with a variety of frameworks, tools, runtimes, and compiler*". <ONNX | Supported Tools>.

120 See Neuropod, "*a library that provides a uniform interface to run deep learning models from multiple frameworks in C++ and Python*" <GitHub - uber/neuropod: A uniform interface to run deep learning models from multiple frameworks>.

121 Devin Coldewey, 'Mac-optimized TensorFlow flexes new M1 and GPU muscles' (2020, TechCrunch) <https://techcrunch.com/2020/11/18/mac-optimized-tensorflow-flexes-new-m1-and-gpu-muscles/>.

II. Common open-source licenses in AI settings

1. Permissive licenses

42 Permissive licenses allow users to freely copy, distribute and modify the software.[122] By not imposing restrictive conditions on the redistribution of the software, they allow licensees to profit from their modifications of the underlying OSS.[123] However, in the decision whether to embrace permissive licenses the following should be considered: as with the rest of open-source licenses, it is mandatory to maintain the copyright and license notice when redistributing the source code.[124] Some permissive licenses, such as Apache 2.0[125], also require the distributor to add notices regarding the modification of the files.[126] Subsequently, it is important to understand the exact scope of the license, especially if patents are involved, and to be aware that the program is provided by the licensor without any warranty and with an exclusion of liability. Instead, those using the licensed software are responsible for obtaining grants for third-party IP rights in case they are infringed.[127]

43 Although there are many permissive licenses, the most popular ones in AI projects are the BSD 2 and 3 Clause, the MIT, and Apache 2.0.

a) BSD 2 and 3 Clause

44 The BSD 2 and 3 Clause licenses are short and at first sight simple to understand. They allow for the "redistribution and use in source and binary form" of the software, "with or without modification".[128] Among the rights conferred on the copyright holder listed in section C, only the right to "redistribute" is expressly mentioned. Nevertheless, the rights of transformation and reproduction are implicitly granted, as the redistribution may be of a modified or unmodified copy.[129]

45 The other explicitly authorised action, i.e., the use of the software, is an exclusive right of the patent holders. This license 'language' raises doubts as to whether an implicit patent license is also granted, and if so, what would be the scope.[130] It should also be observed that the term "sublicensing" does not appear in the text of the license. Thus, to establish whether a sublicense is possible and, if so, what would be its scope, it is necessary to analyse the principles of contract interpretation and the practice of the OSS community.[131]

46 To conclude, the BSD may be an attractive option for ML platform sponsors, since it offers the licensors the flexibility to design their own patent statement.[132] Yet, one should be cautious when combining the BSD with other license terms, as illustrated by the example of the Facebook React Project.[133] The project was issued under the BSD-3 Clause license text plus a Facebook's own custom-written patent declaration, under which those suing Facebook for patent rights, even those not related to the project, would face an automatically revocation of the royalty free patent license. Since the added patent clause received strong criticism by stakeholders, Facebook had to re-license it under MIT.[134]

122 Ayala Goldstein, 'Open-source Licenses Explained' (2010, WhiteSource) <https://resources.whitesourcesoftware.com/blog-whitesource/open-source-licenses-explained>.

123 David J. Kappos, 'Open-source Software and Standards Development Organizations: Symbiotic Functions in the Innovation Equation' (2017) 18 *The Columbia Science & Technology Law Review* 263, 264.

124 Matt Mecoli, 'A Data Scientist's Guide to Open-source Licensing' (2018, towards data science) <https://towardsdatascience.com/a-data-scientists-guide-to-open-source-licensing-c70d5fe42079>.

125 See license text at <http://www.apache.org/licenses/LICENSE-2.0.html>.

126 Clause 4.d).

127 Lawrence Rosen, (n 30) 77,80.

128 See the license in <https://opensource.org/licenses/BSD-3-Clause>.

129 Andrew Sinclair, 'License Profile: BSD' (2010) 2(1) IFOSS L. Rev 2,4.

130 Lawrence Rosen (n 30) 83,84.

131 *Ibid.*

132 Aner Mazur. 'Apache license 2.0, MIT license or BSD license: Who is the fairest of them all?' (2017, snykblog) <https://snyk.io/blog/mit-apache-bsd-fairest-of-them-all/>.

133 Jenn Schiffer, 'Over React? Open-source licensing, Facebook, WordPress, and Patents' (2018, Medium) <https://medium.com/glitch/over-react-open-source-licensing-facebook-wordpress-and-patents-efeece333f12>; Martin Husovec, 'Standardization, Open-Source, and Innovation: Sketching the Effect of IPR Policies', in Jorge Contreras (ed.) *Cambridge Handbook of Technical Standardization Law* (Cambridge University Press, 2019).

134 Quincy Larson, 'Facebook just changed the license on React. Here's a 2-minute explanation why' (2017, freeCodeCamp)

b) MIT

47 The MIT license shares the principles of, but it is more comprehensive than, the BSD license. The MIT gives permission free of charge to "use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software."[135] Therefore, it refers to all the economic rights of copyright holders and, except for the right to "make", targets almost all the exclusive rights under patent law. Then, under a broad interpretation, the MIT implicitly includes a patent license, whose scope is nevertheless uncertain.[136] As stated previously, this is relevant for stakeholders who might not be aware of which patents are granted, for what purpose, and whether sublicenses are permitted.[137] In the event that the patent license does not cover the derivative works, licensees must obtain directly from the original licensor of the software an explicit grant of the patent rights that are required to use its modified versions.[138]

48 MIT is also a highly flexible license that leaves significant freedom in designing the scope of patent grants. Nevertheless, clear and explicit patent grants entitle the licensee to use, modify, distribute and—under some open-source licenses—sublicense software covered by the patent with greater certitude.[139] Consequently, although it is clearer in its terms than the BSD, some other licenses, as the Apache 2.0., seem to be more aligned with the interests of the ML platform's sponsors.

c) Apache 2.0

49 Apache 2.0 is a permissive "perpetual, worldwide, non-exclusive, no-charge and royalty free" license for copyright and patents.[140] Whilst it has similar principles to the BSD and MIT licenses, Apache 2.0 is much more detailed and thus provides more certainty to its adopters.

50 Apache 2.0 includes a comprehensive copyright grant and includes the right to sublicense and distribute in source or object both original and derivative software.[141] In addition, there is an explicit grant of any patents of the contributor that other collaborators of the project governed by the Apache license automatically infringe by using its contribution; as well as of any patents infringed by the resulting combination on the date of submission of such contribution with the Apache 2.0 licensed software to which it was provided.[142] Licensable patent claims include those that may be acquired in the future, "as long as they read on the original contribution as made at the original time".[143] However, the license does not extend to patents that would be infringed by an intermediate contribution altering the upstream code or combining it with the work in a new way.[144]

51 The most sensitive element of this license for a patent holder is its patent retaliation clause. This clause provides that any patent rights granted under the Apache 2.0 will be immediately revoked against a contributor that initiates a patent infringement litigation regarding the work or a contribution incorporated in the work.[145] The purpose of patent retaliation is to discourage any licensee from suing for patent infringement over the Apache licensed software.[146]

52 Apache 2.0 is the predominant license used in AI OSS projects due to its specificity in terms of licensees' obligations. The clarity, especially regarding the granting of patents, helps to attract the organisations that are most concerned about lack of access to software patents.[147] Yet, being

<https://www.freecodecamp.org/news/facebook-just-changed-the-license-on-react-heres-a-2-minute-explanation-why-5878478913b2/>.

135 See license in <https://opensource.org/licenses/MIT>.

136 Anna Haapanen, 'Free and Open-source Software & the Mystery of Software Patent Licenses' (2015) *7(1) International Free and Open-source Software Law Review 20.*

137 *Ibid.*

138 Lawrence Rosen (n 30) 88,90.

139 Andrew M. St Laurent (n 30) 14,24.

140 Clauses 2 and 3.

141 Clause 2.

142 Clause 3.

143 See FAQ about Apache Licensing, 'What is the scope of patent grants made to the ASF?' <http://www.apache.org/foundation/license-faq.html#PatentScope>.

144 Andrew Sinclair, 'License Profile: Apache License, Version 2.0' *(2010) 2(1) IFOSS L. Rev.* 109,110.

145 Clause 3.

146 Jay P. Kesan, 'The Fallacy of OSS Discrimination by FRAND Licensing: An Empirical Analysis' (2011) *Illinois Public Law Research Paper No. 10-14* 6; Eli Greenbaum (n 109).

147 Joseph Morris, 'Which License Should I Use? MIT vs. Apache vs. GPL' (2016, Exygy) <https://exygy.com/blog/which-license-should-i-use-mit-vs-apache-vs-gpl/>.

aware from the beginning of the scope of the patents covered by the license and the potential risk of a patent retaliation clause is crucial for adopting an adequate OSS strategy.

53 However, companies choosing permissive licenses must be aware of the possibility of competitors' appropriation and improvement of the released software tool. A recent example that illustrates both the complexities of license compatibility and its articulation with companies' business models can be found in Elastic. The company launched two projects under Apache 2.0, Elasticsearch and Kibana[148], but has recently changed its licensing model apparently due to some frictions with Amazon Web Services (AWS) products.[149] Elastic decided that future versions of these two programs would be dual-licensed, allowing users to choose between Elastic's own license[150] and the Server-Side Public License (SSPL).[151] Both licenses impose stricter conditions than Apache 2.0 on the use and modification of derivative works. Hence, by their adoption Elastic has rendered future versions of its projects incompatible with other licenses that allow the distribution of modified software as commercial services. In response, AWS[152] and other companies[153] have announced that they will create and maintain an Apache 2 licensed fork of Elasticsearch and Kibana.[154]

148 ElasticSearch is a database manager designed for enterprise search, and Kibana is a data visualisation tool. See their respective webpages at <https://www.elastic.co/de/elasticsearch/, https://www.elastic.co/de/kibana>.

149 Steven J. Vaughan-Nichols, 'Elastic changes open-source license to monetize cloud-service use' (2021) ZDNet <https://www.zdnet.com/article/elastic-changes-open-source-license-to-monetize-cloud-service-use/>.

150 See license at <https://www.elastic.co/licensing/elastic-license>.

151 See license at <https://www.mongodb.com/licensing/server-side-public-license>.

152 Carl Meadows, Jules Graybill, Kyle Davis, and Mehul Shah, 'Stepping up for a truly open-source Elasticsearch' (2021, AWS Open-source Blog) <https://aws.amazon.com/blogs/opensource/stepping-up-for-a-truly-open-source-elasticsearch/>.

153 Tomer Levy, 'Truly Doubling Down on Open-source' (2021, logz.io) <https://logz.io/blog/open-source-elasticsearch-doubling-down/>.

154 Steven J. Vaughan-Nichols, 'AWS, as predicted, is forking Elasticsearch' (2021, ZDNet) <https://www.zdnet.com/article/aws-as-predicted-is-forking-elasticsearch/>.

d) Permissive licenses' allocation in ML frameworks

"Project"	License	Datasets	Models	STK + Complementary Material[155]	Interfaces
Tensorflow	Apache 2.0	X	X	X	X
Pythorch	BSD 3	X	X	X	X
ParlaAI	MIT	X	X	X	X
Microsoft Cognitive Toolkit	MIT		X	X	X
Paddle Paddle	Apache 2.0	X	X	X	X
Keras	Apache 2.0	X	X	X	X

Table 1. Examples of ML Frameworks: technical components' licensing

54 Relevant ML frameworks are released under permissive open-source licenses. Although Apache 2.0 predominates, and is used in Tensorflow, Padle Padle, Keras; BSD-3 is used in another of the most relevant frameworks, Pytorch, as well as MIT in the Microsoft Cognitive toolkit and Parla AI.

55 It is worth noting that many platforms, in addition to the software toolkit for model training and the code that incorporates the different ML algorithms[156], offer other tools, such as datasets[157], APIs[158] and models.[159] Two different open-source licensing practices should be considered: tool-by-tool licensing and umbrella licensing. Under umbrella licensing, which is most used[160], all the software tools under the ML framework are embedded under a single license. Conversely, under the tool-by-tool

155 STK means software tool kit. Complementary material might be composed by the tools provided in addition to the software development kit needed to run and/or train the model, and training algorithms

156 See TensorFlow <https://github.com/tensorflow/models> <Libraries & extensions | TensorFlow> <Tools | TensorFlow>; Catboost <GitHub - catboost/catboost: A fast, scalable, high performance Gradient Boosting on Decision Trees library, used for ranking, classification, regression and other machine learning tasks for Python, R, Java, C++. Supports computation on CPU and GPU.>; ParlAI <Standard Agents — ParlAI Documentation>; Microsoft Cognitive Toolkit <GitHub - microsoft/CNTK: Microsoft Cognitive Toolkit (CNTK), an open-source deep-learning toolkit>; Paddle Paddle <GitHub - PaddlePaddle/Paddle: PArallel Distributed Deep LEarning: Machine Learning Framework from Industrial Practice （『飞桨』核心框架，深度学习&机器学习高性能单机、分布式训练和跨平台部署）>; In addition to the code provided in these platforms, we can also find other AI libraries, such as Scikit learn: ML library for ML basics <https://scikit-learn.org/stable/>; AI Fairness 360: *"includes a comprehensive set of metrics for datasets and models to test for biases"* <https://github.com/Trusted-AI/AIF360>, and AI Explainability 360: *"The AI Explainability 360 Python package includes a comprehensive set of algorithms that cover different dimensions of explanations along with proxy explainability metrics".* <https://ai-explainability-360.org/>.

157 See TensorFlow <Models & datasets | TensorFlow>; ParlAI <Tasks — ParlAI Documentation>; and Pythorch < https://pytorch.org/vision/0.8/datasets.html>.

158 See TensorFlow <https://www.tensorflow.org/versions>; Keras <https://keras.io>; Pythorch <https://pytorch.org/cppdocs/api/library_root.html>; Padle PAdle <https://github.com/PaddlePaddle/Paddle-Lite>; Catboost <catboost/CatboostModelAPI.md at master catboost/catboost · GitHub> and Microsoft Cognitive Toolkit: <https://docs.microsoft.com/en-us/cognitive-toolkit/cntk-library-api>.

159 ParlAI <Model Zoo — ParlAI Documentation>; TensorFlow <Models & datasets | TensorFlow> <TensorFlow Hub>; Pythorch <https://pytorch.org/vision/stable/models.html>; Microsoft Cognitive Toolkit <CNTK/PretrainedModels at master · microsoft/CNTK · GitHub>; and Paddle Paddle <https://github.com/PaddlePaddle/PaddleHub>.

160 This is the case of, for instance, Tensorflow, Paddle Paddle, and Keras.

licensing, each software tool of the ML framework has its own license.[161]

56 In practical terms, it might seem pertinent to ask whether there is any difference between the modular approach of tool-by-tool licensing, and the holistic approach of umbrella licensing. At a first glance, as the target is the same, it might look indifferent to use either when releasing each feature or all the features of the framework in an OSS repository. Even more, umbrella licensing might streamline the licensing of the entire framework and avoid transactions costs and time investment integrating individual licenses, although being the same, in each tool of the framework. Nonetheless, it must be further explored whether the adoption of a single license for an entire ML framework might also have the effect of prima facie covering tools for which IP protection is uncertain, such as APIs and algorithms, by an open-source license.

57 It must also be observed that further contributions to the various projects may be released under different licenses. In the same vein, the datasets used for training the model may have a different license than the framework with which they interact. Interoperability between frameworks and elements is therefore essential for AI development. It is equally important to ensure compatibility between the different open-source licenses covering each feature.[162] There are no drawbacks in this regard in the cases under review, since they are covered by permissive licenses, and they impose no restrictions on what code is added to the program or how it can be distributed. However, if it is intended to combine components that have a permissive license with a restrictive one, the situation becomes more complicated, as copyleft provisions in some restrictive licenses might be incompatible with permissive licenses' scope.[163]

2. Restrictive licenses: GPL family

58 Restrictive—also called hereditary[164] or reciprocal[165]—licenses, impose strict distribution requirements on the recipient. In principle, the distribution[166] of the modified software must be carried under the same license.[167] This idea is secured by so-called 'copyleft' clauses, which guarantee that those who wish to enjoy the freedom related to the licensed software have to give back to the community the same that they received from it in the first place.[168]

a) GPL as a strategic competitive tool

59 Despite initially having access to the core software feature, implementers might be forced to disclose follow-on innovation under the same license, benefiting the sponsor. Furthermore, the same action might lead in the mid/long run to the commoditisation of a given software layer and to the exclusion of any price competition. As a result, competitors for whom price competition is an essential parameter to remain competitive in the market could be affected.[169] Quality and innovation are thus going to be the leading competition parameters, which might not be affordable for every market actor. In a different setting, a company willing to "over throne" a competitor whose software product is becoming the standard in the market might release a competing GPL alternative.

161 OpenAI have many repositories with different licenses (mainly Apache 2.0 and MIT), and models are released in different ways. For instance, GPT-2 is licensed under a "modified MIT" <gpt-2/LICENSE at master · openai/gpt-2 · GitHub>; the dataset of GTP-2 outputs under MIT as well, but GPT 3 not, and actually has been exclusively licensed to Microsoft.

162 Even if many platforms also provide APIs for this purpose, it is likewise possible to find projects that seek interoperability between tools and frameworks to train models, as well as to use models trained in diverse ML frameworks, such as ONNX and Neuropod, mentioned above.

163 For OS licenses' compatibility, see Heather Meeker (n 61) 63; See this post listing which licenses are compatible with GPL at: <https://www.gnu.org/licenses/license-list.html#GPLCompatibleLicenses>; Richard Stallman, 'License Compatibility and Relicensing' (20 November, 2020, GNU operation system) <https://www.gnu.org/licenses/license-compatibility.html>.

164 Heather Meeker, *The Open-source Alternative: Understanding Risks and Leveraging Opportunities* (Wiley, 2008) 57.

165 Ronald R. Mann, 'The Commercialization of Open-source Software: Do Property Rights Still Matter?' (2006) 20(1) *Harvard Journal of Law & Technology* 15.

166 For discussions around the scope of the term 'distribution' under the GPL see Steven Weber (n 21) 180; Ross Gardler, 'Open-source and Governance', in Noam Shemtov, Ian Walden (n 37) 74.

167 Josh Lerner, Jean Tirole (n 34) 22; Elad Harison (n 34) 90.

168 Steven Weber (n 21) 180; Ross Gardler (n 166) 73.

169 See Mingqing Xing, 'The effect of competition from open-source software on the quality of proprietary software in the presence of network externalities' (2015) *Journal of Industrial Engineering and Management; Terrence August*, Wei Chen, Kevin Zhu, 'Competition Among Proprietary and Open-source Software Firms: The Role of Licensing in Strategic Contribution' (2020) *67(5) Management Science*; Blind et al. (n 13) 43.

With this move the company aims to attract a mass of users by facilitating 'open' zero price access to the software, and beyond, block the competitor's proprietary use of its software.[170]

b) Copyleft effect on the output of the ML system

60 In the context of ML techniques, such as natural language processing, models are trained to generate weights. The weights can be considered as the output of the process and might take the form of a machine-readable codified dataset from which interpretations are extracted.

61 In a context where some of the ML material, such as the trained model based on which weights are produced, is released under a GPL-style license it might be pertinent to ask whether the output result of running the model should be considered either a "derivate work"[171] or a "covered work" and "work based on the program"[172], depending on the version of the GPL. For instance, companies such as OpenAI expressly modify the open-source license in order to clarify that there is no claim of ownership on the *content* created with GPT-2.[173] Nonetheless, without those disclaimers there is uncertainty on the scope and effect of copyleft on the weights generated by the trained model.

c) Two examples of AI business models and GPL provisions

- ML-as-a-service and the limits of Affero GPL

62 Running an ML system might be offered as a cloud service, by which the user accesses the ML system by means of an API, such as OpenAI's GPT-3[174] and Amazon SageMaker.[175] If not yet, ML-as-a-service has the potential to become a standard practice, thus cloud-native licensing implications should be considered in the context of OS. GPL licenses, even Affero GPL[176] (AGPL), do not efficiently address remote server use, mainly due to the uncertainty around a lack of definition of terms essential for the triggering of the copyleft, e.g., "user", "interacting remotely through a computer network".[177] More precisely, it is doubtful whether the copyleft clause would be triggered in case the AGPL software is indirectly used, e.g. infrastructure-as-a-service where the AGPL software is just a module comprised in a software infrastructure, and thus it can be argued that the user does not directly interact with the AGPL software (i.e., a finetuned commercial application of the model).

- GPL3's flexibility and commercial compatibility

63 The GPL3 qualifies as a 'strong copyleft' license due to the broad restrictions required for the distribution of works derived/based on the licensed program.[178] Yet, there is an interesting section of GPL3 bringing flexibility to both the IPR holder willing to implement the license and potential licensees: Section 7. Section 7 allows the IPR holder, either the sponsor of the software or a company having created a new derived version of it, to add further "additional permissions" which are described as "exceptions from one or more of its conditions". "Additional permissions" may be freely removed from downstream licensees at their choice when conveying the work. However, for the latter to be integrated within the GPL3, it has to be made by the company holding IPRs related to the additional permissions, and not by any third party.[179]

64 This section brings flexibility in terms of potential combination of the license with other OSS licenses, such as Apache 2.0, or even allowing subsequent proprietary extensions. A clear example of its use

170 Heather Meeker (n 164) 231.

171 See GPL2 license.

172 See GPL3 license.

173 See OpenAI's GPT-2 Github repository <https://github.com/openai/gpt-2/blob/master/LICENSE>; Another example, although not in the field of AI, is the one of GNU Image Manipulation Program, where the software is licensed under GPL3 but the artwork generated by it is free from GPL3 restrictions <https://www.gimp.org/docs/userfaq.html#can-i-use-gimp-commercially>.

174 OpenAI API < https://openai.com/blog/openai-api/>.

175 Free Machine Learning Services on AWS <https://aws.amazon.com/free/machine-learning/?nc1=h_ls>.

176 Affero GPL <https://www.gnu.org/licenses/agpl-3.0.en.html>.

177 See Heather Meeker (n 164) 168; Jakub Mencl, W Kuan Hon, 'Copyleft in the Cloud', in Noam Shemtov, Ian Walden (n 37) 345.

178 See more in Luke McDonagh, 'Copyright, Contract, and FOSS'. in Noam Shemtov, Ian Walden (n 37) 82; Clark D. Asay, 'The General Public License Version 3.0.: Making or Breaking the FOSS Movement?' (2008) *14 Michigan Telecommunications and Technology Law Review* 274.

179 Free Software Foundation, 'Opinion on Additional Terms' (2006) <https://gplv3.fsf.org/additional-terms-dd2.html/>.

is the case of KNIME[180], which provides its KNIME Analytics Platform under a GPL3 license with a specific extension of it granting additional permission for licensees to use a standard API enabling the adding of proprietary node extensions.[181] Thus, if an implementer develops new software nodes based on KNIME's platform, it has the certainty under the extension granted by KNIME beyond the GPL3, that these nodes are not covered works of KNIME Analytics Platform. This can be perceived as sharp strategy from the sponsor's side. While a GPL family license is used to restrict possible private derivations of its platform, there is also flexibility to develop proprietary extensions by using a standard API, potentially provided by KNIME. This allows KNIME to keep control over the platform and over which kind of commercial extensions are created, as well as the restriction of some others.

E. Conclusion

65 There are several reasons for tech companies to employ open-source strategies in AI development. Some of them include achieving a competitive advantage in adjacent component markets from which they seek to derive revenue, gaining "first-mover advantages," or preventing a competitor from patenting a core technology. Foremost, the main goal of certain market players is to attract a critical mass of users in order to create an ecosystem around their ML platforms. This is facilitated by the use of permissive licenses.

66 Employing open-source in the development of some emerging technologies has proven to create positive effects. Open-source licenses can reduce transaction costs and promote faster adoption of the technology. In addition, OSS platforms serve as a free testing area where bugs and risks can be corrected. Nonetheless, while understanding that participating in OSS projects could open great opportunities for small players, OSS should not equate free of charge with unconditional access. Thus, contributors to AI OSS platforms must be aware of the licensing terms before committing to such projects. For instance, an open-source license might oblige the licensee not to enforce certain infringed IPRs within the OSS, e.g., through reciprocity, non-assertion and retaliation clauses. Therefore, companies seeking a direct return on investment from the monetisation of their IPRs should have a clear understanding of the scope of the OSS license in question, especially when it involves patents, and be sure that they are not granting more than what would be detrimental to their business model.

67 However, it should be stressed that for an OSS license to be effective, IPRs must exist. The protection by different IPRs of several elements essential to the development of AI systems, such as datasets, algorithms, ML models and APIs, is currently hotly debated. This is an issue of great importance that needs to be deeply analysed.

68 Nowadays, aside private R&D efforts carried by big tech and governments, the AI technology race is primarily taking place in open-source platforms and ecosystems.[182] Moreover, open-source is also experiencing a tough competition for future disruptive technologies.[183] Consequently, governments around the globe are recognising the importance of open-source in the success of these AI developments.[184] Derived from it, long term open innovation policies are trying to align with

180 KNIME is a company focused on data science and analytics <https://www.knime.com/knime-open-source-story>.

181 KNIME Analytics Platform license <https://www.knime.com/downloads/full-license>.

182 Ministry of Industry and Information Technology (n 70). There is also a trend on opening hardware infrastructure design for AI purposes, see Blind et al. have found opposed views for ML code, see Blind et al., (n 13) 309,310.

183 See Will Douglas Heaven, 'Google is making it easier to develop quantum machine-learning apps' (2020) MIT Technology Review <https://www.technologyreview.com/2020/03/09/905420/google-software-tensorflow-quantum-machine-learning-apps-ai-computing/>; Kyle Wiggers, 'Baidu open-sources Paddle Quantum toolkit for AI quantum computing research' (2020) Venturebeat <https://venturebeat.com/2020/05/27/baidu-open-sources-paddle-quantum-toolkit-for-ai-quantum-computing-research/>.

184 Blind et al., (n 13); Alexandra Theben, Laura Gunderson, Laura López Forés, Gianluca Misuraca, Francisco Lupiáñez Villanueva, *Challenges and limits of an open-source approach to Artificial Intelligence*, (European Parliament, 2021) Study for the Special Committee on Artificial Intelligence in a Digital Age (AIDA), Policy Department for Economic, Scientific and Quality of Life Policies; European Commission, Communication from the Commission,"Open-source Software Strategy 2020 – 2023, Think Open" (2020) 7149 final <https://ec.europa.eu/info/sites/default/files/en_ec_open_source_strategy_2020-2023.pdf>; National Institute of Standards and Technology, "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools Prepared in response to Executive Order 13859. (2019) <https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf>; Ministry of Industry and Information Technology - Informatization and Software Services Division (n 70); Chen Du, 'Chinese AI lab challenges Google, OpenAI with a model of 1.75 trillion parameters' (2021, PingWest) <https://en-pingwest-com.cdn.ampproject.org/c/s/en.pingwest.com/amp/a/8693>.

innovation phenomena like open-source. Therefore, beyond the scope of this paper, it remains to be seen (and further explored) which role open-source is going to play in geopolitical innovation strategies.

Annex I – Scrutinised OSS AI projects

	AI related feature	**OSS License**	Further information
Acumos H20 Model Builder	Model building and export	Apache 2.0	https://github.com/acumos/model-builder-h2o-model-builder
Adlik	Optimising framework for DL models	Apache 2.0	https://github.com/Adlik/Adlik
Adversarial Robustness Toolbox	ML Python library	MIT	https://github.com/Trusted-AI/adversarial-robustness-toolbox
AI Explainability 360	ML Python library	Apache 2.0	https://github.com/Trusted-AI/AIX360
AI Fairness 360	ML Python/R library	Apache 2.0	https://github.com/Trusted-AI/AIF360
Amundsen	Metadata engine	Apache 2.0	https://github.com/amundsen-io/amundsen
Angel	ML and graph/computing platform	Apache 2.0	https://github.com/Angel-ML/angel
Apache Singa	Distributed DL Library	Apache 2.0	https://github.com/apache/singa
Apache Mahou	Distributed linear algebra framework	Apache 2.0	https://github.com/apache/mahout
Apache Spark	Analytics engine	Apache 2.0	https://github.com/apache/spark
Apache MXNet	DL framework	Apache 2.0	https://github.com/apache/incubator-mxnet
Apache PredictionIO	ML server	Apache 2.0	https://github.com/apache/predictionio
Apache SystemDS	ML system for end-to-end data science lifecycle	Apache 2.0	https://github.com/apache/systemds
BERT	Pre-trained language model(s)	Apache 2.0	https://github.com/google-research/bert
CatBoost	ML Method	Apache 2.0	https://github.com/catboost/catboost
Caffe	DL Framework	BSD-2	https://github.com/BVLC/caffe
CLIP	Trained neural network	MIT	https://github.com/openai/CLIP
Dagli	ML Framework	BSD-2	https://github.com/linkedin/dagli
DeepDetect	ML API and server	GPL3	https://github.com/jolibrain/deepdetect
DeepLearning4J	DL framework	Apache 2.0	https://github.com/eclipse/deeplearning4j
DeepMind Lab2D	2D platform for ML	Apache 2.0	https://github.com/deepmind/lab2d
Delta	DL language/speech processing platform	Apache 2.0	https://github.com/Delta-ML/delta
Determined	DL training platform	Apache 2.0	https://github.com/determined-ai/determined
Egeria	Metadata and governance framework	Apache 2.0	https://github.com/odpi/egeria

Elastic Deep Learning	Cloud training and inference of DL models	Apache 2.0	https://github.com/elasticdeeplearning/edl
Fair Learn	Python toolkit for AI fairness assessment	MIT	https://github.com/fairlearn/fairlearn
Fairseq	Sequence modelling toolkit	MIT	https://github.com/pytorch/fairseq
Feast	Feature store for ML	Apache 2.0	https://github.com/feast-dev/feast
ForestFlow	ML model server	Apache 2.0	https://github.com/ForestFlow/ForestFlow
Gym	Reinforcement learning Python library	MIT	https://github.com/openai/gym
Horovod	DL training framework	Apache 2.0	https://github.com/horovod/horovod
H20	In-memory ML platform	Apache 2.0	https://github.com/h2oai/h2o-3
Keras	DL API	Apache 2.0	https://github.com/keras-team/keras/blob/master/LICENSE
Klio	Audio data pipelines	Apache 2.0	https://github.com/spotify/klio
KNIME Analytics Platform	Data analytics platform	GPL3	https://www.knime.com/knime-open-source-story
Kubeflow	ML toolkit	Apache 2.0	https://github.com/kubeflow/kubeflow
Linkedin Fairness Toolkit	Fairness measurement and bias mitigation library	BSD2	https://github.com/linkedin/LiFT
Ludwig	DL framework	Apache 2.0	https://github.com/ludwig-ai/ludwig
Marquez	Metadata service	Apache 2.0	https://github.com/MarquezProject/marquez
Microsoft Cognitive Toolkit	DL Framework	MIT	https://github.com/microsoft/CNTK
Milvus	Vector database	Apache 2.0	https://github.com/milvus-io/milvus/
ML Agents	ML agents toolkit	Apache 2.0	https://github.com/Unity-Technologies/ml-agents
ML Flow	ML dvp platform	Apache 2.0	https://github.com/mlflow/mlflow/
ML Kit samples	Code samples	Apache 2.0	https://developers.google.com/ml-kit/guides
Monai	Healthcare DL framework	Apache 2.0	https://github.com/Project-MONAI/MONAI
Neuropod	Interface library	Apache 2.0	https://github.com/uber/neuropod
NNStreamer	Neural network streamer	LGPL2.1	https://github.com/nnstreamer/nnstreamer
ONNX	Software format for AI models	Apache 2.0	https://github.com/onnx/onnx
Opacus	ML training library	Apache 2.0	https://github.com/pytorch/opacus
Paddle Paddle	DL Framework	Apache 2.0	https://github.com/PaddlePaddle/Paddle
ParlAI	Model testing framework	MIT	https://github.com/facebookresearch/ParlAI

Pyro	Probabilistic programming language	Apache 2.0	https://pyro.ai
OpenAI Baselines	Reinforcement learning implementations	MIT	https://github.com/openai/baselines
Scikit Learn	ML Python module	BSD3	https://github.com/scikit-learn/scikit-learn
Sparklyr	Scale interface for data science and ML worklflows	Apache 2.0	https://github.com/sparklyr/sparklyr
Streamlit	Datascience and ML app framework	Apache 2.0	https://github.com/streamlit/streamlit
TensorFlow	ML framework	Apache 2.0	https://github.com/tensorflow/tensorflow
TensorLy	Tensor Python library	BSD3	https://github.com/tensorly/tensorly
Torch	ML library	BSD3	http://torch.ch
Zero-shot Object Tracking	Object tracking implementation	GPL3	https://github.com/roboflow-ai/zero-shot-object-tracking

Access to Research Data and EU Copyright Law

by **Linda Kuschel and Jasmin Dolling***

Abstract: With the advent of data-driven science and data-based business models in the 21st century, legal questions surrounding data, data rights and data law have become one of the most discussed topics both for lawmakers and for legal scholars globally. This is true particularly in the European Union, which in recent years has introduced data protection legislation, cybersecurity legislation, legislation regarding digital content and digital services, and more. Within this flurry of legal activity, one area of data law goes surprisingly unnoticed—the generation, ownership and use of research data. The slim attention it receives is disproportionate to its relevance in the digital economy. Not only are research data essential for the development of new technologies, they also feed machine-learning algorithms and are produced in any and all academic institutions. In order to maximize innovative potential, it is essential that researchers operate with legal certainty when using research data. The article seeks to contribute to this aim by exploring the legal framework in which research data can be accessed and used in EU copyright law. First, it delineates the authors' understanding of research data. It then examines the protection research data currently receives under EU and Member State law via copyright and related rights, as well as the ownership of these rights by different stakeholders in the scientific community. After clarifying relevant conflict-of-laws issues that surround research data, it maps ways to legally access and use them, including statutory exceptions, the open science movement and current developments in law and practice.

Keywords: Copyright; research data; freedom of science; open access; Open Science

Recommended citation: Linda Kuschel and Jasmin Dolling, Access to Research Data and EU Copyright Law, 13 (2022) JIPITEC 247 para 1.

A. Copyright and Research: Friends or Foes?

1 The rationale behind copyright law appears as relevant for research data as it is for creative works in the traditional sense: creativity should be incentivized while the embedded information should circulate and be disseminated as freely as possible. The temporary monopoly that copyright protection grants is not intended to deprive the general public of ideas, methods or doctrines,[1] as this would endanger the scientific communication process[2] and societal advancement. Why, then, does copyright often appear to get in the way of conducting research?

2 Arguably, copyright's focus has shifted from promoting intellectual creations towards protecting investments. The standard of creativity is low;[3] related rights grant protection to products such as audio recordings and photographs, which can contain no creativity of their own. The *sui generis* protection of databases, which stems from European

* Prof. Dr. Linda Kuschel, LL.M. (Harvard) holds a junior professorship in civil law, intellectual property law and law and digitization at Bucerius Law School, Hamburg. Jasmin Dolling is a graduate research assistant at Bucerius Law School, Hamburg. We thank Tarmio Frei for valuable research assistance.

1 BGHZ 39, 306 = FCJ 27 March 1963 – I b ZR 129/61 – NJW 1963, 1877, 1878 – *Rechenschieber*.

2 Cf Michael Fehling, 'Verfassungskonforme Ausgestaltung von DFG-Förderbedingungen zur Open-Access-Publikation' (2014) OdW 179, 189.

3 See further infra, B.I.

law, even rewards solely an investment effort. For researchers not versed in the terrain of copyright law, obligations when using or generating data have become increasingly unclear in the face of varied and ever-new types of protection, divergent requirements for protection between and sometimes even within jurisdictions and complex meshes of rightholders. The article therefore seeks to illuminate the role of research data and its useability in European copyright law,[4] presenting a definition of research data (B.), the types of protection they may enjoy (C.), common rightholders (D.), conflict-of-laws problems in international use (E.) and, finally, ways to legally access and use them, including statutory exceptions, the open science movement and current developments in law and practice (F.).

B. Research Data: An Attempt to Clarify

3 Before examining the legal questions that arise when using research data, one must delineate which types of data this term encompasses. A universal definition is not self-evident, as perspectives on what research data are, what form they take and which purpose they have differ between and sometimes even within scientific disciplines.[5] A natural and technical science approach, for example, might define research data as "experimental results, observations and computer-generated information[,] which form the basis for the quantitative analysis underpinning many scientific publications".[6] On the other end of the spectrum, there are initiatives like NFDI4Culture, a consortium for the digitization and integration of research data on material and immaterial cultural heritage. Their understanding of research data includes digital representations of cultural assets such as, eg, paintings, photographs and sketches, 3D models of buildings and musical or stage performances, as well as procedural research data resulting from research on these cultural assets, amongst others.[7]

4 In order to benefit different scientific disciplines, the term research data must therefore be interpreted broadly. For the purposes of this article, research data are thus understood to be objects of information subject to the scientific cognitive process.[8] They can exist at the outset of the research activity as well as be generated, or rather developed through interpretation during its course.

5 Further, the present consideration includes not only digital, but also analogue objects of information, such as handwritten notes or photographs. While it is indubitable that digitization gives rise to new possibilities of production, storage and analysis of research data, not all data are originally digital. Moreover, the assessment of research data's eligibility for copyright protection largely takes place irrespective of whether data exist in analogue or digital form.

C. Layers of Legal Protection

6 Research data can appear in many different shapes and sizes. The assessment of their legal protection (under copyright law) is invariably contingent on their specific manifestation.[9] In the following section, the ways in which research data and EU copyright protection intersect are presented by (I.) charting copyright's core, the protection of works, (II.) exploring related rights and (III.) outlining the *sui generis* right in databases, which indirectly includes even raw data.

4 Additionally, aspects of data (protection) law, patent law or trade secrets law can be of particular relevance. These are beyond the scope of the present article.

5 Cf Thomas Hartmann, 'Urheberrechtliche Schutzfähigkeit von Forschungsdaten' in Jürgen Taeger (ed), *Law as a Service. Recht im Internet- und Cloud-Zeitalter* (OlWIR 2013) 505, 508; Heinz Pampel, Hans-Jürgen Goebelbecker, Paul Vierkant, 're3data.org: Aufbau eines Verzeichnisses von Forschungsdaten-Repositorien. Ein Werkstattbericht' in Bernhard Mittermaier (ed), *Vernetztes Wissen. Daten, Menschen, Systeme* (Forschungszentrum Jülich 2012) 61, 62; Jakob Voß, 'Was sind eigentlich Daten?' (2013) 23 LIBREAS. Library Ideas 4, 6 <https://libreas.eu/ausgabe23/02voss/> accessed 14 March 2022.

6 European Commission, Towards better access to scientific information: Boosting the benefits of public investments in research, Communication from 17 July 2012, COM(2012) 401 final, 3.

7 Torsten Schrade, 'NFDI4Culture', (2022) 5 Politik & Kultur 7; Reinhard Altenhöner et al., 'NFDI4Culture - Consortium for research data on material and immaterial cultural heritage', (2020) 6 Research Ideas and Outcomes, <https://doi.org/10.3897/rio.6.e57036> accessed 5 July 2022.

8 This is in keeping with previous definitory endeavors, such as Art 2(9) Open Data Directive ("[D]ocuments in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results") or the definition posed by the Alliance of German Scientific Organizations' focus initiative digital information ("data generated in the course of scientific projects", cf <www.allianzinitiative.de/archiv/forschungsdaten/> accessed 8 June 2022).

9 BGHZ 112, 243 = FCJ 27 September 1990 – I ZR 244/88 – GRUR 1991, 523, 525 – *Grabungsmaterialien*.

I. Research data as protected works

7 Copyright protects the rights of authors for "works in the literary, scientific and artistic domain".[10] Thus, protection under copyright requires a work. While European copyright directives do not contain an express definition of the term "work", the Court of Justice of the European Union ("ECJ") has developed two conditions that must both be satisfied for copyright eligibility:[11] first, there must be an original subject matter, ie, the author's own intellectual creation; second, only the expression of this creation can be copyright-protected as a work.[12] Assessing whether and when these conditions are fulfilled has largely been left to the Member States to determine on a case-by-case basis; however, the ECJ has ruled on copyright protection in certain constellations, enabling general conclusions on the Court's understanding of these conditions. In *Brompton*, a case for copyright infringement of a folding bicycle able to take three distinct positions, the Court confirmed that copyright protection extends to products whose shape is at least partially necessary to obtain a certain technical result, so long as, through the shape, the author expresses their creative ability by making free and creative choices, so that the shape reflects their personality.[13] In *Cofemel*, respectively, the Court denied copyright protection for (in this case, clothing) designs that, beyond their practical purpose, generate only an aesthetically significant visual effect. The Court held that an aesthetic effect alone was not enough to determine whether a design constitutes an author's intellectual creation, and a subjective aesthetic effect further did not equate to an expression, ie, a subject matter that is existing and identifiable with sufficient precision and objectivity.[14] This case law allows two conclusions to be drawn for research data: first, while research data will often be of a technical, functional nature (eg, the results of a clinical trial or studies of a chemical reaction), this does not in principle exclude them from copyright protection; second, research data must reflect their author's creativity in order to be eligible for protection as copyrighted works.

8 In many academic disciplines, particularly the humanities, research is conducted by analyzing sources including literature, musical compositions, artistic works, photographic works or films, which will generally enjoy copyright protection if they are not already in the public domain. Copyright protection expires seventy years after the author's death (Article 1(1) Copyright Term Directive[15]), or after the death of the last surviving joint author (Article 1(2) Copyright Term Directive). Within this exclusive period, if research data consists of collected pre-existing material, such as literary texts or other creative content, it is likely to be copyright-protected and its use must be in accordance with statutory exceptions or contractual licenses.[16]

9 If research data does not consist of such material that clearly falls into the realm of copyright, its protection depends upon its form; research data that exist in the form of written text can be protected as literary works if they constitute the authors' own intellectual creations. While the threshold for the level of creativity in literary works is relatively low,[17]

10 Sec 1 *Urheberrechtsgesetz* 1965 (Copyright Act Germany); cf also Sec 1 no 2 *Zakon o autorskom pravu i srodnim pravima* 2003 (Copyright Act Croatia); Sec 2(1) *Autorský zákon* 2000 (Copyright Act Czech Republic); Sec 1(2) no 1 *Autoriõiguse seadus* 1992 (Copyright Act Estonia); Sec L112-2 *Code de la propriété intellectuelle* 1992 (Copyright Act France); Sec 2(1) Copyright Act Greece; Sec 1(1) *Törvény a szerzői jogról* 1999 (Copyright Act Hungary); Sec 1(1) *Autorių teisių ir gretutinių teisių* įstatymas 1999 (Copyright Act Lithuania); Sec 1 *Auteurswet* 1912 (Copyright Act Netherlands); Sec 1(1) no 1 *Zakon o avtorski in sorodnih pravicah* 1995 (Copyright Act Slovenia).

11 The ECJ's competency for establishing an autonomous, uniform definition of the term is debated amongst scholars (cf Mireille van Eechoud, 'Along the Road to Uniformity – Diverse Readings of the Court of Justice Judgments on Copyright Work' (2012) 3 JIPITEC 60, paras 90ff; Eva-Marie König, *Der Werkbegriff in Europa* (Mohr Siebeck 2015), 22ff; Haimo Schack, 'EuGH: Kein Urheberrechtsschutz *für* Lebensmittelgeschmack mangels Werkcharakter - Levola/Smilde' (2019) 1 GRUR 75 (note)). The Court deems itself competent because the relevant Directives, particularly Council Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 (InfoSoc Directive), do not expressly place the subject matter into the scope of competency of the Member States (cf ECJ, Case C-310/17 *Hexenkaas* [2018] ECLI:EU:C:2018:899 para 33; ECJ, Case C-5/08 *Infopaq International* [2009] ECR I-06569 para 27).

12 Cf ECJ, Case C-683/17 *Cofemel* [2019] ECLI:EU:C:2019:721 para 29.

13 ECJ, Case C-833/18 *Brompton* [2020] ECLI:EU:C:2020:461 paras 23ff.

14 Cf ECJ, Case C-683/17 *Cofemel* [2019] ECLI:EU:C:2019:721 paras 53f.

15 Council Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights [2006] OJ L372/12.

16 Note that if copyright in a previously unreleased work has expired and this work is then released or communicated to the public for the first time, an exclusive right of exploitation is granted for 25 years (Art 4 Copyright Term Directive).

17 FCJ 15 September 1999 – I ZR 57/97 – GRUR 2000, 144, 145

a text of certain length is generally required. At the same time, there is no fixed word or character limit,[18] theoretically even single sentences[19] or tweets[20] are eligible for protection if the author expresses themself in a particularly creative fashion. For research data in text form describing the results of an experiment, documenting an observation or annotating data for machine learning purposes, such a creative mode of expression will be unlikely and, in any case, hardly wanted.[21] However, creative efforts consisting in expressing complex facts as clearly and precisely as possible are also rewarded.[22] It follows that research data presented in a piece of writing may well enjoy copyright protection—although generally only where there is enough leeway to describe the results found in individual words, and only with regard to their creative expression.[23] Very brief texts predominantly composed of fixed terminology, such as anamnesis reports, are rather unlikely to merit protection. Moreover, the methods, theories and results expressed within the text remain copyright-free.[24]

10 Illustrations of a scientific or technical nature can also be protected works.[25] The examples provided in many of the statutes[26] (in Germany, eg, "drawings, plans, maps, sketches, tables and three-dimensional representations") are visualizations often used in connection with research data. As with texts, a sufficient measure of creative expression is required. This measure is not reached where the representation is purely schematic and dictated by scientific norms.[27] However, copyright protection is not precluded by the content of a representation being of technical nature and the information being presented as clearly as possible.[28]

11 Collections and databases also enjoy copyright protection. Protected collections are "[c]ollections of literary or artistic works such as encyclopaedias and anthologies which, by reason of the selection or arrangement of their contents, constitute intellectual creations [...]."[29] Thus, protection arises from the particular selection and arrangement of elements, not from their content, and relates only to that specific selection and arrangement.[30] The same applies to database works eligible for protection under Article 3(1) Database Directive.[31] They are collections

– *ComicÜbersetzungen II*.

18 Cf Winfried Bullinger, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 2 paras 27f; Axel Nordemann, *Urheberrecht* (Axel Nordemann, Jan Bernd Nordemann et al. eds, 12th edn, W. Kohlhammer 2018), § 2 para 59; Haimo Schack, *Urheber- und Urhebervertragsrecht* (9th edn, Mohr Siebeck 2019), para 202; Ulrich Loewenheim and Matthias Leistner, *Urheberrecht* (Ulrich Loewenheim, Matthias Leistner and Ansgar Ohly eds, 6th edn, C.H. Beck 2020), § 2 para 45.

19 Regional Court of Munich 8 September 2011 – 7 O 8226/11 – GRUR-RR 2011, 447 – *Karl Valentin*. Cf also ECJ Case C-5/08 *Infopaq* [2009] ECR I-06569 paras 47f.

20 Higher Regional Court of Cologne 8 April 2016 – 6 U 120/15 - K&R 2016, 423; Regional Court of Bielefeld 3 January 2017 – 4 O 144/16 - MMR 2017, 641 (in these specific cases, protection was denied for lack of the required level of creativity). Cf also Gernot Schulze, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 2 para 83; Hannes Ludyga, 'Urheberrechtlicher Schutz von Tweets' (2017) 48 AfP 284.

21 Cf Hartmann (n 5) 511; Nordemann (n 18) para 118; Schulze (n 20) para 93. Critical Helmut Haberstumpf, 'Wem gehören Forschungsergebnisse?' (2001) 11 ZUM 819, 821.

22 FCJ 11 April 2002 – I ZR 231/99 – GRUR 2002, 958, 959 – *Technische Lieferbedingungen*.

23 FCJ 21 November 1980 – I ZR 106/78 – GRUR 1981, 352, 353 – *Staatsexamensarbeit*. Cf also Bullinger (n 18) para 57; Schulze (n 20) para 93.

24 BGHZ 39, 306 = FCJ 27 March 1963 – I b ZR 129/61 – NJW 1963, 1877, 1878 – *Rechenschieber*; FCJ 21 November 1980 – I ZR 106/78 – GRUR 1981, 352, 353 – *Staatsexamensarbeit*. Cf also Bullinger (n 18) para 50; Loewenheim (n 18) para 71; Schulze (n 20) para 93.

25 Cf eg Sec 2 no 3 *Urheberrechtsgesetz* 1936 (Copyright Act Austria); Sec 4(3) no 2 Copyright Act Estonia; Sec L112-2 no 12 Copyright Act France; Sec 2(1) no 7 Copyright Act Germany; Sec 2(1) Copyright Act Greece; Sec 5(2) no 12 Copyright Act Slovenia.

26 Sec 2(1) no 7 Copyright Act Germany. Cf also Sec 5(2) Copyright Act Croatia; Sec 4(3) no 2 Copyright Act Estonia; Sec L112-2 no 12 Copyright Act France; Sec 2(1) Copyright Act Greece; Sec 4(2) no 21 Copyright Act Lithuania; Sec 5(2) no 12 Copyright Act Slovenia.

27 Hartmann (n 5) 511.

28 FCJ 10 May 1984 – I ZR 85/82 – GRUR 1985, 129, 130 – *Elektrodenfabrik*.

29 Art 2(5) Berne Convention for the Protection of Literary and Artistic Works. Cf also Sec 6 Copyright Act Austria; Sec 7(1) Copyright Act Croatia; Sec 4(3) no 22 Copyright Act Estonia; Sec L112-3 Copyright Act France; Sec 4(1) Copyright Act Germany; Sec 2(2) Copyright Act Greece; Sec 7(1) Copyright Act Hungary; Sec 4(3) no 3 Copyright Act Lithuania; Sec 10(2) Copyright Act Netherlands.

30 Cf FCJ 7 December 1979 – I ZR 157/77 – GRUR 1980, 227, 230f – *Monumenta Germaniae Historica*.

31 Council Directive 96/9/EC of 11 March 1996 on the legal

"of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Article 1(2) Database Directive). In the context of research, a collection of raw data, such as measurement data from a test series, will generally be comprehensive in nature and therefore not subject to an individual selection; the arrangement in turn will follow logical criteria (eg, time, quantity, size), as the representation should meet scientific standards and be as clear and verifiable as possible. Therefore, there is little room for creative selection or arrangement.[32] The case may be different, eg, in the humanities or cultural studies, where a research database could consist of a selection of poetry[33] (based on individual criteria[34]) or newspaper articles.[35] Yet, the investment or work effort put into a database or the expertise necessary cannot be taken into account in the question of whether a research database constitutes an intellectual creation.[36] However, they play a role in the related *sui generis* right in databases.[37]

12 Computer programs can also be protected by copyright, provided they contain the programmers' own intellectual creation and, as such, reflect a minimum of individuality.[38] Entirely trivial program designs or pre-existing program elements, therefore, are not protected.[39] In any case, protection arises only for the expression of the program, not for its underlying ideas and principles (cf Article 1(2) Computer Programs Directive).[40]

II. Related rights to research data

13 While copyright is granted only for intellectual creations, related rights extend to certain non-creative efforts related to copyright-protected works. For research data, the related rights to photographs and moving pictures and the protection of producers of audio recordings play a particular role.[41]

14 In a number of Member States, photographs and "products manufactured in a similar manner to photographs" are protected.[42] The term photograph encompasses any type of photography, irrespective of its specific imaging technology, and therefore includes, for example, aerial and satellite photographs.[43] Products manufactured in a similar manner are all images produced using radiant energy.[44] These include, eg, infrared images, medical x-ray or ultrasound images, as well as magnetic resonance or computer tomography images, which are particularly relevant for research data.[45]

15 Moreover, sequences of images or sequences of images and sounds that are not protected as cinematographic works, ie, which do not fulfil the requirements for copyright protection, can still receive protection as moving pictures in two Member States.[46] Typically, these are films that merely docu-

protection of databases [1996] OJ L77/20.

32 This view is also supported by Fehling (n 2) 188; Hartmann (n 5) 512; Gerald Spindler, 'KoLaWiss-Gutachten AP 4: Recht' (2009), 30ff.

33 BGHZ 172, 268 = FCJ 24 May 2007 – I ZR 130/04 – NJW 2008, 755, 756 – *Gedichttitelliste I*.

34 Cf Sören Rieger, *Der rechtliche Schutz wissenschaftlicher Datenbanken* (Mohr Siebeck 2010) 101.

35 Higher Regional Court of Hamm 26 February 2008 – 4 U 157/07 – ZUM 2008, 598, 601.

36 ECJ, Case C-604/10 *Football Dataco et al.* [2012] ECLI:EU:C:2012:115 para 42. Cf also Eva-Marie König, *Der Werkbegriff in Europa* (Mohr Siebeck 2015), 18f; Thomas Dreier, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 4 para 11.

37 See infra, C.III..

38 Cf Eva-Marie König, *Der Werkbegriff in Europa* (Mohr Siebeck 2015), 16f; Nordemann (n 18) para 75.

39 FCJ 20 September 2012 – I ZR 90/09 – GRUR 2013, 509 para 25 – *UniBasic–JDOS*; Higher Regional Court of Berlin 6 September 2010 – 24 U 71/10 – ZUM-RD 2011, 544, 547 – *FRITZ!Box*. Cf also Schulze (n 20) para 127.

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

41 See infra, C.III., on the *sui generis* protection of makers of database.

42 This protection is not mandated by EU law, cf Art 6 third sentence Copyright Term Directive. It is granted in Austria (Sec 73 Copyright Act Austria), Denmark (Sec 70 *Ophavsretsloven* 2014 (Copyright Act Denmark)), Germany (Sec 72 Copyright Act Germany), Finland (Sec 49a *Tekijänoikeuslaki* 1961 (Copyright Act Finland)), Spain (Sec 128 *Ley de Propiedad Intelectual* 1996 (Copyright Act Spain)) and Sweden (Sec 49a *Upphovsrättslagen* 1960 (Copyright Act Sweden)).

43 Cf Gernot Schulze, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 72 para 3f.

44 Cf Schulze (n 43) para 6; Dorothee Thum, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 72 para 24.

45 Cf Schulze (n 43) para 6; Thum (n 44) para 24.

46 In Austria, Secs 73(2), 74 Copyright Act Austria, and Germany,

ment an event or a process without employing tools of creative cinematic design.[47] Research data that, for example, capture a test procedure, a natural event or an interview on film, are therefore protected as moving pictures (alongside the protection of the individual film frames as photographs).

16 The most important difference between the protection of photographs or films as works and the related rights for photographs or moving pictures is that the latter do not depend on creative expression and extend to faithful, objective reproductions of events.[48] Therefore, research data in form of images and films can usually elicit protection as photographs or moving pictures (only). The scope of related rights for photographs and moving pictures differs from the protection of copyrighted works primarily through a shorter term of protection granted by the Member States—50 years after publication (or production) rather than 70 years *post mortem auctoris* (pma).[49] In addition, there is a particularity for photographs of works of visual art that are in the public domain. For a long time, it was controversial whether photographic replications of two-dimensional originals, especially photographs faithful to an original painting, could enjoy protection under copyright law.[50] Notably, the legal setting has changed after the adoption of the DSM Directive[51], effective June 6, 2019 (the transposition period ended June 7, 2021). The Directive establishes in its Article 14 that "when the term of protection of a work of visual art has expired, any material resulting from an act of reproduction of that work is not subject to copyright or related rights, unless the material resulting from that act of reproduction is original in the sense that it is the author's own intellectual creation". This precludes photographic replications of works of visual art in the public domain from being protected as photographs; they may only enjoy copyright protection as photographic works if the associated higher standards of creative expression are fulfilled (see supra, B.I.). For research data, this will predominantly not be the case.

17 The Member States can provide for a related right to critical and scientific publications, which is granted for publications that contain works no longer protected by copyright.[52] In Germany, this right is also granted for scientific publications of unprotected texts, such as letters, maps or judicial proceedings, and for works not protected by copyright for other reasons.[53] It requires, however, that there has been scientifically organized activity and (in case the works or texts contained therein, which have been published previously) that they differ significantly from previous editions of the works or texts.[54] Scientifically organized activity requires sighting, organizing and evaluating work, employing scientific methods.[55] The right can be granted for 30 years at most.

18 Finally, research data can exist in the form of audio recordings, such as of interviews, group discussions or nature sounds. Regardless of a possible copyright protection (for example in the case of a creative speech that has been recorded), the production of the audio recording as such is protected under Article 2 lit c InfoSoc Directive.[56] As opposed to the speaker's

Sec 95 Copyright Act Germany. Cf on this Günter Poll, 'Die Harmonisierung des europäischen Filmurheberrechts aus deutscher Sicht' (2003) 4 GRUR Int 290, 293f.

47 Cf Schack (n 18) para 730.

48 Cf Thum (n 44) para 22.

49 Cf for photographs, Sec 74(6) Copyright Act Austria, Sec 70(2) Copyright Act Denmark, Sec 72(3) Copyright Act Germany, Sec 49a(2) Copyright Act Finland, Sec 49a(2) Copyright Act Sweden; for moving pictures, Sec 95 in conjunction with 94(3) Copyright Act Germany, Secs 73(2), 74(6) Copyright Act Austria. This is in synchronicity with the protection terms for related rights established in Art 3 Copyright Term Directive.

50 Cf Schulze (n 43) para 10; Thum (n 44) para 23. This is because even protection only as a photograph must demonstrate at least a small minimum of own intellectual (but not creative) effort, which is not present, eg, in reproductive photocopies or scans (Schack (n 18) para 722; Schulze (n 43) para 9). This fundamental concept was confirmed by the German Federal Court of Justice in its decision *Museumsfotos* (FCJ 20 December 2018 – I ZR 104/17 – GRUR 2019, 284, 286 para 23). In the case at hand, however, the FCJ considered the photographers' decisions on lighting, angle and distance to the photographed painting to be a sufficient intellectual effort for protection as a photograph. According to these standards, research data depicting two-dimensional works (in the public domain), such as in art or media studies, would generally enjoy protection as photographs.

51 Council Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market [2019] OJ L130/92.

52 Art 5 Copyright Term Directive. This right has been introduced in Estonia and Germany, cf Sec 74[1](2) Copyright Act Estonia; Sec 70 Copyright Act Germany.

53 Anne Lauber-Rönsberg, *Urheberrecht* (Hartwig Ahlberg, Horst-Peter Götting and Anne Lauber-Rönsberg eds, 33rd edn, C.H. Beck 2022), § 70 para 5.

54 Cf Sec 70(1) Copyright Act Germany.

55 FCJ 23 May 1975 – I ZR 22/74 – GRUR 1975, 667, 668 – *Reichswehrprozess*.

56 Council Directive 2001/29/EC of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

copyright, the rights of the audio recording's producer expire 50 years after the fixation or, in case of lawful publication or communication to the public within this period, 50 years from the date of the first act of publication or communication, Article 3(2) Copyright Term Directive.

III. Protection of research data in databases

19 The previous sections dealt with research data that have, in different ways, taken a creative form. Raw data, meaning non-edited data such as measurements, do not enjoy copyright protection as such. They can, however, constitute a protected database under Article 3(1), 1(2) Database Directive insofar as they exist in larger number and are ordered systematically.

20 The *sui generis* right for the maker of a database encompasses any "collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means" (Article 1(2) Database Directive) and the "obtaining, verification or presentation" of which requires "qualitatively and/or quantitatively a substantial investment" (Article 7(1) Database Directive). Usually, a research database is a collection of works, data or other individually (electronically or otherwise) accessible elements. "Independency" requires that the elements can be separated from each other without adversely affecting the value of their content.[57] This is intended to prevent an extension of the term "database" to include all items composed of individual components (such as musical compositions, which are made up of musical notes). The elements must make sense independently, not only in their combination.[58] However, the ECJ applies a rather generous standard: the individual data arising from a topographic map (terrain altitude, location of traffic roads etc.) are sufficiently independent, even if the purpose of a map unfolds only in viewing all its elements in combination.[59] For research data, this means that not only a collection of different data, but a single document (such as a drawing of an archaeological excavation site) may already constitute a database—provided that it fulfils the other requirements for protection.

21 The requirement of a systematic or methodical arrangement is intended to distinguish a database from a mere collection of raw data not compiled by organizational criteria.[60] Since research data are compiled according to plausible organizational criteria in order to ensure their scientific useability, this prerequisite is easily fulfilled.

22 Finally, the database must show that there has been a substantial qualitative or quantitative investment. The *sui generis* database right was intended to reward the investment effort of a database producer, thereby creating an incentive to develop "modern information storage and processing systems".[61] An investment cannot only be the expenditure of money, but also of time, work or technical means.[62] In four judgments from November 9, 2004, the ECJ clarified that only investments associated with the creation of the database, ie, obtaining, verifying or presenting the data, are relevant.[63] In this respect, investments serving the generation of data are not considered.[64] For research data, a—not entirely

57 ECJ, Case C-604/10 *Football Dataco et al.* [2012] ECLI:EU:C:2012:115 paras 26f; ECJ, Case C-203/02 *The British Horseracing Board et al.* [2004] ECR I-10415 para 31. Cf also Kirsten Johanna Schmidt and Herbert Zech, 'Datenbankherstellerschutz für Rohdaten?' (2017) 33 CR 417, 418.

58 Schmidt and Zech (n 57) 419.

59 ECJ, Case C-490/14 *Freistaat Bayern v Verlag Esterbauer GmbH* [2015] ECLI:EU:C:2015:735 paras 25f. Critical Matthias Leistner, 'Was lange währt…: EuGH entscheidet zur Schutzfähigkeit geografischer Karten als Datenbanken' (2016) 1 GRUR 42.

60 Cf Rec 21 Database Directive; ECJ, Case C-444/02 *Fixtures Marketing II* [2004] ECR I-10549 para 30; Schmidt and Zech (n 57) 420; Martin Vogel, *Urheberrecht* (Ulrich Loewenheim, Matthias Leistner and Ansgar Ohly eds, 6th edn, C.H. Beck 2020), § 87a para 22.

61 Cf Rec 12 Database Directive.

62 Cf FCJ 1 December 2010 – I ZR 196/08 – GRUR 2011, 724, 725, para 18 – *Zweite Zahnarztmeinung II*; Estelle Derclaye, 'Database Sui Generis Right: What Is a Substantial Investment? A Tentative Definition' (2005) IIC 4ff; Thomas Dreier, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 87a para 12; Schmidt and Zech (n 57) 421.

63 ECJ, Case C-203/02 *The British Horseracing Board et al.* [2004] ECR I-10415, para 31; ECJ, Case C-338/02 *Fixtures Marketing I* [2004] ECR I-10497 para 24; ECJ, Case C-444/02 *Fixtures Marketing II* [2004] ECR I-10549 para 40; ECJ, Case C-46/02 *Fixtures Marketing III* [2004] ECR I-10365 paras 31ff.

64 ECJ, Case C-203/02 *The British Horseracing Board et al.* [2004] ECR I-10415 para 31; ECJ, Case C-338/02 *Fixtures Marketing I* [2004] ECR I-10497 para 24; ECJ, Case C-444/02 *Fixtures Marketing II* [2004] ECR I-10549 para 40; ECJ, Case C-46/02 *Fixtures Marketing III* [2004] ECR I-10365 paras 31ff. Cf also Matthias Leistner, 'ECJ, Case C-203/02 *The British Horseracing Board et al.* [2004] ECR I-10415' (2005) JZ 408, 409 (note).

trivial—distinction between investments in data generation and investments in data obtainment and collection must therefore be made.[65]

23 Partially, the distinction is made by separating data that are "found", ie, pre-existing data and data that are "invented".[66] Only the latter are said to carry the danger of monopolizing information, as the inventor of the data is in the exclusive position to collect them.[67] On the other hand, data that are collected as part of scientific measurements or observations are said to be pre-existing in nature and the expenditure to collect them therefore to constitute an eligible investment.[68] The argument made against this criterion is that in nature, only "potentially semantic information" pre-exists, which needs human perception to be turned into de facto information and, thereby, into data.[69] Indeed, it does not seem entirely plausible to classify factual events as "pre-existing data" before they are documented. Instead, it is proposed to use a criterion of general perpetual accessibility, ie, to ask whether "third parties could, with similar expenditure, create the same data".[70] In case of ephemeral events, such as weather data, the observations could not be replicated and are therefore not perpetually accessible.[71] In principle, these criteria are persuasive and consistent, but they are not free of concerns; at least in the natural sciences, it is questionable whether a parallel observer would, in fact, identify "the same data". Surely, they would concede similar or equal results, but it is uncertain whether the data would be exactly identical. Moreover, the German Federal Court of Justice (FCJ) decided in the context of the motorway tolling system that the data collected within its framework, such as date and duration of drives subject to tolling, are "not created, but only collected and arranged".[72] However, these traffic data are also dynamic processes that can be assessed only in one specific moment. Therefore, the characterization of data as "found" or "invented" is highly difficult. Yet, it is important to keep in mind that, for the database protection right, it is not the nature of the data that is decisive, but rather which kind of investment was made. All investments that are necessary to initiate collectible information, ie, to launch a procedure that leads to information, are not relevant. For measurement data obtained from an experiment in the natural sciences, we must therefore differentiate between investments in the experimental setup and investments in measuring the experimental procedure and result. Only the latter can be taken into account for the *sui generis* database right. The same distinction can be made in social science experiments: costs for mobilizing experimental subjects (eg, recruitment) and the organizational planning of the experiment are irrelevant, while the expenditure of time by researchers documenting the procedures is to be included. Expenses for the processing of collected raw data constitute another area of investment; they are relevant costs for presentation of the data.[73]

24 Not to be included—at least under the aforementioned ECJ case law[74]—are investments in generating "synthetic data". Synthetic data are created in the context of machine learning algorithms with the aim to counterbalance misrepresentations in a given dataset. Over- or under-representation of individual groups (eg, in terms of gender or ethnicity) in a dataset can lead to discriminatory decisions or findings by the algorithm and thus has to be balanced out.[75] Since this kind of adjustment in training data is important as well as desirable, one might consider

65 Cf on this Rieger (n 34) 142ff.

66 Kai Hermes, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 87a paras 49ff; Vogel (n 60) para 53; Leistner, '*The British Horseracing Board et al.*' (n 64) 409; Matthias Leistner, 'Datenbankschutz. Abgrenzung zwischen Datensammlung und Datengenerierung' (2018) 34 CR 17, 20.

67 Leistner, 'Datenbankschutz' (n 66) 20.

68 Leistner, '*The British Horseracing Board et al.*' (n 64) 409.

69 Schmidt and Zech (n 57) 422. On this problem, cf also Timo Ehmann, *Wettbewerbsfreiheit und Investitionsschutz für Datenbanken* (C.H. Beck 2011), 109f.

70 Schmidt and Zech (n 57) 422.

71 Schmidt and Zech (n 57) 422.

72 FCJ 25 March 2010 – I ZR 47/08 – GRUR 2010, 1004, 1005 para 19 – *Autobahnmaut*.

73 Leistner, 'Datenbankschutz' (n 66) 19f. Appearing to dissent, Higher Regional Court of Hamburg 8 June 2017 – 5 U 54/12 – BeckRS 2017, 138204 para 247.

74 Philipp Hacker, 'Immaterialgüterrechtlicher Schutz von KI-Trainingsdaten' (2020) 10 GRUR 1025, 1030 argues for an interpretation of Art 7(1) Database Directive in light of Art 20 of the Charter of Fundamental Rights of the European Union [2012] OJ C326/391, that would allow for the inclusion of investments made in synthetic data for the purposes of balancing a given dataset.

75 This is also listed as one potential requirement related to training data by the EU Commission in its "White Paper on Artificial Intelligence" (COM(2020) 65 final, 19).

incentivizing respective investments by way of the database *sui generis* right, which is currently under revision.[76]

25 As opposed to database *works*, the selection and arrangement of individual elements requires no intellectual, creative effort to award the protection to database producers. It follows that, for research data, the *sui generis* right is much more relevant.[77] The duration of protection, however, is shorter: the protection for databases expires 15 years after publication or 15 years after production of the database, if it was not published within that period (Article 10(1), (2) Database Directive).

26 Similar to collections of works and database works, the protection for databases relates not to the individual data, but rather to the overall result, ie, the database. Therefore, the rightholder has the exclusive right to reproduce, distribute or make publicly available the database as a whole or "a qualitatively or quantitatively substantial part" of it (Article 7(1) Database Directive). However, the use of an insubstantial part of the database can already infringe the database producer's right if it is a "repeated and systematic" act that "runs contrary to a normal utilization of the database or unreasonably impairs the legitimate interests of the producer of the database" (Article 7(5) Database Directive). This "circumvention clause"[78] is intended to prevent systematic access to insubstantial parts of the database resulting in a prohibited use of a substantial part of or even of the entire database.[79] In its 2021 *Melons* judgment, the ECJ clarified that the use of a protected database is infringing if it adversely affects the database maker's investment in obtaining, verifying or presenting the content of the database (ie, constitutes a risk to the possibility of redeeming the investment through the normal operation of the database).[80] This follows from balancing the interests of the parties involved, in order to foster innovation and avoid a too far-reaching right of exclusivity for database makers.

27 The database right shall be further clarified by the proposed Data Act,[81] in which Article 35 holds that the sui generis right "does not apply to databases containing data obtained from or generated by the use of a product or related service" (see below, F.III.).

D. Rights to Research Data: Who and how many?

28 The previous section has shown that research data is almost always protected in some way; due to the rather extensive term of protection, only a fraction of research material is in the public domain. Access to and use of research data is further complicated by uncertainties about ownership and exclusive rights.

I. Authorship and original ownership

29 Particularly in the legal history of continental European copyright systems, the work's author takes center stage.[82] At least initially, copyright law has the genius (single) creator in mind,[83] whom it awards the exclusive rights to their work.[84] If multiple people have created the work, they also hold copyright jointly.[85] The same applies to related rights; here,

76 European Commission, *Communication, Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience* (25 November 2020), COM(2020) 760 final, 14f; European Commission, Communication, *Commission Work Programme 2021* (19 October 2020), COM(2020) 690 final, Annex I, 6b.

77 Cf Hartmann (n 5) 513.

78 ECJ, Case C-203/02 *The British Horseracing Board et al.* [2004] ECR I-10415 paras 84ff.

79 ECJ, Case C-203/02 *The British Horseracing Board et al.* [2004] ECR I-10415 paras 84ff. Cf also Kai Hermes, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 87b para 66.

80 ECJ, Case C-762/19 *CV-Online v Melons* [2021] ECLI:EU:C:2021:434 para 47.

81 European Commission, Data Act Proposal, 23 February 2022, COM(2022) 68 final.

82 Cf only Walter Bappert, *Wege zum Urheberrecht* (V. Klostermann 1962) 105ff; Martha Woodmansee, 'The Genius and the Copyright. Economic and Legal Conditions of the Emergence of the "Author"' (1984) 17 Eighteenth-Century Studies 424; Swedish Royal Commission, *Report on the Copyright to Literary and Artistic Works Bills*, SOU 1956:25 p 85 (authors' works are "their spiritual child").

83 This modern, auctorocentric notion of authorship arose in the eighteenth century in response to authors seeking to proprietarize their then expanding livelihood; this presents a break from the previous view of the author as an instrument, either of the court by which they were employed or of divine powers (Woodmansee (n 82) 425).

84 Cf for example in Austria, Sec 10(1) Copyright Act Austria, in Denmark, Sec 1(1) Copyright Act Denmark, in Estonia, Sec 28(1), (2) Copyright Act Estonia, in Finland, Sec 1(1) Copyright Act Finland, in Germany, Sec 7 Copyright Act Germany, in Ireland, Sec 21 *Copyright and Related Rights Act* 2000 (Copyright Act Ireland).

85 Cf eg Sec 11(1) Copyright Act Austria, Sec 6 Copyright Act

the person that has made the effort is awarded the right.[86] For films, the person that has made the economic and organizational effort of producing the film is entitled to the rights thereto (Article 2 lit d InfoSoc Directive)—the same applies to moving pictures by virtue of Member State legislation.[87] For research data generated by multiple people, the creator or producer of every element must be assessed individually.[88]

30 As seen, the *sui generis* database right is based on the hypothesis that the promise of legal protection furthers investments in the arrangement and structuring of data. Accordingly, the database producer, ie, the person that has made the substantial investment, is awarded the rights to a database eligible for protection, Article 7(1) Database Directive.[89] For university research, this is generally the university itself or a third party in case of funded or commissioned research.[90] Yet, the group of persons eligible for the *sui generis* database protection is restricted in an important way: only nationals of an EU Member State or persons whose habitual residence is located therein as well as companies and firms formed in accordance with the law of a Member State and having their registered office, central administration or principal place of business within the Community benefit from the database right (Article 11(1) and (2) Database Directive).

31 The basic assumption of copyright law, being that individual people create works, often fails to reflect the reality of large research projects.[91] This is because here, *groups of researchers* generally manage the project, and many different people participate in the generation of research data. Besides one or multiple group leaders, doctoral candidates and perhaps also research assistants and non-academic personnel often participate in a project. When the materials protected under copyright or related rights are assembled in a large database, a conglomerate is created, to which many different people have rights.[92]

II. Derivative rights

32 Legal systems in the Anglo-American copyright tradition allow not only for the transfer of copyright[93] but also for the initial ownership of an employer (work made for hire-doctrine).[94] Where these copyright regimes acknowledge moral rights,[95] they are—although not alienable—waivable.[96] Due to their roots in the right of personality, continental European author's rights systems, on the other hand, take, a different approach. Copyright consists of economic and moral rights that are always vested

Denmark, Sec 30(1) Copyright Act Estonia, Sec 6 Copyright Act Finland, Sec 8(1), (2) Copyright Act Germany, Sec 7(1) Copyright Act Greece, Sec 22(1), (4) Copyright Act Ireland, Sec 12(1) Copyright Act Slovenia.

86 Cf Thomas Dreier, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), Pre §§ 70ff para 13; Justine Pila and Paul LC Torremans, *European Intellectual Property Law* (1st edn, Oxford University Press 2016), 294.

87 Cf Sec 95 in conjunction with Sec 94 Copyright Act Germany; Sec 73(2) in conjunction with Sec 74(1) Copyright Act Austria. Cf also FCJ 6 February 2014 – I ZR 86/12 – GRUR 2014, 363, 364, para 23; Gernot Schulze, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 95 para 2.

88 Cf BGHZ 112, 243 = FCJ 27 September 1990 – I ZR 244/88 – GRUR 1991, 523, 525 – *Grabungsmaterialien;* Bernhard Ulrici, 'Kooperation in der Wissenschaft: Das Recht am und auf das Arbeitsergebnis' (2015) 48 WissR 318, 319f; Bernhard Ulrici, 'Geistiges Eigentum in Forschungsverbünden' (2018) OdW 129, 131.

89 Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' (7 September 2018), 5ff, <https://ssrn.com/abstract=3245937> accessed 19 September 2022; Michael Beurskens, 'Schranken des rechtlichen Schutzes von Datenbanken (Balancing Public and Private Interests in Database-Protection)', *Center for Business & Corporate Law Research Paper Series No. 0003* (21 November 2004), 51ff, <https://ssrn.com/abstract=646664> accessed 19 September 2022.

90 Anne Lauber-Rönsberg, Philipp Krahn and Paul Baumann, 'Gutachten zu den rechtlichen Rahmenbedingungen des Forschungsdatenmanagements' (2018), 5.

91 Cf on this Florian Möslein, 'Privatrechtliche Regelsetzungsfragen der wissenschaftlichen Kooperationsform: Angebot des Gesetzgebers oder selbstgestaltetes Recht?' (2018) OdW 99, 101.

92 Cf on the organization of access to research and research data generated during academic research projects *infra*, F.II.

93 Sec 120(1) Copyright Act Ireland; Sec 90(1) *UK Copyright, Designs and Patents Act* 1988 (Copyright Act UK).

94 Sec 23(1)(a) Copyright Act Ireland; Sec 11(2) Copyright Act UK. Notably, this rule is also employed in Sec 7 Copyright Act Netherlands.

95 Cf Calvin D Peeler, 'From the Providence of Kings to Copyrighted Things (and French Moral Rights)' (1999) 9(2) Ind Int'l & Comp L Rev 423; Cyrill P Rigamonti, 'Deconstructing Moral Rights' (2006) 47(2) Harvard Int L J 353; Stig Strömholm, 'Droit Moral – The International and Comparative Scene from a Scandinavian Viewpoint' (2002) 42 Scandinavian Stud L 217.

96 Sec 116(1) Copyright Act Ireland; Sec 87(2) Copyright Act UK.

in the author and may not be waived.[97] However, a closer examination reveals that the author's rights systems differ, too. In Germany, for example, copyright is construed monistically, economic and moral rights being an integrated whole, and the transfer of copyright[98] is thus precluded per se.[99] In France, commercial rights and moral rights are seen to be two separate pillars of copyright law, only the latter being inextricably linked to the creator's person, the former transferable.[100] However, even in countries where copyright is not transferable, third parties can be granted a right of use to the work, which may be extensive. Rights can either be granted explicitly via a contract of rights of use or arise implicitly from a private-law employment relationship or a public-law service relationship.[101] A number of particularities arise for (copyright-protected) research data produced at academic institutions.

1. Academic professors

33 The freedom of science guaranteed in many Member States' constitutions declares scientific research to be an autonomous area, free of government control,[102] so as not to endanger the role of research and teaching in furthering progress and understanding.[103] From this, we can deduce that the general rule for works created during the course of employment in most Member States, according to which the employer obtains rights of use in works created by the employee or is considered as their owner,[104] cannot be applied to works of academic professors without restrictions.[105] Other independently working researchers, such as private lecturers, adjunct professors or visiting lecturers, must be equated to academic professors.[106]

34 In this regard, Latvia has taken a pioneering role by introducing a Law on Scientific Activity stipulating that scientists, including academic professors, hold the exclusive rights to their research, insofar as there is no contractual agreement to the contrary.[107] While other states have similar statutes applicable to patents or utility models,[108] an explicit regulation for other IP rights to scientific research has thus far been lacking.

97 Cf Schack (n 18) paras 343f, 1114f.

98 In the majority view, the same applies to photographs. For German law cf Schulze (n 43) para 16; Thum (n 44) para 125. The rights of the producers of audio recordings (Sec 85(2) first sentence Copyright Act Germany) and of producers of films (Sec 95 in conjunction with 94(2) first sentence Copyright Act Germany), on the other hand, are transferrable.

99 Sec 29(1) Copyright Act Germany. Cf also Sec 23(3) Copyright Act Austria, Sec 42(1) Copyright Act Croatia, Sec 9(1), (3) Copyright Act Hungary.

100 Secs L121-1, L122-7 Copyright Act France. Cf also Sec 11(2) and (3) Copyright Act Estonia in conjunction with Sec 39 Constitution of the Republic of Estonia, Sec 12 Copyright Act Greece, Secs 14, 38 Copyright Act Lithuania; Sec 70 Copyright Act Slovenia.

101 Sec L113-9 Copyright Act France; Sec 43 Copyright Act Germany and, for computer programs, Sec 69b Copyright Act Germany; Sec 9(2) Copyright Act Lithuania.

102 Cf Sec 68 *Ustav Republike Hrvatske* 1990 (Croatian Constitution); Sec 77 *Danmarks Riges Grundlov* 1953 (Danish Constitution); Sec 38 *Eesti Vabariigi põhiseadus* 1992 (Estonian Constitution); Sec 5(3) *Grundgesetz* 1949 (German Constitution); Sec X *Magyarország alaptörvénye* 2011 (Hungarian Constitution); Sec 113 *Satversme* 1922 (Latvian Constitution); Sec 42 *Lietuvos Respublikos Konstitucija* 1992 (Lithuanian Constitution); Ch 2 Sec 18 *Regeringsformen* 1974 (Swedish Instrument of Government).

103 For Germany, this follows from BVerfGE 35, 79, 113 = German Federal Constitutional Court 29 May 1973 – 1 BvR 424/71 and 325/72 – NJW 1973, 1176. Cf on this Klaus F Gärditz, 'Die grundrechtliche Stellung der Wissenschaftlerinnen und Wissenschaftler in der Hochschulorganisation' (2016) 49 WissR 349, 357f.

104 Jurisdictions that transfer rights of use include Lithuania, Slovenia, Germany and Hungary. The rights of use may be obtained for a limited time (eg for 5 years in Lithuania, Sec 9 Copyright Act Lithuania, or for 10 years in Slovenia, Sec 101 Copyright Act Slovenia) or unlimitedly (eg in Germany, Sec 43 Copyright Act Germany, or Hungary, Sec 30 Copyright Act Hungary). A notable exception is Croatia, in which rights of use remain with the employee unless specified otherwise by law or contract (Sec 76 Copyright Act Croatia). All of these legislative rules are subject to differing contractual agreements. Jurisdictions that consider the employer as author include Ireland (Sec 23a Copyright Act Ireland) and the Netherlands (Sec 8 Copyright Act Netherlands).

105 Cf BGHZ 112, 243 = FCJ 27 September 1990 – I ZR 244/88 – GRUR 1991, 523, 525 – *Grabungsmaterialien*; Thomas Dreier, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 43 para 12; Haberstumpf (n 21) 825f; Peter W Heermann, 'Der Schutzumfang von Sprachwerken der Wissenschaft und die urheberrechtliche Stellung von Hochschulangehörigen' (1999) 6 GRUR 468, 474f.

106 Cf Dreier (n 105) para 12; Haberstumpf (n 21) 827; Heermann (n 105) 473.

107 Sec 8(3) *Zinātniskās darbības likums* 2005.On the definition of 'scientist', cf Sec 5(1), (3) of the Law.

108 Such as the German *Arbeitnehmererfindungsgesetz* 1957 or the Danish *Bekendtgørelse af lov om arbejdstageres opfindelser* 2012.

35 Yet, not all research data that is produced by academic professors necessarily falls within the scope of the privilege. In Germany, the privilege applies only to pure research.[109] Insofar as the creation of research data occurs at least partly in fulfilment of official duties, such as generating a patient file that is also used for research purposes, the employer is entitled to a right of use.[110] Where they generate research data within the scope of a certain commissioned research, such as in cooperation with a commercial company, researchers must generally also grant a right of use to their commissioners.[111]

36 If research data are collected on a larger scale and gathered in a research database, a *sui generis* database protection may exist. Generally, as previously established, the higher education institution or the commissioner or third-party funder is entitled to this protection. In this case, scientific freedom could make a reverse-direction impact: so as not to endanger the success of the research and to leave the decision of how and whether the data are used in future projects to the project-leading scientists, they should be granted a simple right of use to the *sui generis* database right.

2. Non-academic personnel

37 Especially in large-scale research projects, non-academic personnel may be deployed and commissioned with generating research data. If they do so, they also obtain possible rights thereto. This group of people includes, for example, medical technical assistants or student assistants. As their work is carried out fully bound by instructions, researchers' privileges stemming from the freedom of science do not apply.[112] Thereby, generally following from the employment contract, the employer obtains the exclusive rights to the protected materials. It has been proposed to grant the right of use to the research group leader, if the research results arose under their instruction.[113] However, since it is still the employer who has the right of direction, it appears reasonable to grant both—instructing researcher and employer—rights of use in these situations. This solution takes into account the economic interests of the employer and is in consistency with the database right on the one hand. While on the other hand, the further development of the research project is secured by granting the instructing researcher a right to use.[114]

3. Research assistants

38 Scientific freedom benefits not only academic professors: "every person acting or seeking to act scientifically is entitled to [it]".[115] This means that the employer is not granted a right of use to research data produced by research assistants in the scope of their own research, such as for academic qualifications.[116] For results of work carried out bound by instruction, however, the same principles as for non-academic personnel apply (cf supra, D.II.2.). This distinction can sometimes be difficult in larger research endeavors, such as in medical research. A variety of researchers of different hierarchies are regularly involved, working simultaneously on an overall project and on their own research as part of a sub-issue. In this case, origin and purpose of the specific research data are decisive: if it is material gathered while bound by instruction and supplied to the overall project, rights of use to it are granted. However, the employer does not obtain rights of use to research data gathered independently and texts (such as a dissertation) by the research assistant. With regard to the question of who obtains the rights of use, the same applies as for non-academic personnel (D.II.2.).

4. Externals (esp. external doctoral candidates)

39 Authors or rightholders that are not in employment or service relationships with an institution, such as external doctoral candidates and students, generally

109 Artur-Axel Wandtke, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 43 para 26.

110 FCJ 26 October 1951 – I ZR 93/51 – GRUR 1952, 257 – *Krankenhaus-Kartei*.

111 Ulrici, 'Kooperation in der Wissenschaft' (n 88) 328.

112 Cf BGHZ 112, 243 = FCJ 27 September 1990 – I ZR 244/88 – GRUR 1991, 523, 525 – *Grabungsmaterialien;* Haberstumpf (n 21) 827; Lauber-Rönsberg/Krahn/Baumann (n 90) 4.

113 Cf Haberstumpf (n 21) 827. Potentially with participation in a possible profit (cf Dreier (n 105) para 12; Haberstumpf (n 21) 827).

114 This functional approach can also be found in the decision BGHZ 112, 243 = FCJ 27 September 1990 – I ZR 244/88 – GRUR 1991, 523, 527 – *Grabungsmaterialien*.

115 BVerfGE 35, 79, 112 = German Federal Constitutional Court 29 May 1973 – 1 BvR 424/71 and 325/72 – NJW 1973, 1176, 1176.

116 Cf Dreier (n 105) para 12; Haberstumpf (n 21) 827; Heermann (n 105) 472; Lauber-Rönsberg/Krahn/Baumann (n 90) 4.

are not obliged to grant rights of use to the materials they create.[117] This is self-evident and unproblematic for texts produced for the purpose of academic qualification, such as dissertations. Often, however, these externals, particularly external doctoral candidates, are involved in generating research data for the collaborative project.[118] While they often do not receive compensation, they can access the research data pool and use it for their own research. Assuming that, nevertheless, these externals would not have to grant rights of use to the data they generate would lead to significant issues, eg, when the research database is intended to be made accessible to the public. It is possible to construe the supervision agreement as a *sui generis* contract, from which arises, *inter alia*, that the doctoral candidate grants rights of use to the research data produced by them for the overall project. This would presumably be compatible with the broad definition that the German FCJ gives of an employment relationship for the purposes of copyright, under which it suffices that the author "acts, in a more or less strongly dependent relationship, for the exploitation purposes of another", with the "intended purpose" of the work being decisive.[119] In favor of the external doctoral candidate, the contract could in turn give rise to protection and fiduciary duties of the supervising researcher. As such, it would for example have to be assured that the external doctoral candidate actually receives access to the data relevant for their research, especially when the supervisor changes institutions in the interim. Ideally, the parties' potential rights and obligations would be determined at the beginning of the cooperation. In doing so, for example, an arrangement would have to be made in case the supervision is terminated prematurely (in mutual agreement or otherwise).

5. Digression: Research cooperations

40 For research data created of research cooperations, the abovementioned generally applies, as well as potential explicit arrangements in research and development contracts. Despite the enormous scientific and economic relevance of research cooperations, jurisprudence and literature in this area are rare.[120] Proposals for a specific legal structure to be newly created for research cooperations are thus welcome.[121] Advantages of a cooperation structure with legal capacity would include the cooperation itself being the holder of the *sui generis* database right and concluding employment contracts in its own name.[122] Potential rights of use would fall directly to the research cooperation. Moreover, the cooperation structure could persist despite individual researchers withdrawing due to, eg, leaving the institution.[123] This way, access to the research data could be permanently ensured, benefiting the research project's success.[124] At the same time, concerns of scientific freedom related to the (continued) use of research data should be safeguarded via appropriate governance structures,[125] rather than battled out on the level of copyright rights of use.

E. International Research and Conflict of Laws: Aggravating the Problem

41 Particularly for international researchers, eg, visiting scholars, research fellows or visiting student researchers, the question of which country's copyright law applies to their research and their contribution to a larger research project can be both difficult to answer and decisive in determining which protection they receive and in what ways they can, in turn, use others' research data. The European conflict of laws rules apply where a court in a Member State is dealing with a case involving a conflict of laws, eg, where a German researcher working in a French institution claims an infringement of their research data by a third party located in the Netherlands. It

117 Cf Haberstumpf (n 21) 828; Heermann (n 105) 475.

118 On this, see also Ulrici, 'Kooperation in der Wissenschaft' (n 88) 147.

119 FCJ 22 February 1974 – I ZR 128/72 – GRUR 1974, 480, 482 – *Hummelrechte*.

120 Cf Möslein (n 91) 99. Cf also Nils Heide, 'Patentschutz und Patentlizenzen in Forschungskooperationen' (2013) InTer 2, who relates the lack of jurisprudence, besides the existing legal uncertainty, to the fact that possible disputes are more likely carried out before arbitral tribunals for reasons of secrecy.

121 Wolfram Eberbach, Peter Hommelhoff and Johannes Lappe, 'Eine Kooperationsform für die Wissenschaft' (2017) OdW 1, 5ff. See also Stefan J Geibel, 'Rechtsform und Zurechnungen zwischen Transparenz und Abschirmwirkung am Beispiel der Wissenschafts- und Forschungskooperationen' (2018) OdW 87; Möslein (n 91) 99.

122 Cf also Eberbach/Hommelhoff/Lappe (n 121) 8f.

123 Christoph Kumpan, 'Die Governance einer Forschungskooperationsgesellschaft – Struktur, Kompetenzen und Verfahren' (2018) OdW 115, 117.

124 Cf on this also BGHZ 112, 243 = FCJ 27 September 1990 – I ZR 244/88 – GRUR 1991, 523, 527 – *Grabungsmaterialien*.

125 See on this Kumpan (n 123) 117ff.

can lead to third countries' laws being applicable, even though they are not Member States (principle of universal application, Article 2 Rome I, Article 3 Rome II).

42 The law applicable to *infringements* of IP rights is determined by the conflicts rule of Article 8(1) Rome II, which follows the *lex loci protectionis* principle—the law of the country for which the plaintiff seeks protection is applicable.[126] The applicability of Article 8 Rome II is, however, debated in particular with regard to preliminary questions in copyright infringement proceedings. While Article 15 Rome II determines the scope of the laws applicable under the Regulation's conflicts rules, it is unclear whether this extends to the existence of copyright (and related rights) and its initial ownership.[127] The practical effect of denying applicability of Article 8 Rome II to these areas of copyright is that recourse to the conflict of laws rules of the competent Member States must be made. Often, Member States' respective conflicts rules will also apply the *lex loci protectionis* principle, so that identical results are achieved.[128] Yet, some Member States—most of which also follow the universality principle instead of the territoriality principle in questions of existence and initial ownership of copyright[129]—traditionally adhere to the rule of *lex originis* to questions of creation and initial ownership and would thus apply the law of the state in which the work was first made lawfully accessible to the public, or, if unpublished, the author's personal status.[130] The latest endeavor to provide unified conflict of laws rules for intellectual property, the Kyoto Guidelines, follows a third path and suggests that initial ownership in copyright and related rights should be governed by the law of the state with the closest connection to the creation of the work (cf Kyoto Guidelines 2020, Guideline 20(2)).[131]

43 For *contractual obligations* in connection with copyright, the general rules of Article 3, 4 Rome I apply.[132] These grant priority to the parties' choice of

126 Cf Rec 26 first sentence Rome II; ECJ, Case C-170/12 *Pinckney* [2013] ECLI:EU:C:2013:635. For the sake of completeness, note that for industrial property rights protected EU-wide (such as EU trade marks), Art 8(2) Rome II supersedes Art 8(1), which determines EU law, or, in case of gaps, the law of the place where the event which gave rise to the harm occurred, to be applicable.

127 Josef Drexl, *Münchener Kommentar zum BGB*, vol 13 (Franz Jürgen Säcker et al. eds, 8th edn, C.H. Beck 2021), Art 8 Rome II paras 177ff; Nerina Boschiero, 'Infringement of Intellectual Property Rights. A Commentary on Article 8 of the Rome II Regulation' (2007) 9 YPIL 87, 102f.

128 This is the case, eg, in Germany, Austria and France (cf for Germany, Regional Court of Munich I, Judgment of 14 May 2012, Case no. 21 O 14914/09, BeckRS 2012, 13691; for Austria, Austrian Supreme Court, Judgment of 17 December 2013, Case no. 4 Ob 184/13g, ZUM-RD 2014, 607, 610; for France, French Court of Cassation, Judgment of 10 April 2013, Case no. 11-12508, GRUR Int 2013, 955 (this judgment marks a shift in the French conflicts rule, which had previously applied the right of the country of origin)). On other Member States, see Boschiero (n 127) 99f; Toshiyuki Kono, 'Jurisdiction and Applicable Law in Matters of Intellectual Property' in Karen B Brown and David V Snyder (eds), *General Reports of the XVIIIth Congress of the International Academy of Comparative Law* (Springer 2012), 393, 410f; Pedro A de Miguel Asensio, 'The Private International Law of Intellectual Property and of Unfair Commercial Practices: Convergence or Divergence?' in Stefan Leible and Ansgar Ohly (eds), *Intellectual Property and International Private Law* (Mohr Siebeck 2009) 137 para 11. For completeness' sake, it should be noted that results may differ with respect to the nature of the conflicts rule – while Member States' autonomous conflicts rules may deem a state's entire law to be applicable and therefore allow *renvoi* (this is the case, eg, in Germany), Rome II excludes rules of private international law from referrals (cf Art 24 Rome II). Therefore, while the same state's law is applicable both under Rome II's and under Member States' conflicts rules, the latter includes the referred state's rules on conflict of laws, which may in turn provide for a different rule and therefore deem another law applicable (cf Drexl (n 127) para 176).

129 Michael Grünberger, 'Das Urheberrechtsstatut nach der Rom II-VO' 108 (2009) ZVglRWiss 134, 150.

130 These include Greece, Portugal and Romania (Art 67 *Νόμος Πνευματική Ιδιοκτησία* 1993 (Copyright Act Greece); Art 48(1) *Código civil* 1966 (Civil Code Portugal); Art 60 Romanian Private International Law Act); cf de Miguel Asensio, 'The Private International Law of Intellectual Property' (n 128) para 11; Katharina de la Durantaye, *Rome Regulations Commentary* (Gralf-Peter Calliess and Moritz Renner eds, 3rd edn, Wolters Kluwer 2020), Art 8 Rome II para 3.

131 This is assumed to be the state in which the person who created the subject matter of the work was habitually resident at the time of creation. For the existence, scope and transferability of IP rights, as well as their infringement, the Kyoto Guidelines follow the *lex loci protectionis* principle (cf Kyoto Guidelines, Guidelines 19, 25.).

132 Employment contracts with research institutions will usually fall within the scope of Art 8 Rome I. For researchers in public service relationships (such as state university professors), private law (and thus, Rome I) applies insofar as they do not exercise sovereign powers. Cf Dieter Martiny, ***Münchener Kommentar zum BGB***, vol 13 (Franz Jürgen Säcker et al. eds, 8th edn, C.H. Beck 2021), Art 1 Rome I para 6; Peter Mankowski, *Europäisches Zivilprozess- und Kollisionsrecht*, vol 1 (Thomas Rauscher ed, 5th edn, Otto Schmidt 2021), Art 20 Brussels Ia Regulation, para 79ff; Ulrich Magnus, *Internationales Vertragsrecht 1* (Julius von Staudinger ed, Sellier de Gruyter 2021), Art 8 Rome I para 47.

law. If no choice of law was made,[133] they alternatively provide for connections based on the type of contract (Article 4(1) Rome I). Yet, contracts dealing with copyright, such as licensing agreements or assignments, may fall under multiple contract types and therefore be difficult to categorize.[134] In the absence of a specific contract type, the law of the country "where the party required to effect the characteristic performance of the contract has his habitual residence"[135] will be applicable under Article 4(2) Rome I. However, establishing the characteristic performance in contracts related to copyright can be equally difficult due to their wide variety and differing levels of complexity.[136] While it appears evident that the author's or rightholder's performance is characteristic when it is given in exchange for financial remuneration, the determination is less clear when the other party itself is obligated to perform specific actions, such as to exploit a work or exercise rights granted to it. The situation becomes even more complicated if one contract is concluded between multiple parties (granting, for example, exploitation rights to multiple persons to use the work or when multiple authors assign their rights to another party). Often, therefore, the law applicable to IP contracts will be determined on a case-by-case basis under Article 4(4) or under Article 4(3), as the law of the country with which the contract is most closely connected.[137] This could be the country of the author or copyright holder, the country of the other party (eg, licensee or assignee), the country for which protection exists, or another country depending on the specifics of the contract. Similarly, the Kyoto Guidelines provide that, in the absence of a choice of law by the parties, contracts dealing with IP granted for more than one state (other than employment contracts) are governed by the law of the state with which the contract is most closely connected (Kyoto Guidelines, Guideline 22(2)). Connecting factors include the common habitual residence of the parties, the habitual residence of the party effecting the characteristic performance,[138] and the habitual residence of one of the parties when this habitual residence is located in one of the states covered by the contract. Employment contracts in employment relationships where employees may create intellectual property should be governed, in the absence of a choice of law by the parties, by the law of the state in which or from which the employee habitually carries out their work in performance of the contract (Kyoto Guidelines, Guideline 23(3)).

44 In international research projects, where a large number of researchers collaborate in creating research data that may be protected by copyright or related rights, Articles 4(1) and 4(2) Rome I cannot provide satisfactory results. The closest connection must therefore be determined under Article 4(4). We submit that the countries of the collaborating researchers cannot provide the closest connection, because this would result in different countries' laws applying simultaneously. The law of the country in which the research is conducted (eg, if there is one research institution) appears to be better suited—it falls short, however, if multiple institutions collaborate and research is conducted multi-nationally. In this case, there may be need to identify the main seat of a research project, such as the leading institution.

F. Access and Usability: Current Practices and Future Solutions

45 The practical need for access to research and research data goes far beyond its current accessibility.

133 A choice of law can also be implied by other terms of contract, cf Art 3(1) second sentence Rome I. On requirements to assume implied choice of law, see Dieter Martiny, *Münchener Kommentar zum BGB*, vol 13 (Franz Jürgen Säcker et al. eds, 8th edn, C.H. Beck 2021), Art 3 Rome I paras 46ff; Richard Plender and Michael Wilderspin, *The European Private International Law of Obligations* (5th edn, Sweet & Maxwell 2020, paras 6-026ff.

134 Kono (n 128) 410f; Paul LC Torremans, 'Licences and Assignments of Intellectual Property Rights under the Rome I Regulation' (2008) 4 JPIL 397, 403; Pedro A de Miguel Asensio, 'Applicable Law in the Absence of Choice to Contracts Relating to Intellectual or Industrial Property Rights' (2008) 10 YPIL 199, 207ff, examining a number of specific IP contracts to determine whether and where they fall with regards to Art 4(1) Rome I.

135 The habitual residence of natural persons is their center of life, which requires residence for a certain time. If they are acting within the scope of their business activity, which includes dependent employment, their principal place of business is decisive. International researchers will generally only be with an institution for a finite period of time with the intention of returning to their home country or relocating elsewhere after the research has been completed. This *animus revertendi* has the effect of applying the law of the researcher's home country, rather than the law of the country in which the researcher is currently located, cf Georg John, 'Der Begriff des gewöhnlichen Aufenthaltes und seine Bedeutung im europäischen Privat- und Zivilverfahrensrecht (Teil I)' (2018) 2 GPR 70, 78; Marc-Philippe Weller and Alix Schulz, 'Unterhaltsklage nach Kindesentführung: Zuständigkeit am „unrechtmäßigen" gewöhnlichen Aufenthalt des Kindes?' (2015) 2 IPRax 176, 179f.

136 Kono (n 128) 410f; Torremans (n 134) 403f; de Miguel Asensio, 'Applicable Law in the Absence of Choice' (n 134) 207ff.

137 Torremans (n 134) 404.

138 The Guidelines acknowledge that, in case of complex IP contracts, it is not always possible to identify a characteristic performance (cf Kyoto Guidelines, 52, para 41).

This is illustrated by the advent of so-called 'shadow libraries', most famously Sci-Hub, whose self-proclaimed aim is "to provide free and unrestricted access to all scientific knowledge" and which boasts a collection of over 88 million pdf files.[139] The website violates copyright and related rights by bypassing access limitations of established scientific websites, allowing users to access existing research at no cost. Other initiatives, like the Internet Archive,[140] merely act as digital archives of cultural artifacts such as books, images or audio recordings, also including internet sites themselves. Through its "Open Library", the Internet Archive provides free downloads of public domain works and digital lending of modern books. A third type of platform, like Researchgate or SSRN, operates more like a repository rather than a library and enables researchers themselves to share their publications, if they so wish. It is highly disputed whether these business models are in compliance with the rules of copyright law.[141] However, the popularity of such websites (Sci-Hub claims that in June 2022, over 10 million papers were downloaded around the world; at the time of completion of this article, nearly 2 million papers had been downloaded via SSRN in the last 30 days)[142] evidences a practical need to facilitate low-threshold access to scientific knowledge.

46 Currently, research data can be used lawfully either where such use is allowed under a statutory exception or limitation or where the authors themselves have permitted such use factually or contractually. The second option is relevant in particular for research conducted at universities and some independent research institutions, which adopt so-called open science policies. In keeping with the EU's legislative trend, future rights of use tailored to research data are also conceivable.

139 Cf <https://sci-hub.hkvisa.net/> accessed 5 July 2022; <https://sci-hub.ru/about> accessed 5 July 2022.

140 Cf <https://archive.org/about/> accessed 5 July 2022.

141 The Internet Archive was sued in the State of New York by four major US publishers (Hachette, Harper Collins, Wiley and Penguin Random House), claiming that its "Controlled Digital Lending" program infringes the publishers' copyright and is not covered by fair use or the first sale doctrine (Hachette Book Group, Inc. et al. v. Internet Archive, Case No. 1:20-CV-04160-JGK); Researchgate was sued in Germany by several publishers from the "Coalition for Responsible Sharing", led by Elsevier and the American Chemical Society, for making available several publications on the platform (LG München I, 31.1.2022 – 21 O 14450/17).

142 Cf <https://sci-hub.ru/stats> accessed 5 July 2022; <https://papers.ssrn.com/> accessed 12 July 2022.

I. Statutory exceptions and limitations

47 Perhaps most importantly, a number of uses of research data are permitted by law without needing to acquire a license from the rightholder. While such statutory exceptions do not apply specifically to research data, they include certain of its uses within their broader scope. If the data are used for scientific research or educational activities, the mandatory exception for text and data mining for the purposes of scientific research (Article 3 DSM Directive)[143] and the facultative exceptions for scientific research (Article 5(3) lit a InfoSoc Directive)[144] can apply. Researchers can rely on these exceptions both when using and archiving pre-existing works in a research database, as well as using research data generated by others (within certain boundaries). Further, the right of quotation provided in Article 5(3) lit d InfoSoc Directive can enable not only the collection of preexisting research data itself, but also the use of these data within one's own scientific research.

48 The exception for scientific research applies to the methodical pursuit of knowledge in a broad sense, including (but not limited to) research conducted by university professors, research institutions and research assistants.[145] The exception's scope is determined by the Member States when transposing the InfoSoc Directive into national law.[146] According to Section 60c(1) of the German Copyright Act, "up to 15 per cent of a work [or an object protected by related rights] may be reproduced, distributed and made available to the public for the purpose of non-commercial scientific research", for a specifically limited circle of persons for their personal scientific research (number 1) or for individual third persons

143 Romain Meys, 'Data Mining Under the Directive on Copyright and Related Rights in the Digital Single Market: Are European Database Protection Rules Still Threatening the Development of Artificial Intelligence?' (2020) 5 GRUR Int. 457, 465.

144 Frederik Leenen, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), InfoSoc Directive Art 5 para 101.

145 Thomas Dreier, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 60c para 1.

146 Art 5(3) lit a InfoSoc Directive stipulates only certain minimum requirements: The work must be used for the sole purpose of scientific research; the source, including the author's name, should be indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved. On Member State's implementation, cf Sec 19(2) Copyright Act Estonia; Sec 60c Copyright Act Germany; Secs 22, 58(5) Copyright Act Lithuania; Sec 9(1) lit h Copyright Act Malta; Sec 44 *Autorský Zákon* 2015 (Copyright Act Slovakia).

insofar as this serves the monitoring of the quality of scientific research (number 2). For example, a group of researchers can set up a shared database in which (up to 15 per cent of) sections of relevant monographs are made available. Also, "illustrations, isolated articles from the same professional or scientific journal, other small-scale works and out-of-commerce works" may be used fully (paragraph 3).[147] This means that pre-existing works can also be included in a research database (within the permitted scope). However, this research database can then only be made available to a personally distinct group of researchers or for the purposes of monitoring the results of the research by third persons.

49 Section 60c(2) of the German Copyright Act allows the reproduction of a work on a larger scale (75 per cent), but only for personal scientific research, meaning the used extracts of works cannot be made available to others within a research database.

50 Not only do researchers deal with individual works and related rights, they also use text and data mining to automatically search and analyze large quantities of text and data.[148] Although text and data mining as such, ie, the automated evaluation alone, is not relevant to copyright law,[149] it requires data to be in a machine-readable format (corpus), which generally necessitates a reproduction of the material.[150] Moreover, in the context of machine learning algorithms it might be necessary to annotate and adjust the text or data before using it for the training of the system.[151] The DSM Directive establishes a uniform European foundation for text and data mining for the purposes of scientific research (Article 3 DSM Directive) and allows it, in limited scope, for other purposes (Article 4 DSM Directive). In Germany, it is implemented in Section 60d Copyright Act (revised), and in Austria in Section 42h Copyright Act. Section 60d of the German Copyright Act permits both potential reproductions of the source material (paragraph 2, first sentence), as well as making the corpus available to the public for a specifically limited circle of persons for their joint scientific research, or to individual third persons for the purpose of monitoring the quality of scientific research (paragraph 4, first sentence). This exception, however, applies only to material to which a lawful access already exists; it does not create a "claim for access to protected source material".[152] The revised provision also allows for the material reproduced in the area of scientific research to be permanently stored and retained (Article 3(2) DSM Directive, Section 60d(5) Copyright Act Germany).

51 The exceptions both in the DSM Directive and the InfoSoc Directive privilege non-commercial research (Article 2(1) lit a var 1 DSM Directive, Article 5(3) lit a InfoSoc Directive). The non-commercial character of a research project is not forfeited by third-party funding or by the prospect of a profitable publication.[153] The DSM Directive also privileges research with commercial gains, insofar as potential profits are fully reinvested into the research (Article 2(1) lit a var 2 DSM Directive).[154]

52 Finally, the right of quotation can allow the use of research data protected as works or under related rights within one's own research, even if this research does not pass the originality threshold to warrant copyright protection itself.[155] To fall within the right of quotation, the data must be used to illustrate an assertion, defend an opinion or allow an intellectual comparison between the data and the assertions of its user.[156] The requirements are context-specific, meaning they are determined on a case-by-case basis by considering the specific use at hand. For quotations of text, the user must "establish a direct and close link between the quoted

147 For articles from non-scientific journals, however, the per cent boundary of para 1 (or para 2) applies.

148 BT-Drs 18/12329, 40. On the scientific relevance of text and data mining, see only Benjamin Raue, 'Rechtssicherheit für datengestützte Forschung' (2019) 8/9 ZUM 684; Louisa Specht, 'Die neue Schrankenregelung für Text und Data Mining und ihre Bedeutung für die Wissenschaft' (2018) OdW 285.

149 Cf BT-Drs 18/12329, 40; Rec 9 DSM Directive.

150 Cf Katharina de la Durantaye, 'Neues Urheberrecht für Bildung und Wissenschaft. Eine kritische Würdigung des Gesetzentwurfs' (2017) 6 GRUR 558, 561; Raue (n 148) 685.

151 Cf Lisa Käde, *Kreative Maschinen und Urheberrecht* (Nomos 2021) 65ff, 70f; Björn Steinrötter and Lina-Marie Schauer, 'Text und Data Mining, Forschung und Lehre' in Malek Barudi (ed), *Das neue Urheberrecht* (1st edn, Nomos 2021) para 5; Philipp Hacker, 'Computer-Generated Works im deutschen Urheberrecht? Überlegungen zur Schutzfähigkeit von KI-Erzeugnissen in komplexen technischen Entwicklungsprozessen' in Linda Kuschel, Sven Asmussen and Sebastian Golla (eds), *Intelligente Systeme – Intelligentes Recht* (Nomos 2021) 234f.

152 BT-Drs 18/12329, 41.

153 BT-Drs 18/12329, 39. Cf also Thomas Dreier, *Urheberrechtsgesetz* (Thomas Dreier and Gernot Schulze eds, 7th edn, C.H. Beck 2022), § 60c para 6; Stefan Lüft, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 60c para 12.

154 Cf on this also Raue (n 148) 690.

155 ECJ, Case C-145/10 Painer [2011] ECLI:EU:C:2011:798, para 137.

156 ECJ, Case C-516/17 Spiegel Online [2019] ECLI:EU:C:2019:625, para 78.

work and his own reflections, thereby allowing for an intellectual comparison to be made with the work of another" and "the use of the quoted work must be secondary in relation to the assertions of that user".[157] This exception is voluntary for the Member States.[158] A particular limitation for research data is that the exception requires the cited works to have previously been lawfully made available to the public by the rightholder.[159] This may not always be the case, particularly in a natural sciences context, as research data may often be shared only between peers, without satisfying the requirements for being made available to the public (ie, allowing access by an indeterminate number of potential recipients and involving a fairly large number of people).[160]

II. Open Science

53 Besides the statutory exceptions for the handling of research data, which may be unclear and/or too restrictive in individual cases, a rising number of researchers subscribe to so-called open science policies to allow the exploitation of their research and research data in a controlled form. Most higher education institutions have introduced open access and open science policies, which require a portion of or even all research conducted under the aegis of the institution to be accessible freely, ie publicly and free of charge, via the internet (eg in open access research journals and/or institutional or disciplinary digital repositories).[161] This is also the case for many prestigious research funding organizations or programs, such as the European Research Council's funding under the Horizon Europe program.[162] Where open science policies exist, free accessibility extends to research data as such, as well as research software and teaching materials. These policies are intended to benefit the free dissemination of knowledge and foster good scientific practice, as well as reduce the cost of scientific publication.

54 Depending on the policy, primary or secondary open access publication is required.[163] In case of secondary open access publication, ie after the research (data) has already been published in a periodical scientific journal,[164] Germany grants a digital second publication right (Section 38(4) Copyright Act Germany), which gives authors the right to republish the accepted manuscript of their work 12 months after first publication. This right requires the work to have been created within the course of research financed at least in half by public funding and to have been published in a periodical collection (appearing at least bi-annually). The republication cannot serve a commercial purpose. This right cannot be excluded in the contract between author and (first) publisher. While this right is an important initiative on the way to more open access-friendly legislation, it is arguably too narrow to be truly effective. Particularly in the natural sciences, the waiting period of 12 months may cause the work to lose relevance before being available for republishing, the manuscript version is not ideal to encourage academic discussion as citations are made difficult (the relevant journal page numbers are not available), and the exception imposes artificial requirements excluding a large number of research papers ab initio.

55 In 2015, a German university has amended its bylaws to make secondary open access publication a mandatory obligation for its researchers; this has been challenged and is currently under judicial review with the German Federal Constitutional Court.[165] If there is no institutional policy in place,

157 ECJ, Case C-516/17 Spiegel Online [2019] ECLI:EU:C:2019:625, para 79.

158 Note that the right of quotation has been made mandatory in the context of user generated content on online content-sharing service platforms by Art 17(7)(2) lit a DSM Directive.

159 ECJ, Case C-145/10 Painer [2011] ECLI:EU:C:2011:798, para 127; ECJ, Case C-516/17 Spiegel Online [2019] ECLI:EU:C:2019:625, para 89.

160 ECJ, Case C-392/19 VG Bild-Kunst [2021] ECLI:EU:C:2021:181, para 31; ECJ, Case C-263/18 Tom Kabinet [2019] EU:C:2019:1111, para 66; ECJ, Case C-265/16 VCAST [2017] EU:C:2017:913, para 45.

161 Cf on the definition of open access, Budapest Open Access Initiative, Declaration (2002) <https://www.budapestopenaccessinitiative.org/read/> accessed 19 September 2022.

162 Horizon Europe, the EU's research and innovation funding programme from 2021-2027, requires all scientific publications to be open access and research data management under the FAIR Principles. Cf European Research Council, *Open Research Data and Data Management Plans – Information for ERC grantees*, 2022, p 4.

163 Discussing the constitutional permissibility of publication obligations in funding eligibility conditions in depth, Fehling (n 2) 179.

164 As opposed to scientific publication series, handbooks, monographs, commentaries and similar singular publications (Artur-Axel Wandtke and Eva-Marie König, *Praxiskommentar Urheberrecht* (Artur-Axel Wandtke and Winfried Bullinger eds, 5th edn, C.H. Beck 2019), § 38 para 20), but also online repositories such as JSTOR or SSRN.

165 The case is on file with the Higher Administrative Court of Baden-Württemberg, which in 2016 suspended the proceedings to request a ruling from the Federal Constitutional Court (Case

the researcher as copyright holder can decide whether they wish to publish open access or not; however, university target obligations or financing incentives may influence this decision.[166] The research (data) so published may be used lawfully as determined by the repository rules; usually, there will be no legal limitations beyond authors retaining control over the integrity of their work and their proper acknowledgement and citation.[167] This is often achieved by employing Creative Commons licenses generally or Open Data Commons licenses specifically for data collections.

56 Not all research data can or should be made openly available. However, where open access is not provided to research data, they should at least be processed in a sustainable way, ensuring access and reusability by others. One way to arrive at this goal is by implementing the "FAIR Data Principles" (Findable, Accessible, Interoperable and Reusable).[168]

III. Current developments and future desiderata

57 Currently, a number of endeavors at the EU level target an improvement of access to data and data governance. For instance, the Data Act proposal published in February of this year clarifies the lack of protection of machine-generated data under the *sui generis* database right, which had thus far been subject to legal uncertainty.[169] Further, the proposal for a Data Governance Act aims to enable the reuse of public-sector data subject to the rights of others. Although the Act does not apply to IP rights, public-sector bodies are encouraged to exercise their copyright in a way that facilitates re-use.[170] This may point to public sector-conducted or -financed research using open access policies on a larger scale in the future. In 2019, the recast Open Data Directive had already stressed the importance of open data licensing for public sector data.[171] Finally, the EU's 2020 IP Action Plan recognizes researchers' struggle with IP protection, promising to boost IP asset management by increasing know-how and to "[take] steps [...] to ensure that publicly funded IP is used in a fair and effective manner".[172]

58 But individual organizations are also becoming more aware of the benefits of research data management. Research institutions increasingly provide model contracts or templates containing clear provisions on rights to research data and individual project agreements are becoming more common. Nevertheless, this is by no means standard practice for research projects and should be continually encouraged at the institutional level.

59 Adjacent to these piecemeal developments largely resting on recommendations and organizations' own actions, there is a case to be made for creating clear and universal rules on IP protection for research data. Of course, such legislation would need to respect fundamental rights, specifically fall within the limits of the freedom of science, property rights and the freedom of business (particularly of scientific publishers).[173] The abovementioned Latvian Law on Scientific Activity could well serve as a model for EU-level legislation, as it gives clear definitions for research workers and sets out unambiguous rules for intellectual property ownership to research.

---

no. 9 S 2056/16), cf on this Manfred Löwisch, 'Streit um die Zweitveröffentlichungspflicht geht zum Bundesverfassungsgericht' (2018) OdW 43. To date, the Constitutional Court has not ruled. Generally on secondary publication obligations in higher education bylaws, see Volker M Haug, 'Open Access in Baden-Württemberg: Rechtswidriger Zweitveröffentlichungszwang zwischen Urheber- und Hochschulrecht' (2019) OdW 89.

166 When evaluating research proposals for Horizon Europe grants, the quality and appropriateness of open science practices is taken into account. Cf European Commission, Directorate-General for Research and Innovation, *Horizon Europe, Open Science: Early Knowledge and Data Sharing, and Open Collaboration* (2021) https://data.europa.eu/doi/10.2777/79699 accessed 19 September 2022.

167 Budapest Open Access Initiative, Declaration (2002) (n 161). For Open Data, cf the Open Knowledge Foundation's Open Definition <http://opendefinition.org/> accessed 19 September 2022.

168 FAIR Guiding Principles for scientific data management and stewardship, <www.go-fair.org/fair-principles/> accessed 19 September 2022.

169 European Commission, Data Act Proposal, 23 February 2022, COM(2022) 68 final, p 5, Rec 84, Art 35.

170 European Council, Council Approved Data Governance Act Proposal, 4 May 2022, PE-CONS 85/21, Rec 17, 18.

171 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, Rec 44.

172 European Commission, IP Action Plan, 25 November 2020, COM(2020) 760 final.

173 For an in-depth assessment under German law, see Philipp Overkamp and Miriam Tormin, 'Staatliche Steuerungsmöglichkeiten zur Förderung des Teilens von Forschungsdaten', (2022) OdW 39.

G. Conclusion

60 There are many ways in which research data can be protected under EU copyright law, either as copyrighted works or via related rights. Even in areas where the law is not harmonized, parallel protection regimes can often be found in the Member States. This protection can impede the access to and use of research data, particularly in the context of larger research groups as well as in international and multi-organizational research projects. These complexities could be reduced by introducing legal instruments that take into account the particularities of research activity and research data, thereby providing a more functional approach to copyright in this area. The Latvian Law on Scientific Activity is a lighthouse in this regard, as it gives clear definitions for researchers and sets out unambiguous rules for intellectual property ownership of research. The current momentum of data-related regulation on the EU level could well be used to further this aim.

61 In the predominant absence of specific rules for access to and use of research data in the EU and its Member States, it is crucial that researchers themselves negotiate contractual rules to govern their legal relationships. The protection copyright offers for research data proves useful only where it is actively wielded, rather than subsequently applied. Conducting research together with other researchers, assistants and non-academic personnel without individual project agreements may create a thicket of rights that can jeopardize the success of the project. Researchers should therefore take care to negotiate the rights to their data, as well as who and how it can be used in advance within the legal framework provided. Research institutions should make it their practice to provide guidelines and complete detailed contractual rules on research data with their students and personnel, in order to minimize legal uncertainty and ensure the copyright regime does not become an encumbrance for future developments.

Wiki (POCC) authorship: The case for an inclusive copyright

by **Sunimal Mendis***

Abstract: Public open collaborative creation (POCC) constitutes an innovative form of collaborative authorship that is emerging within the digital humanities. At present, the use of the POCC model (or Wiki authorship model) can be observed in many online creation projects the best known examples being Wikipedia and free-open source software (FOSS). This paper presents the POCC model as a new archetype of authorship that is founded on a creation ideology that is inclusive and as such, challenges the existing individualistic conception of authorship in exclusivity-based copyright law. Based on a comparative survey of the copyright law frameworks on collaborative authorship in France, the UK and the USA, the paper demonstrates the inability of the existing framework of exclusivity-based copyright law to give adequate legal expression to the relationships between co-authors engaged in collaborative creation within the POCC model. It proposes the introduction of an 'inclusive' copyright to the copyright law toolbox which would be more suited for giving legal expression to the qualities of inclusivity and dynamism that are inherent in these relationships.

Keywords: authorship; POCC; Wiki authorship model; FOSS

Recommended citation: Sunimal Mendis, Wiki (POCC) authorship: The case for an inclusive copyright, 13 (2022) JIPITEC 267 para 1.

A. Introduction

1 Since its inception, the evolution of modern copyright law has been characterized by a dominant narrative of exclusive property rights.[1] Exclusivity can be defined as the quality of a legal right in a tangible or intangible good that precludes any person other than the rightholder from benefitting from the utilities of that good.[2] The essence of copyright law is the exclusive copyright that is granted to an author over the work created by them. The exclusive copyright enables the author to reserve the utilities of that work (e.g. reproduction, adaptation, communication to the public etc.) to their own individual enjoyment

* Assistant Professor in Intellectual Property Law, TILT, Tilburg University, The Netherlands. Email: sunimal.mendis@gmail.com. This article presents research carried out within the framework of the INCLUSIVE project ("Inclusive rights: A new model to organize legal relations to shared resources in tangible property and intellectual property") funded by the European Research Council (Grant agreement no: 616103). I would like to thank Prof. Séverine Dusollier (Chief Investigator of the INCLUSIVE project) for her guidance in formulating the notion of POCC authorship and the concept of an inclusive copyright.

1 As noted by Dagan, the right to exclude is the defining feature of property rights and is ingrained in the conventional narrative of property (and not just in the narrative of intellectual property rights). Hanoch Dagan, 'Exclusion and Inclusion in Property' in Hanoch Dagan (ed.) *Property: Values and Institutions* (Oxford Scholarship Online 2011) 37, at p 37.

2 Gérard Cornu exclusive as « De ce qui écarte de la jouissance d'un droit toute autre personne que la titulaire » [That which precludes any person other than the owner of the right of enjoyment thereof]. Gérard Cornu, 'Exclusif,ive'. Vocabulaire juridique (11th edn. PUF 2016) 430 (author's translation).

(i.e. 'mine not yours'). It further grants the author an affirmative claim to prevent any other person from benefitting from the utilities of the copyright protected work without their authorization.[3]

2 The exclusivity-based narrative is reinforced by copyright's individualistic conception of authorship that frames authorship as an individual relationship subsisting between a specific person (i.e. author) and the expression (i.e. work) that is created by that person (or originates from them). This individualistic conception of authorship is at the core of copyright law's perception of an author as a solitary romantic genius who is the sole creator of unique works that originate from their own individual intellect.[4]

3 This paper posits that *Wiki* authorship—an emerging model of collaborative creation in the digital humanities—challenges this individualistic conception of authorship and consequently the dominant exclusivity-based narrative of copyright law. It further argues that, in order to give legal expression to the relationships that exist among authors engaged in the creation of a work under the *Wiki* authorship model, it is necessary to introduce a parallel notion of an 'inclusive' copyright to the copyright law toolbox. In doing so, it proposes a paradigm shift in the conception of copyright as a tool for individual ownership ('mine *not* yours') to a property right that is capable of collective ownership by an open community of rightsholders ('mine *and*yours').

4 The notion of an 'inclusive' copyright that is advanced in this paper, is based on the concept of an 'inclusive' property right proposed by Dusollier.[5] Dusollier envisages an inclusive property right as a legal relationship between a person and a tangible or intangible good that is characterized by the absence of a power of exclusion and a plurality of persons being included in the collective use of that good.[6] Accordingly, Dusollier's concept of an 'inclusive' property right is based on two key characteristics: (a) a legal right to a good that is held by a plurality of persons which is characterised by the collective enjoyment of the utilities of that good; (b) an absence of a power or privilege on the part of any person to exclude an owner of the inclusive property right from benefitting from the utilities of the good. 'Inclusivity' can thus, be described as the quality of a legal right to benefit from all or some utilities of a tangible or intangible good that is held by a plurality of legal subjects in a collective way without any person having the power to exclude the rightholder from such benefit. Dusollier, acknowledges that inclusivity is a spectrum and identifies different types of property regimes that display varying degrees of inclusivity. For instance, the public domain—where inclusivity arises through an absence of exclusive property rights—would be located at one end of the inclusivity spectrum while copyleft licenses such as GPL and *Creative Commons* (CC)—that use contract as a tool to include others in the collective enjoyment of a good subject to exclusive copyright—would be located towards the other end.[7] The inclusive copyright that is proposed in this paper is situated at a mid-point on this spectrum. As elaborated in greater detail in section D.I below, it refers to a copyright that is shared among an open and indeterminate community of contributing authors which grants to each of them an equal and symmetrical right to collectively benefit from the utilities of a work (good), without one single author having a power or privilege to exclude another author from such benefit. Unlike

3 This is in accordance with Hohfeld's conception of jural relations, wherein a legal right is defined as an affirmative claim held by one person over another. Wesley Newcomb Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' 23 Yale Law Journal (1913) 55. This also reflects the Kantian notion of property as an individual right that "is rightfully mine (*meum iuris*) with which I am so connected that another's use of it without my consent would wrong me". Immanuel Kant, *Gesammelte Schriften*. Edited by the Königliche Preußische Akademie der Wissenschaften (Reimer/de Gruyter 1900) at p 245 (as cited in David James, 'Independence and Property in Kant's Rechtslehre' 24 British Journal for the History of Philosophy (2016) 302, at p 312).

4 Martha Woodmansee, 'On the Author Effect: Recovering Collectivity' 10 Cardozo Arts & Entertainment Law Journal (1992) 279, at p 279. *See also* Martha Woodmansee and Peter Jaszi, 'Introduction' in M. Woodmansee and P. Jaszi (Eds), *The Construction of Authorship: Textual Appropriation in Law and Literature* (Duke University Press 1994) pp 2-3.

5 S. Dusollier and J. Rochfeld, 'Propriété Inclusive ou Inclusivité', in M. Cornu, F. Orsi et J. Rochfeld (eds.), *Le Dictionnaire des Biens Communs* (PUF, 2017) 983. *See also,* S. Dusollier, 'Intellectual property and the bundle-of-rights metaphor' in P. Drahos, G. Ghidini & H. Ullrich (eds.) *Kritika: Essays in Intellectual Property* (Edward Elgar 2020)146; S. Dusollier, *Inclusive properties* (Cambridge University Press, forthcoming). It is noted that similar the notions of inclusive property rights have been advanced by several scholars such as Hanoch Dagan in relation to property rights, ibid (n 1) and by Geertrui Van Overwalle in relation to patent rights, *see* Geertrui Van Overwalle 'Inventing Inclusive Patents. From Old to New Open Innovation' in P. Drahos, G. Ghidini & H. Ullrich (eds.) *Kritika: Essays on Intellectual Property* (Edward Elgar 2015) 206.

6 Ibid, Dusollier and Rochfeld at p 985 (author's translation).

7 Ibid.

in the case of copyleft licenses, here the quality of inclusivity materializes through a positive legal right that is held *in rem* by each inclusive copyright holder (as opposed to a right *in personam* that is granted by the holder of an exclusive copyright by contract). Yet, unlike goods in the public domain, inclusive copyright does not denote an absence of exclusive rights. Rather, inclusive copyright grants each rightholder a positive right of ownership in the common work (good) that can be 'defensively' enforced to prevent the exclusive appropriation of the work by any person (including any other inclusive copyright holder) and to prevent its use in violation of generally applicable terms and conditions. Thus, the inclusive copyright will comprise a dimension of exclusivity that, unlike the classical notion of exclusive property rights, is not directed towards preserving the individual enjoyment of the work (good) but rather aims to sustain and perpetuate the inclusive and collective enjoyment of the common work (good) over time by preventing its exclusive appropriation.[8]

5 This paper proceeds in four parts. Part B describes the *Wiki* authorship model—which I refer to as authorship carried out under Public Open Collaborative Creation (POCC) model—as a new archetype of collaborative creation that is based on a creation ideology that is collective and inclusive. Part C analyses the inability of the existing notion of exclusive copyright to give adequate legal expression to the relationships between persons engaged in the creation process under the POCC model. Part D proposes the development of an 'inclusive' copyright that would be more suited for giving legal expression to the relationships among the authors of a POCC work. The concept of an inclusive copyright is still at a very early stage of development and many issues relating to its scope, area of application and modalities of enforcement remain unresolved; part E provides a glimpse into some of these issues and discusses possible strategies for their resolution.

B. POCC as a new archetype of collaborative creation

6 POCC is a term I coined to describe a collaborative creation model that is steadily gaining in popularity within the digital humanities. I define it as creation taking place through the contributions of a multiplicity of persons under a model of sequential creation, resulting in the production of a literary, artistic or scientific work, which remains in a continuous state of change and development over an undefined period of time.[9] As per the structure of the POCC model, a plurality of authors collaborate in the creation of a single work by modifying and building upon expression contributed by each other within a process of incremental creation. This process of creation takes places within an open-ended time span which allows it to continue over an indefinite period of time. The term 'work' is used here to denote that the intellectual content created under a POCC model of authorship would typically display sufficient originality to qualify for copyright protection.

7 At present, the use of the POCC model can be observed in many collaborative creation projects that result in the production of a diverse array of literary, artistic and scientific content. The best-known examples of such creation projects are the online encyclopaedia *Wikipedia*[10] (hence the term *Wiki* authorship) and free open-source software (FOSS) creation projects such as *VLC*[11] and *Debian*[12]. In addition, it is used for the creation of collaborative fictional stories by the *Folding Story*[13] platform and *This Exquisite Forest*[14] project used it in the creation of collaborative graphic art.

8 Ibid.

9 Sunimal Mendis, 'POCC: A new archetype of authorship' 22 Journal of World Intellectual Property Law (2019) 59, at p 60.

10 Wikipedia: the free encyclopedia <https://en.wikipedia.org/wiki/Wikipedia> accessed 5 May 2022.

11 VLC media player <http://www.videolan.org/vlc/> accessed 5 May 2022.

12 Debian operating system <https://www.debian.org/intro/about.en.html> accessed 5 May 2022.

13 Folding Story < http://foldingstory.com/> accessed 5 May 2022. The Folding Story project uses the POCC model to allow members of the public to collaborate in the creation of fictional stories over an Internet platform. Each contributor writes a line or a paragraph of a story that is added to by other contributors, resulting in the creation of a short story or fictional narrative that is in a constant state of development.

14 This Exquisite Forest <www.exquisiteforest.com/concept> accessed 5 May 2022. *This Exquisite Forest* is a collaborative graphic art project conceived by artists Chris Milk and Aaron Koblin and produced by the Tate Modern in London and the Google Data Arts team. It used the POCC model to create graphic animations exploring specific themes that built upon each other, along a chain of sequential creation. Members of the public were able to participate in the creation process over an Internet platform as well as by using digital drawing tablets that were made available to visitors at the Tate Modern. The project was operative from July, 2012 to August, 2014.

8 To illustrate the POCC model better, let us consider the creation process of a *Wikipedia* article (or 'page' as they are commonly referred to). Every *Wikipedia* article on a given topic is created by a multiplicity of contributors each building upon the expression contributed by previous contributors by means of adding to, modifying and in some instances even overwriting that expression. Even though the individual contributions may differ both in quantitative and qualitative terms, each contribution constitutes an integral step in the creation process. While this sequential creation process results in a literary work that remains in a constant state of evolution it nevertheless succeeds in preserving the work's character as a single coherent work that, taken as a whole, will qualify for copyright protection at each stage of its evolution.[15]

9 In many cases, the contributions will take the form of 'tweaks' or very incremental changes or additions to existing content. This process of 'tweaking' is a hallmark of the POCC process and the following example that is based on the creation process of the headnote of the *Wikipedia* article on 'Alexander the Great' serves to elucidate this process.[16]

10 In November 2004, **Participant 'T'** makes the following contribution to the headnote.

...Alexander the Great, was one of the most successful military commanders of the Ancient world

In May 2007, **Participant 'U'** revises it as follows,

...Alexander the Great, was one of the most successful Ancient Greek military commanders of the Ancient world in history

In June 2007, **Participant 'V'** deletes the words 'Ancient Greek' as he feels it confuses the sense of what the sentence seeks to convey,

...Alexander the Great, was one of the most successful Ancient Greek military commanders in history

In January 2011, **Participant 'X'** partially re-writes the sentence,

Alexander was known to be undefeated in battle and is considered one of the most successful commanders of all time

11 For the moment, the POCC model is employed in the digital sphere and is primarily used in the creation of digital content over Internet platforms.[17] The genesis of the POCC model within the digital sphere is understandable as the potential for connectivity and networking offered by the Internet and the tools and infrastructure offered by digital technology for collaborative and incremental creation[18] provide the perfect conditions for the model to flourish. Nonetheless, it is important to note that the POCC model has the potential to be used in non-digital offline settings as well, for example in the creation of street art and graffiti and in the creation of music through jamming sessions. Indeed, it is possible to draw comparisons between the POCC model and folkloric traditions of storytelling, indigenous art and traditions of religious discourse. This gives rise to the interesting question whether the POCC model is in fact a completely 'new' archetype of authorship or whether it in fact signals the re-emergence of an ancient form of collaborative creation within the digital sphere.[19]

12 The value of the POCC model lies in its ability to harness the skills, talents, knowledge and experience of a large and diverse group of otherwise unconnected individuals from all corners of

15 Although it may be possible to separately identify the different stages of an article's evolution (in the form of different 'versions' of the same article), it would nevertheless be artificial to compartmentalize each point in the incremental creation process into a series of separate static works. Such compartmentalization would also go against the objective of the creative endeavour which is to create a single yet evolving work, as opposed to the modification of an existing work so as to create a series of new versions that are separate from each other.

16 Please note that, although the example is based on the actual editing history of the headnote of the *Wikipedia* article (page) on Alexander the Great, it has been heavily edited and the names and identification information of the contributors have been changed.

17 One exception was *This Exquisite Forest* project that enabled members of the public to engage in creation under the POCC model through digital drawing tablets that were made available onsite at the Tate Modern, London.

18 For example, editing tools, the possibility of maintaining logs on creation history.

19 This discussion is not within the scope of this paper. However, it suffices to say that anthropological and ethnographic studies carried out on the folkloric tradition of authorship and the creation of the Jewish Talmud point to substantial similarities with the POCC model of creation. *See* for example David Atkinson, *The English Traditional Ballad* (Routledge 2002); Eva Axer, 'Choir of the Minds', in Mathias Denecke, Anne Ganzert, Isabell Otto, Robert Stock (eds), *Reclaiming Participation* (Transcript 2016); David Buchan, *The Ballad and the Folk* (Routledge 1972); TF Henderson, *The Ballad in Literature* (Cambridge University Press 1912); Hermann L Strack and Gunter Stemberger *Introduction to the Talmud and Midrash* (Markus Bockmuehl tr, Fortress Press 1992); Jacob Neusner *Invitation to the Talmud* (Wipf & Stock 2003).

the globe within a common collaborative value creation endeavour. These individuals are motivated to participate in the POCC process through non-pecuniary considerations[20] such as peer-recognition[21], the enjoyment derived from engaging in a creative pursuit within a community of like-minded individuals and the satisfaction derived from collaborating in the creation of content that generates social, cultural and scientific value.[22]

13 The capacity of the POCC model to direct and sustain a large-scale collaborative authorship effort resulting in high-quality creative output is testified by the *Wikipedia* project that has matched (and in some respects overtaken) other conventional encyclopaedias published by corporate entities both in terms of comprehensiveness (number of articles and range of disciplines)[23] and reliability.[24] Similarly, *VLC* software has overtaken *Windows Media Player* in relation to robustness, sophistication and simplicity of use.[25] Thus, the POCC model of authorship holds significant implications for the democratization of creative production by reflecting a commons-based approach[26] to creation that challenges the traditional market-based creative economy.

I. The POCC model

14 The POCC model can be described in relation to four main characteristics: openness, chain of sequential creation[27], creative autonomy and ideology. As will be discussed below, these characteristics imbue POCC authorship with an inclusivity and dynamism that differentiates it from conventional models of collaborative authorship that are recognized by copyright law.

1. Openness

15 The quality of openness can be described in relation to two aspects of the POCC process.

20 Volker Wittke and Heidemarie Hanekop, 'New Forms of Collaborative Innovation and Production on the Internet' in Volker Wittke and Heidemarie Hanekop (eds.) *New Forms of Collaborative Innovation and Production on the Internet: An Interdisciplinary Perspective* (Göttingen University Press 2011) 12.

21 *See* Andrea Forte and Amy Bruckman, *Why do people write for Wikipedia? See* Andrea Forte and Amy Bruckman, *Why do People Write for Wikipedia?* Georgia Institute of Technology (2005) <http://www.andreaforte.net/ForteBruckmanWhyPeopleWrite.pdf> accessed 5 May 2022. *See also* Ruediger Glott, Philipp Schmidt and Rishab Gosh, *Wikipedia Survey-Overview of Results* (UNU-MERIT 2010) 9-10. <http://www.ris.org/uploadi/editor/1305050082Wikipedia_Overview_15March2010-FINAL.pdf > accessed 5 May 2022.

22 *See* Why do people write articles for Wikipedia, despite not getting any recognition or incentives?' (*Quora* February 22, 2016) <https://www.quora.com/Why-do-people-write-articles-for-Wikipedia-despite-they-dont-get-any-recognition-or-incentives> accessed 5 May 2022. *See* also Alexander Hars and Shaosong Ou, 'Working for Free? Motivations of Participating in Open Source Projects', Proceedings of 34th Annual Hawaii International Conference on System Sciences (HICSS-34) 25; Georg Von Krogh, Stefan Haefliger, Sebastian Spaeth, and Martin W Wallin, 'Carrots and rainbows: Motivation and social practice in open source software development (2012) MIS quarterly 649.

23 *Wikipedia* has overtaken other conventional encyclopaedias in terms of the number of articles, range of disciplines and number of languages in which it is available. *See* 'Wikipedia: Size Comparisons' <https://en.wikipedia.org/wiki/Wikipedia:Size_comparisons> accessed 5 May 2022.

24 *See* I. Casebourne, C. Davies, M. Fernandes, N. Norman, *Assessing the accuracy and quality of Wikipedia entries compared to popular online encyclopaedias: A comparative preliminary study across disciplines in English, Spanish and Arabic* (Epic 2012). Available at, <https://en.wikisource.org/wiki/Assessing_the_accuracy_and_quality_of_Wikipedia_entries_compared_to_popular_online_encyclopaedias> accessed 5 May 2022.

25 *Slant* (a product recommendation community) ranks VLC 4th and Windows Media Player 26th in the 'Best audio player applications for Windows' category. *See* 'What are the best audio player applications for Windows?' Slant <https://www.slant.co/versus/1430/1608/~windows-media-player_vs_vlc > accessed 5 May 2022.

26 'Commons' refers to an institutional form of structuring the rights to access, use, and control resources that is not based on asymmetric exclusion typical of property but where the inputs and outputs of the process are shared, freely or conditionally, in an institutional form that leaves them equally available for all to use as they choose at their individual discretion. Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006) 61-62.

27 The term 'sequential creation' is used here in the place of the better-known term 'sequential innovation' to denote that the POCC model is defined (for the purposes of this study) in relation to the production of intellectual expression that qualify for copyright protection as opposed to scientific inventions. However, this is not to discount the potential held by the POCC model for the production of a diverse array of intellectual goods including inventions that could potentially qualify for patent protection.

a) Open creation process.

16 Firstly, the POCC process is 'open' to any member of the public, subject to generally applicable terms and conditions of participation. These terms and conditions are twofold. The most important category are terms and conditions that regulate the way in which any member of the public can benefit from the utilities of the POCC work (or any portion thereof) by engaging in the sequential creation process. These terms and conditions are applicable without distinction to persons who seek to use the POCC work both within and (where such use is permitted by the terms and conditions) outside the dedicated platform. They are usually imposed through standard-form open-public licenses (e.g. CC and GPL) but can also take the form of specific terms and conditions that are formulated to fulfil requirements of a particular creation project. For example, *Wikipedia* articles are subject to a CC-BY-SA 3.0 license that determine the ways in which they can be reproduced, adapted or made available to the public. Any person who wishes to use a *Wikipedia* article (or any portion thereof) must agree to be bound by the terms of the CC-BY-SA 3.0 license, regardless as to whether the intended use is to be carried out within the *Wikipedia* platform or outside it.[28] Similarly, in the case of FOSS programs contributors agree to abide by the terms of the GPL license. The choice of applicable license or the formulation of the specific terms and conditions are typically determined by the project initiator[29] although members of the creator community can sometimes be invited to participate in modifying these to suit the changing needs of the project.[30] The second category of terms and conditions is community governance rules that are designed to regulate the behaviour of creators (contributors) who engage in the POCC process. These community governance rules reflect an institutionalized framework of shared norms, goals and standards of conduct.[31] For instance, they could prescribe standards of conduct to be observed by creators in interacting with each other and delineate the nature and scope of the powers and authority vested in individuals empowered to carry out editorial and administrative functions. Such community governance rules are typically associated with creator communities engaging in the POCC authorship process within a dedicated online platform.[32] However, it is possible that they may also apply to diffused creator communities that do not engage in creation within a specific dedicated space but are dispersed both temporally and spatially. By setting out a common framework and/or set of values and ideals, they bind creators together within a common governance framework (and often within a common value system) that serves to create a sense of community among contributors and enables them to develop a common identity (e.g. a common identity as *Wikipedians*).[33] While the POCC model is not reliant on the existence of a community governance framework or a common value system, these contribute in no small measure towards the sustenance of the POCC process and

28 For a contrary view see the opinion expressed by Emmanuel Pierrat, that the CC-BY-SA license would not impose any obligation on third parties who seek to use that content outside of the platform. *Cited in* Marie Kostrz, 'Houllebecq, gratuit sur le net: Flammarion va attaquer.' Rue89 (2010). <http://rue89.nouvelobs.com/rue89-culture/2010/11/25/houellebecq-gratuit-sur-le-net-flammarion-va-attaquer-177707> accessed 5 May 2022. It is argued that this view is untenable as it would mean that the CC-BY-SA license is limited to use within the borders of a specific digital space. This would seriously affect the utility of a CC-BY-SA license and also be contrary to accepted legal principles regarding the scope of application of a contractual agreement.

29 The project initiator is the person or entity who designs the project and/or is in charge of operating the online platform (digital space) on which the POCC process takes place. For instance, as regards *Wikipedia,* the project initiator Jimmy Wales determined that content contributed to a *Wikipedia* article would be subject to a GNU Free Documentation License (GFDL) 1.2 (this was later changed to a CC-BY-SA license). Similarly, the terms and conditions under which content contributed to the *Folding Story* platform and *This Exquisite Forest* project is made available to downstream contributors was determined by the initiators of those projects.

30 In 2009, when the *Wikimedia Foundation* which owns and manages the *Wikipedia* platform decided to migrate from the GFDL license to the CC-BY-SA license, the relicensing proposal was put to a vote by individuals who had a registered account on a *Wikimedia Foundation* project with at least 25 edits prior to March 15, 2009. *See* 'Licensing update/Result' <https://meta.wikimedia.org/wiki/Licensing_update/Result> accessed 5 May 2022.

31 For a detailed exposition of the importance of social norms in the *Wikipedia* creation process *see* Christian Pentzold, 'Imagining the Wikipedia community: What do Wikipedia authors mean when they write about their "community"?' 13 New Media & Society (2011) 704

32 For example, as per the community guidelines of the *Wikipedia* platform persons engaging in creation on that platform agree to submit to editorial interventions made by 'editors' appointed by the community. 'Wikipedia: Administration'< https://en.wikipedia.org/wiki/Wikipedia:Administration> accessed 5 May 2022.

33 According to Pentzold, *Wikipedia* can be perceived as *ethos-action community*. Membership and thus the boundaries are defined by adherence to a set of standards regarding the project's purpose, norms, values, and valid actions. Pentzold (n 31) at p 714.

could be a critical ingredient in ensuring the success of the creation endeavour. Both categories of terms and conditions are capable of enforcement: the first category through legal action (e.g. enforcement of CC licenses in a court of law); and the second through community action (e.g. by 'blocking' and thereby excluding any person from continuing to engage in the common creation endeavour). However, as long as an individual abides by the terms of the license and community governance rules, no person has the power or privilege to exclude them from participating in the common creation endeavour. Thus, the borders of the POCC creator community are porous and any individual is able to gain membership of the creator community by agreeing to abide by generally applicable terms and conditions.

b) Open resource

17 Secondly, openness refers to the fact that the work created within the POCC process constitutes an 'open-resource' that can be added to, modified and built upon by members of the public both within the POCC process and in some instances even outside it (e.g. in creating stand-alone derivative works that are based on the POCC work but do not become part of the common work). Members of the public who engage in the creation process by adding to, modifying the POCC work or re-using the POCC work or portions thereof in the creation of independent derivative works can be referred to as 'active users'. In addition, under the POCC model, the work is typically made available to 'passive' users who seek to use the content without making further additions or modifications to that work (e.g. a student who wishes to cite a portion of a Wikipedia page in a term paper). Of course, the degree of 'openness' of different POCC works can differ depending on the terms on which they are made available for use and re-use. For instance, the Folding Story project allows members of the public to develop and build upon content using the POCC model within the dedicated platform in accordance with specified terms and conditions of use. However, as regards use outside the online platform, the content is made available subject to the exclusive copyright of the respective authors. Therefore, while the POCC work created through the Folding Story project constitutes an 'open-resource' as regards the members of the creator community who engage in the POCC process within the dedicated online platform, it comprises a 'closed-resource' as regards third parties.

18 The POCC authorship process reflects a collective endeavour within which the contributions of a multitude of otherwise unconnected persons[34] serve to create a single identifiable work that is available for the use and enjoyment of members of the public who agree to abide by generally applicable terms of use. In this sense, it corresponds closely to von Hippel's model of 'open collaborative innovation' (OCI) that has been defined as development projects in which multiple users collaborate and contribute for free and openly share what they develop.[35] However, the fact that this concept has been formulated with reference to innovation economics and the vague terms in which it has been defined makes it unsuitable for founding a legal analysis of POCC authorship.

19 Figure I illustrates the POCC creation process; a, b, c and d being contributors to the creation process (i.e. members of the creator community) and g, f and h being members of the public who are hoping to contribute to the creation process at a future date (i.e. intending to obtain membership of the creator community).

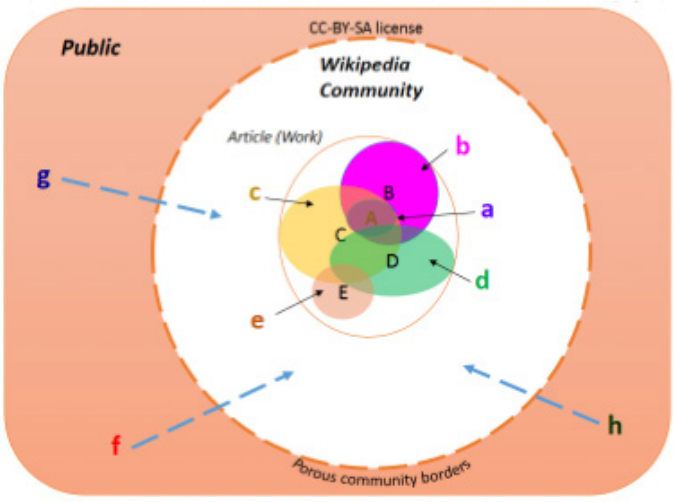

Fig. I: Illustration of POCC process

34 The term 'unconnected' denotes that interactions between contributors are usually limited to the creation process itself although they may sometimes develop through interactions taking place on community forums (e.g. the 'village pump' forum of *Wikipedia*). But the contributors are typically strangers who come together *via* the creation process and have no personal relationships outside it.

35 Eric von Hippel, 'Definition of open collaborative innovation' *(Financial Times)* <http://lexicon.ft.com/Term?term=open-collaborative-innovation> accessed 5 May 2022; *See also* Carliss Y Baldwin and Eric A von Hippel, 'Modeling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation'. Available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1502864> accessed 5 May 2022.

2. Chain of sequential creation

20 The POCC process involves a multiplicity of persons building upon and adding to content contributed by each other within a chain of sequential creation. Each contributor dedicates their contribution to the common creation effort to be added to, modified and built upon by downstream contributors. As a result, the contributions made by individual contributors become inseparably linked and intertwined with each other contextually and/or physically. Each contribution depends on preceding contributions for their context and meaning and this results in each contribution (no matter how small) being imbibed with an inherent dynamism, in that, it has the potential to inspire and direct the nature and substance of future contributions along the chain of sequential innovation. The open time-frame that enables the creation process to continue for an indefinite period of time enhances this dynamism by enabling the work to constantly adapt and update itself as an evolving 'living' work that can cater to contemporary requirements. Therefore, the POCC model is particularly suited for the creation of content that is in constant need of revision and updating such as FOSS and encyclopedia articles such as *Wikipedia.*

3. Creative autonomy

21 The POCC process proceeds in a random and sporadic manner, without a pre-determined creation design (agenda) or consensus among the authors as to the exact nature of the ultimate work. In addition, the POCC model is heterarchical[36] meaning that each contributor enjoys an equal degree of power and authority in determining the direction and outcome of the creation endeavour. Therefore, no person has the power to exercise control over the creative decision-making process or to set a creative agenda for another person. Thus, contributors are able to self-select the nature and scope of their individual contributions by exercising their personal creative judgment. In rare instances, contributions made to the common work may be subject to a process of curation such as in the case of *This Exquisite Forest.*[37] However, this curation is limited to the purpose of ensuring that only contributions that meet a certain level of quality are absorbed into the common work and do not set a creative agenda or dictate the actual nature and scope of individual contributions. Thus, each contributor exercises a substantial degree of creative freedom and autonomy in determining the nature and scope of the contribution they make. This also means that each contributor has the ability to modify and develop the POCC work in a way that could not have been intended or foreseen by preceding authors. For instance, in the creation of short fiction under a POCC creation model, a character created by an upstream contributor can be developed and modified by a downstream contributor in a way that was neither intended nor foreseen by its initial creator. This absence of a common creative agenda invests the creation process with considerable dynamism as the work is constantly developing in a manner that is serendipitous and unpredictable.

4. Ideology

22 The POCC model is founded upon an ideology of equality, collectiveness and sharing that is shared and accepted by contributors to the POCC process. This shared ideology and communitarian norms form a powerful incentive for individuals to contribute to the POCC process.[38] Therefore, the preservation and perpetuation of these norms along the chain of sequential creation is a key consideration in ensuring the sustainability of the POCC process.

23 The ideology of equality places each contributor on an equal footing with others and grants equal value to each contribution. Therefore, each contributor obtains an equal claim to the authorship of the work regardless of the value of their individual contribution to the overall work, either in quantitative or qualitative terms. The ideology of collectiveness is reflected through each individual contributor dedicating their expression to the common work that results in that expression becoming intertwined with the expression contributed by others to form a single cohesive work. Thus, the resulting POCC work is the result of a collective creative effort on the part of all contributors. Furthermore, the sequential innovation process proceeds upon a

36 Axel Bruns, 'Towards Produsage' in Fay Sudweeks, Herbert Hrachovec and Charles Ess (eds) *Cultural Attitudes towards Communication and Technology* (Murdoch University, 2006) 275, at p 279. A 'heterarchy' has been defined as "(...) the relation of elements to one another when they are unranked or when they possess the potential for being ranked in a number of ways." Carole L Crumley, 'Heterarchy and the Analysis of Complex Societies' (1995) Archeological Papers of the American Anthropological Association 1, p 3.

37 While contributors to *This Exquisite Forest* project enjoyed a high degree of creative autonomy and freedom in determining the way in which they developed upon the existing content, their contributions were curated by the producers of the project for appropriateness and quality. The producers reserved the right to not include certain submissions in the common work or to remove certain submissions from the platform.

38 Hars and Ou (n 22).

presumption held by each contributor that the value of their individual contribution would be augmented through its combination with other contributions and through modifications and additions effected by downstream contributors in the future. This further enhances the collective nature of the POCC process and gives expression to the ideology of sharing whereby each contributor entertains the expectation of sharing in the benefits of the value created through the contributions made to the work by others. Accordingly, the POCC process not only represents a collaborative endeavour that is designed for the *creation* of value but also for the collective *sharing of that value* with other contributors and (usually) with the public at large.[39]

C. Why is exclusive copyright inadequate?

24 Copyright is granted to the author(s) of a work.[40] Thus, the establishment of authorship is the central criterion for the enjoyment of the ownership of copyright over a work.

25 Copyright law conceptualizes authorship as an individual relationship that exists between a person (i.e. an author) and the expression (i.e. work) that is created by that person (or 'originates'[41] from them). The work thus created, is deemed to remain static and unchanging with the result that the individual relationship between the author and the expression remains similarly fixed and unchanged. Therefore, the current individualistic notion of authorship in copyright is constructed in relation to a product (i.e. the 'work') rather than in relation to the process of creation.

26 This individualistic conception of authorship is underpinned by two dominant theories of copyright law. The labour theory of copyright law (based on the writings of Locke[42]) that justifies copyright protection on the basis of an author's entitlement to enjoy the fruits of their labour. This is founded on "...the concept of a unique individual who creates something original and is entitled to reap a profit from those labours".[43] Similarly, the personhood theory of copyright law (derived from the writings of Kant[44] and Hegel[45]) is based on the premise that a work constitutes an artefactual embodiment of the author's individual personality[46] and that, therefore, its protection under copyright law can be justified as a means of protecting the author's personality.[47]

27 By attributing the work to the personal intellect of an identifiable author, copyright's individualistic conception of authorship reinforces the exclusive nature of the right held by that author over the work. As the work is the product of the author's own individual intellect it is both just and ethical that the author be allowed to reserve the benefits of the utilities of that work (e.g. reproduction, distribution,

39 As noted above, typically, content created under a POCC model is made available for use and re-use by members of the public subject to terms and conditions (usually imposed by open-licenses such as CC and GPL).

40 Exceptions do apply to this rule, for example, the 'work-made-for-hire' doctrine in US copyright law that grants ownership of copyright in a work created by an author within the course of employment to the employer, rather than to the author. *See* 17 U.S. Code [US Copyright Act of 1976] s. 201(b) read with s. 101.

41 The notion of 'origination' from the author is interpreted in two different ways as per the objective and subjective notions of 'originality'. As per the objective notion of originality a work originates from its author if it is the independent creation of its author in the sense that it is not copied (this notion of originality is typically associated with the English common law tradition of copyright, *see* for example, *University of London Press v University Tutorial Press* [1916] 2 Ch 601). As per the subjective notion of originality a work is considered to originate from its author in the sense that it reflects its author's personality (this notion of originality is prevalent in the civil law tradition of author's rights). For a discussion on these two viewpoints of the notion of originality *see* Estelle Derclaye, 'Wonderful or Worrisome? The Impact of the ECJ Ruling in Infopaq on UK Copyright Law' EIPR (2010) 247 and Benoît Michaux, 'L'originalité en droit d'auteur, une notion davantage communautaire après l'arrêt Infopaq' 5 Auteurs & Media (2009) 473.

42 *See* John Locke, 'Second Treatise of Government', The Works of John Locke (Rev ed, Thomas Tegg 1823) <http://socserv2.socsci.mcmaster.ca/econ/ugcm/3ll3/locke/government.pdf> accessed 5 May 2022. For an explanation as to how Locke's theory of property applies to intellectual property in general *see* Lawrence C Becker, 'Deserving to Own Intellectual Property' 68 Chicago-Kent Law Review (1993) 609.

43 Mark Rose, *Authors and Owners: The Invention of Copyright* (Harvard University Press 1993) p 2.

44 Immanuel Kant, *The Philosophy of Law* (W Hastie tr, Clarke 1887).

45 GWF Hegel, *The Philosophy of Right* (SW Dyde tr, G Bell 1896).

46 C.S. Yoo, 'Copyright and Personhood Revisited', 3 University of Illinois Law Review (2012) 1039, at p 1055.

47 William Fisher, 'Theories of Intellectual Property', in Stephen R Munzer (ed), *New Essays in the Legal and Political Theory of Property,* (Cambridge, 2001) 168, at p 171 and Justin Hughes, 'The Philosophy of Intellectual Property' (1988) 77 The Georgetown Law Journal 287, at p 330.

adaptation) to their own individual enjoyment (i.e. 'mine *not* yours') and be granted an affirmative claim to prevent any other person from benefitting from those utilities without their authorization.

28 Copyright law's notion of authorship gives expression to this individualistic bias through three main elements which I refer to as the 'tripod' of copyright's notion of authorship. These are originality, creative control and the existence of a static work. Originality is the primary element that establishes the individual relationship between the author and the work. It pre-supposes the existence of "...a relation of creation between the work and the author."[48] The second element of creative control refers to the 'agenda-setting' ability of the author in determining the final nature and form of the work by exercising control over the creative decision-making process. It thereby foresees the establishment of a direct link between the original expression incorporated in the work and the author's own intellect and personality. Woodmansee gives expression to this element by noting that copyright conceptualizes an author as "an individual who is solely responsible — and therefore exclusively deserving of credit for the production of a unique work."[49] The final element of a static work links authorship to a closed, static product which ensures that the individual relationship between the author and their original expression (incorporated in the work) remains unchanged once it has been established. Any further changes or modifications made to that original expression, either by the author themselves or by a third person, will give rise to a new static (derivative) work as opposed to being recognized as a step in the work's evolution (*see* Figure II).

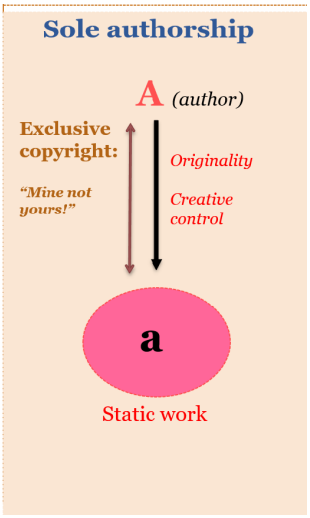

Fig. II: Illustration of individual relationship between author and work of sole authorship

29 As will be discussed in section C.II. this individualistic notion of authorship also permeates copyright's conception of collaborative authorship that is conceptualized as an individual or distinct relationship that exists between an identifiable group of persons (authors) and the original expression (work) originating from them (*see* Figure III).

I. Inability of a POCC work to fit within the existing categories of collaborative authorship

30 At present, copyright law recognizes three models of collaborative creation: joint, derivative and collective creation. This classification applies consistently across different copyright law systems, albeit with nuances in the ways in which they are defined and interpreted. Authorship and the distribution of exclusive rights over a work involving a plurality of authors is determined according to the model of collaborative creation under which that work has been produced. Therefore, identifying the applicable model of collaborative creation is an important step in determining the persons who obtain copyright over the work and how that copyright can be exercised and enforced. At the moment, copyright law does not offer a catch-all-category (or a category *de droit commun*) that is equipped to deal with a work that fails to fall within any one of these categories. It is noted that a POCC work would not fit comfortably within any of these existing categories of collaborative authorship as they are currently defined in the copyright law systems of France, the UK and the US.

31 The joint creation model envisions a group of persons collaborating together in the creation of a specific

48 A. Dietz, The Artist's Right of Integrity Under Copyright Law – A Comparative Approach" IIC (1994) 177, at p 182

49 Martha Woodmansee, 'The Genius and the Copyright: Economic and Legal Conditions of the Emergence of the 'Author" 17 Eighteenth-Century Studies (1984) 425, at p 426.

and as yet unfinished work[50] with the creation process automatically coming to an end once the joint work has been realized. Thus, the joint creation model fails to capture the open-ended nature of the POCC process that is not directed towards the production of a static work but rather a dynamic work that can evolve over an indefinite period of time.

32 Similarly, a POCC work cannot be categorized as a derivative work. The derivative creation model envisions the creation of a new work through the modification, alteration or adaptation of a pre-existing work. Thus, the new work 'derives from' an existing work and constitutes a work of multiple authorship in the sense that it represents a fusion of expression belonging to the author of the pre-existing work and the author of the derivative work. However, the derivative work constitutes an independent work that exists separately from the pre-existing work and *vice versa*. Accordingly, the derivative creation model fails to capture the dynamism that is inherent in the POCC model whereby, any contribution that modifies, adapts or builds upon an existing contribution is absorbed into the common work without enjoying a separate existence from it.

33 The collective creation model envisages the creation of a collective work through the compilation or arrangement of the creative contributions made by a multiplicity of authors, within a logical sequence. The characteristic feature of the collective creation model is that the different authors do not collaborate with each other within a common creative endeavor but instead work independently on their individual contributions. These contributions are later collated together to form a single collective work by a specific person who is usually attributed the authorship of the collective work (provided that the compilation and/or arrangement of the different contributions display sufficient originality in order to qualify them as an author). As such, the absence of collaboration among the different authors within the creation process and the fact that these different contributions usually remain separate and distinct from each other, clearly prevents the POCC process from being located within the collective creation model.

50 The decision delivered by the United States Court of Appeals (9th Circuit), in the case of *Ashton-Tate Corp. v. Ross* [1990] 916. F. 2d. 516, affirmed that, where a contribution is made to a pre-existing work it would not result in a joint work but in a derivative work (at p 522). Similarly, Bently and Sherman observe that a poem written by one person and translated by another will not constitute a joint work but a derivative work. Lionel Bently and Brad Sherman Intellectual Property Law (5th edn OUP, Oxford 2018) at p 132.

II. Notion of collaborative authorship in copyright law

34 Of the three models of collaborative creation currently recognized under copyright law, the joint and derivative models of creation give rise to works of plural authorship whereby the authorship over the work is attributed to more than one person. The collective creation model on the other hand, results in the creation of a work of single authorship as the authorship of the work is attributed to the person or entity who is deemed responsible[51] for compiling the individual contributions made by a multitude of authors in order to create the collective work. Thus, at the outset, it is possible to exclude the collective creation model from our analysis of the notion of collaborative authorship in copyright law. I will proceed to analyse the joint and derivative creation models as they are defined and interpreted in the copyright law frameworks of France, the UK and the US to demonstrate how the tripod of copyright's individualistic notion of authorship permeates the concept of plural authorship in works created under these models of collaborative creation.

1. The joint creation model

a) Originality

35 The joint creation model refers to the creation of a single static work by merging together the creative efforts of a multiplicity of persons. The copyright over the ensuing work is collectively owned[52] by all persons (co-authors) who have contributed original expression to the work. The attribution of authorship over a work created under a joint model

51 In French copyright law this is the 'maître d'oeuvre' who takes the initiative for creation, gives directions as to how the work should be created and takes the initiative to exploit the work. Michel Vivant and Jean-Michel Bruguière, *Droit d'Auteur* (Dalloz, Paris 2009) at pp 245-247. In the UK and the US the copyright in the compilation is granted to the 'editor' or 'compiler' who arranges or compiles the separate works to form a single collective work. Paul Goldstein and P. Bernt Hugenholtz, *International Copyright: Principles, Law, and Practice* (3rd edn, Oxford University Press 2013) at pp 253-254.

52 In France, the joint (collaborative) work forms a whole over which each co-author has an indivisible right. Frédéric Pollaud-Dulian, *Le Droit d'Auteur* (2nd edn Economica, Paris 2014) at p 350 citing the case of "*Donizetti*" Cass. Civ. 7 April 1925, 1925 –I-268. As discussed further in section C.V., under the law of the UK and the US, the co-authors own copyright over the work as 'tenants in common'.

of creation is reliant on a contributor's ability to establish a direct and individual link to the whole or part of the original expression incorporated in that work. In France, this is expressed through the requirement that each author must make an original creative contribution in the sense that it contains the manifestation of the stamp of the author's personality.[53] In the UK it is reflected in the condition that each co-author must make an original and significant contribution to the authorship of the work[54] and in the US by the requisite that each co-author must make a contribution that is copyrightable.[55] Thus, in all three systems of copyright law any person who is not able to establish a direct individual link to the original expression incorporated in the work would be denied a claim of co-authorship and consequently precluded from claiming ownership (or co-ownership) of copyright in the work.

b) Creative Control

36 In France, co-authors of a joint work are deemed to engage in creation under a 'common inspiration' or 'spiritual intimacy' that enables them to work towards a common goal by means of a creative concerted effort.[56] Similarly in the UK, co-authors are deemed to jointly labour together in pursuance of a common goal or in prosecution of a common design.[57] I argue that, as the common inspiration' or 'common design' under which the co-authors labour dictates and directs the original expression that is contributed by each of them to the joint work, this gives rise to a fiction that the group of authors act together as *one single entity* in pursuance of a common creative agenda in the creation of the joint work. Thus, creative control over the work is deemed to be shared by all co-authors acting as a single organic creative entity that enables the establishment of an individual (in the sense of a 'distinct') link between the original expression incorporated in the joint work and the plurality of authors. This fiction therefore allows the creation of a joint work to be subsumed within copyright's individualistic conception of authorship.

37 Arguably, this element of a common creative agenda is also reflected in US copyright law's notion of joint authorship in the criterion of 'mutual intent', which requires that, at the time of making their individual contributions, each co-author intends that their contribution be merged into inseparable or interdependent parts of a unitary whole.[58] Goldstein opines that this requirement of 'mutual intent' essentially mirrors the UK law requirement of the existence of a common design among the authors of a work of joint authorship. Indeed, in the case of *Childress v Taylor*[59], the Second Circuit regarded the sharing of creative decision-making authority among authors as a core element in establishing the 'mutual intent' criterion. It is logical that the existence of an intention on the part of each co-author that their contribution be absorbed into a single unitary work, compels each contributor to create their own contribution in anticipation of those made by others to ensure that the contributions complement each other. This pre-supposes the existence of some form of pre-agreed common scheme of creation or creative agenda that is shared by the co-authors of the work of joint authorship and therefore unifies them in its prosecution. Accordingly, the criterion of 'mutual intent' can also be interpreted as giving rise to a fiction that the co-authors of a joint work act together as a one single entity in the prosecution of a common creative agenda; this yet again locates the authorship of a joint work within copyright law's individualistic conception of authorship.

38 Independently of the 'mutual intent' criterion, the US Court of Appeals for the Ninth Circuit has developed a 'control-based' test pursuant to which the creative and financial control exercised over a joint work is considered a deciding factor in the establishment of co-authorship. Thus, in the case of *Aalmuhammed v Lee*[60], the Ninth Circuit held that, the

53 Ibid, Pollaud-Dulian at p 351 citing Cass. civ.1er, 30 janvier 1974, « *Wogenscky c. Polieri* », Bull. civ. I, n°34, p 30. *See also* André Lucas, Henri-Jacques Lucas and Agnès Lucas-Schloetter *Traité de la propriété littéraire et artistique* (4th edn Lexis Nexis, Paris 2012) p 119.

54 The requirement of 'significance' has been interpreted to mean 'substantial', 'considerable' or 'non-trivial' as opposed to being 'aesthetically important'. Bently and Sherman (n 50) at pp 130-131.

55 *Childress v. Taylor* [1991] 945 F. 2d. 500. In Goldstein's opinion this requirement should be interpreted to mean that the contribution made by each contributor is independently copyrightable. *See* Paul Goldstein, Copyright Vol. I 2005 Supplement (3rd Ed. Aspen Publishers, New York 2005) s.4.2.1. p 4:13.

56 Lucas (n 53) 189 at p 195. *See also* CA Paris, 1er ch., 11 mai 1965 D 1967, p 555 note Françon.

57 This criterion was established in the case of *Levy v. Rutley* (1871) LR 6 CP 523. *See also* Bently and Sherman (n 50) p 126 and W R Cornish, *Intellectual Property* (4th edn Sweet and Maxwell, London 1999) p 386.

58 Goldstein (n 55) s. 4.2.1., at p 4:7.

59 *Childress v. Taylor* [1991] 945 F. 2d. 500. *See also, Thomson v Larson* 47 F.3d 195 (2d Cir. 1998).

60 *Almuhammed v. Lee*, *202 F.3d 1227 (9th Cir. 2000).* See also *Richlin*

absence of control over creative decision-making is "(...) strong evidence of absence of co-authorship". On the other hand, in the case of *Lindsay v Titanic*[61] a high degree of actual control was held to give rise to a presumption of authorship.

c) Static work

39 Once created, the joint work remains closed to further changes and each new addition or modification will result in a separate and independent derivative work as opposed to being absorbed within the joint work. Thus, changes effected to the joint work by subsequent contributors will not affect the legal relationships that exist between the co-authors and the original expression of the work.

2. The derivative creation model

a) Originality

40 The derivative creation model refers to the creation of a new work by modifying, building upon or adding to the original expression of an existing work and by combining it with 'new' original expression. This 'new' original expression enables the author of the derivative work to establish an individual link with the work. Accordingly, in French copyright law, the author of the derivative work is required to imbue it with a sufficient degree of independent originality in order to enable it to be protected as a new work of authorship.[62] In UK copyright law, this is framed in terms of the derivative work incorporating a material alteration or embellishment that is original and suffices to make the totality of the work an original work.[63] In US copyright law, the derivative work must demonstrate a sufficient level of originality in the sense that it incorporates a distinguishable and non-trivial variation from the pre-existing work. On the other hand, an individual link is also established between the derivative work and the author of the pre-existing work by reason of the original expression belonging to that pre-existing work which is incorporated in the new derivative work.[64] The copyright over the new derivative work will therefore belong to the author who produces it, subject to the reservation of the rights of the author of the pre-existing work over their own original expression that is incorporated in the derivative work.[65]

b) Creative control

41 In terms of creative control, the author of the pre-existing work is able to exercise negative control over the creation of the derivative work by imposing restrictions and limitations on the nature and extent to which the original expression belonging to the pre-existing work can be added to, modified, built upon and combined with the new original expression contributed by the author of the derivative work. This ability to exercise negative control, enables the author of the pre-existing work to ensure the preservation of their own individual link with the original expression incorporated in the derivative work (for instance by invoking the moral right to integrity to prevent the modification of their original expression in a way that results in an obliteration of their 'personal stamp' from that expression). Within

v. Metro-Goldwyn-Mayer Pictures, Inc., 531 F.3d 962 (9th Cir. 2008).

61 *Lindsay v Titanic* [1999] 52 U.S.P.Q.2d 1609 (S.D.N.Y. 1999).

62 Once again, originality would be judged under the general standard of originality in French copyright (author's rights) law which requires that the work contains an imprint of the author's personality. Lucas (n 53) p 119.

63 *McMillan and Company Ltd. v. K and J Cooper* (1924) 40 TLR 186.

64 In French copyright law, the derivative work is required to incorporate original elements of the pre-existing work which express the personality of that preceding author. *See* Pollaud-Dulian (n 45) at p 403. Under UK law, in order to qualify as a derivative work, a work must appropriate a substantial part of the content belonging to a pre-existing work. That content must constitute original expressive content which made the pre-existing work an original work. *See* Kevin Garnett, Gillian Davies, Gwilym Harbottle (eds), *Copinger and Skone James on Copyright* Volume I (16th edn Sweet and Maxwell, London 2011) p 232. In the US, a derivative work is required to change i.e. recast, transform or adapt original and expressive content belonging to the pre-existing work. *See* William F. Patry, Patry on Copyright (Thomson/West, USA 2006) 3:47.

65 In France this was emphasised in the decision delivered in « *L'Affaire Tosca* » Cass 1er Civ. 22 juin 1959.

In the UK, if the derivative work reproduces a substantial part of the original expression of a pre-existing work then the authorization of the copyright owner of the pre-existing work is required for the exploitation of the derivative work, *see* Copinger and Skone James on Copyright (n 64) p 232. In the US, decisions delivered in the cases of *Stewart v. Abend* 495 U.S. 207 (1990) and *G. Ricordi & Co. v. Paramount Pictures Inc.* 189 F.2d 469 (2d Cir. 1951) emphasize that, so long as the pre-existing work is under copyright protection, the author of a derivative work is prevented from making use of any part of the pre-existing work that may be contained in the derivative work, without first obtaining the authorization of the copyright owner of that pre-existing work.

the framework of the authorization granted by the author of the pre-existing work, the author of the derivative work is able to exercise positive creative control in terms of determining the way in which the original expression contained in the pre-existing work should be modified, altered and combined with their own original expression to create the new derivative work. Thus, both the author of the pre-existing work and the author of the derivative work can claim an individual relationship to the original expression that is incorporated in that work, thereby rendering the new derivative work a work of plural authorship.

c) Static work

42 Although derivative creation is necessarily an incremental process, existing copyright law artificially compartmentalizes each point in this creation process into a series of separate and static derivative works. Thus, any modification to an existing derivative work will result in the creation of a new derivative work as opposed to being recognized as a point in an evolutionary and incremental process of creation.

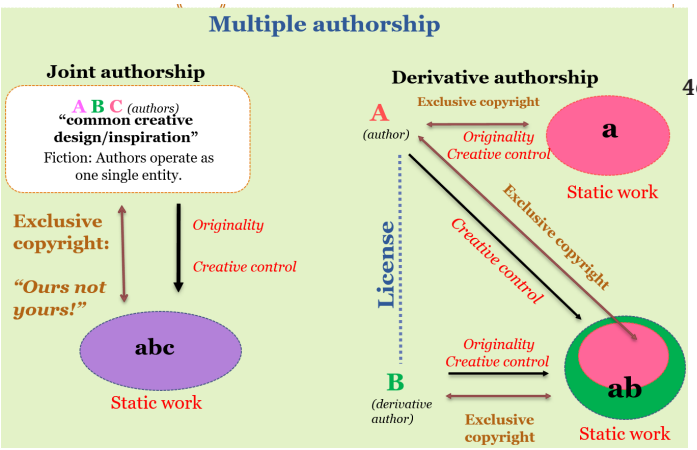

Fig. III: Illustration of individual relationship between authors and works of plural authorship

III. Why does the POCC authorship model not fit within copyright's notion of plural authorship?

43 The architecture of the POCC model precludes any single contributor to a POCC work from establishing an individual relationship between themself and the original expression of the work as envisioned by copyright's conception of individualistic authorship and the tripod of originality, creative control and the existence of a static work.

1. Originality

44 Not all contributions that build upon existing content would be able to demonstrate sufficient originality as required for establishing authorship under copyright law. For example, within the process of 'tweaking' that is commonly used in the creation of POCC works contributions that on their own would fail to satisfy the standard of originality would, through their combination with each other along the process of sequential innovation, give rise to an original copyrightable contribution. In such an instance, it would be difficult to correctly determine the source of that original expression.

45 On the other hand, as upstream contributors are not able to exercise any degree of negative control to limit the ways in which downstream contributors may modify their contributions, it is quite possible that the original expression contributed by an author becomes obliterated[66] from the POCC work in the course of the sequential creation process. Such obliteration would effectively extinguish the individual relationship that author could claim to the POCC work.

2. Creative control

46 The absence of a pre-determined scheme of creation, the high degree of creative autonomy exercised by each contributor and the random and sporadic nature of the contributions precludes the possibility for any person or group of persons to claim creative control over the creation of the POCC work. The open-ended creation process allows any downstream contributor to change the POCC work in a way that could not have been envisioned or anticipated by an upstream author without those authors being able to control or prevent such changes from being effected. Thus, it is not possible to establish the existence of a common creative agenda that enables contributors to act as a single entity in the prosecution of the common work. In contrast, the POCC model relies on and celebrates the existence of different creative visions that enable the work to constantly evolve in new directions.

47 Furthermore, the format of the POCC model does not allow for the existence of such a common creative agenda by reason of the minimal scope that is available for interaction and discussion among

66 This could take-place unintentionally as a consequence of the incremental modifications made to the content of the POCC work within the sequential creation process or as a result of intentional overwriting where this is allowed under the terms and conditions applicable to the creation process.

contributors to a POCC work.[67] Contributors may share a consensus as to the general goal of the creation endeavour (e.g. to create an encyclopaedia entry on a particular topic that can serve as an authoritative source of reference on that topic or the creation of a work of fiction or a work of graphic art). They would (and in most instances do) also share a common goal or objective as regards certain technical aspects of the creation process (e.g. writing style, standard of language to be used etc.). However, this cannot be considered as the sharing of a 'common creation design' or a 'spiritual intimacy'. Those terms refer to a consensus and a shared creative vision on the part of joint authors that relate to the *nature and form of the original expression* that is to be incorporated in the work and thus imply the exercise of shared control over the creative decision-making process. Thus, the existence of a common creation design or spiritual intimacy cannot be reconciled with the POCC process where each contributor makes independent decisions relating to the original expression that is contributed by them and consequently the direction in which the POCC work evolves.

48 As demonstrated by the foregoing discussion, incorporating the POCC work within the existing categories of joint and derivative works would require a radical transformation of the core premise of individuality-based authorship on which they are founded. Furthermore, attempting to fit the POCC model within any of these conventional categories of collaborative authorship recognized under copyright law would lead to different stages of its evolution being artificially compartmentalized, either as successive 'versions' of a joint work or as a series of derivative works, or an mixture of both (as a result of different portions of the work being categorized as different works). This would distort the true nature of a POCC work as a dynamic and evolving work that nevertheless forms a cohesive whole.[68]

IV. Constructing a notion of POCC authorship

49 As Lavik notes, authorship does not possess a timeless quintessence that is independent of human perspectives and purpose.[69] On the contrary, it is a by-product of social, historical and cultural context[70] and as such, is subject to transformation and evolution in accordance with changes in the ways in which creation is carried out and experienced. The following section constructs a new notion of POCC authorship that is founded on the core elements of inclusivity and dynamism.

1. Inclusivity

50 As envisaged by Dusollier, the term 'inclusivity' denotes the quality of a legal right to benefit from all or some utilities of a tangible or intangible good that is held by a plurality of legal subjects in a collective way without any person having the power to exclude the rightholder from such benefit.[71] Thus, it presents a counterpoint to the exclusivity-based notion of individualistic authorship in copyright law. How is this quality of inclusivity reflected in the POCC authorship process?

51 Firstly, the sequential innovation process that is integral to the POCC authorship model relies on the ability of contributors to add to, modify and build upon contributions made by others and sometimes (as in the case of *Wikipedia*) to even overwrite or delete content contributed by others. As noted in section B.I.2. above, this cumulative creation process forms the core of the POCC authorship process and reflects an intention on the part of each contributor to dedicate their own individual contribution to a common creation endeavour in the course of which

67 Although some online platforms such as *Wikipedia* provide spaces (or forums) where contributors can interact and engage with one another, discussions taking place on these forums usually relate to technical aspects of the creation process (e.g. accuracy of factual information, relevance of certain information) or issues relating to the administration and governance of the platform (e.g. decisions taken by editors, complaints relating to the behaviour of certain contributors within the platform). They typically do not relate to creative aspects of the authorship process or to the nature of the original expression incorporated in the work.

68 Interestingly, in a determination delivered by the Court of Appeal of Versailles in France, it was pointed out that the technical and functional developments effected in the successive versions of a software program did not result in the creation of a new software program, but merely a represented stage in the technical and functional evolution of that software program at a given time. The Court of Appeal acknowledged that software programs, such as the one under review, would necessarily constitute an evolutionary product by reason of the practical need to adapt to rapid technological developments, and that this evolutionary process would continue so long as the software program was in the process of commercialization. CA Versailles 4 octobre 2001, *Thomas et SARL Ready Soft c. SARL Codat Informatique et Mattern*, 327 RJDA 3/2002, 276.

69 Erlend Lavik, 'Romantic authorship in copyright law and the uses of aesthetics', in Mireille van Eechoud (ed), *The Work of Authorship* (Amsterdam University Press, 2014) 57.

70 Jessica Reyman, *The Rhetoric of Intellectual Property* (Routledge 2010) 11.

71 *See* section A.

it is absorbed into a common good (i.e. the POCC work) to be used, re-used and enjoyed by all other contributors. Within this collective creation process, individual contributions become contextually inseparable and entwined with each other in terms of relying on preceding and/or succeeding contributions for their context and meaning. This means that, as a matter of practical necessity, contributors are compelled to enjoy the benefits of the utilities of the content contributed by them to the POCC work in a shared and collective manner.

52 Secondly, as noted in section B.I.4. above, the ideology of POCC authorship is built upon the notions of collectiveness, sharing and equality. This ideology reflects the nature of the POCC process as a collaborative value creation and value sharing endeavour. Pursuant to the concept of equality that underscores the authorship process, each contributor has an equal entitlement to engage in the creation process by using and re-using content contributed to the POCC work by upstream contributors, subject to generally applicable terms and conditions (e.g. CC license) and platform governance rules, without any other person (including the contributors of specific content) having any power or privilege to exclude them from such use or re-use. In turn, upstream contributors expect to share in the benefits of the value created through new expression contributed to the work by downstream contributors, without any downstream contributor having the power or privilege to exclude them from sharing in that value.

53 Thus, the relationship between contributors to the POCC work mirrors the quality of inclusivity in terms of each of them having an equal claim to benefit from the utilities of the POCC work in terms of adding to, modifying, building upon the POCC work and reproducing, distributing communicating and making it available to the public either in whole or in part, subject to generally applicable terms and conditions (e.g. CC license in the case of a *Wikipedia* article).

54 Accordingly, authorship under the POCC model represents a collaborative value creation and value sharing endeavour wherein authors are compelled to enjoy the utilities of the POCC work in a shared and collective manner, without any single author having a discretionary power to exclude another from benefitting from those utilities.

2. Dynamism

55 Dynamism relates to two aspects of POCC authorship. First, the POCC process is dynamic in terms of the potential held by each contribution to inspire and direct succeeding contributions and to determine the trajectory of the creation process. Secondly, the output of the POCC process is a dynamic and evolving work as opposed to a static unchanging work. Within this sequential innovation process the expression contributed by a contributor could become obliterated at any point in time thereby disrupting the individual relationship that may be considered to exist between the contributor and the POCC work. The dynamic nature of the POCC work demands that any person who has contributed to the work at any point in its evolution is recognized as having an equal claim to the authorship of the work. This equal claim to authorship is not reliant on the quantitative or qualitative nature of the contribution since a relatively small contribution, which appears unimportant or commonplace at the time at which it is made, may have a significant influence on the work's evolution based on the way in which it is interpreted and built upon by downstream contributors.

56 Accordingly, the notion of POCC authorship presented here, diverges from copyright's concept of collaborative authorship by being based on a notion of collective as opposed to individual authorship (*see* Figure IV). Furthermore, it is not dependent on the establishment of an individual link between the original expression incorporated in the POCC work and the person claiming authorship. Thus, as opposed to the conventional notion of authorship in copyright law the notion of POCC authorship needs to be conceptualized as a relationship that exists between a person (i.e. an author) *and* an incremental process of creative exchange (i.e. the POCC process) that culminates in the production of a dynamic and evolving work (i.e. the POCC work).

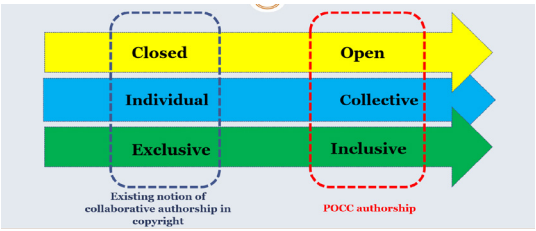

Fig IV: POCC as a new archetype of collaborative authorship

57 Therefore, the notion of POCC authorship presents a new archetype of collaborative authorship that is open, collective and inclusive. The existing exclusivity-based copyright law that is founded upon the conventional closed, individualistic notion of collaborative authorship does not have the capacity to give legal expression to the inclusivity that is inherent in the relationships among the authors of a POCC work. Nor can it adequately capture the dynamism of the POCC work and the temporal dimension of rights of authorship over the evolving POCC work.

V. Inadequacy of exclusive copyright in giving expression to inclusivity and dynamism in POCC authorship.

58 As noted in the foregoing discussion, within the POCC authorship process, the contributions of each author are dedicated to the common creation endeavour. In the course of the sequential innovation process, the original expression contributed by each individual author becomes inextricably linked in such a manner that prevents any author from benefitting from the utilities of the original expression created by them without also benefitting from the original expression created by another. The individual copyrights held by contributors over the original expression contributed by them become similarly intertwined in a manner that precludes any single contributing author from exercising or enforcing their copyright without encroaching upon the copyright belonging to another. Thus, the final POCC work is subject to a web of copyrights, the individual exercise and enforcement of which would give rise to a host of ideological and practical problems. This section will explore the impact of the application of exclusivity-based copyright law to a POCC work as regards the exercise and enforcement of copyright over a POCC work. It will focus on the implications for the copyright clearance procedure (i.e. the ability of an individual to obtain authorization to modify and build upon the POCC work) and the ability of an author(s) of the POCC work to bring a legal action against the infringement of their rights (both copyright and contractual rights) in the POCC work.

59 As noted above, the application of exclusive copyright would lead to different stages of evolution of a POCC work being artificially compartmentalized into a series of separate static works that may be categorized either as joint works or as derivative works or even as a mixture of both. This would result in the fragmentation of copyright over the POCC work among a multiplicity of authors. The nature and extent of the exclusive copyright granted to these individual authors over the work would differ according to whether their particular means of collaboration within the POCC creation process leads to their classification as a co-author of a joint work or as an author of a derivative work. As discussed below, the granting of an exclusive copyright to each author over their specific contribution to the work would go against the ideological framework of inclusivity on which the POCC authorship model is based and create inefficiencies relating to the exercise and enforcement of copyright over the POCC work. In the long-term it would also threaten the sustainability of the POCC process.

60 Under both joint and derivative authorship models, exclusive copyright grants to each individual author (i.e. co-author of a joint work or author of a derivative work) a copyright that can be exercised individually and according to personal discretion. For instance, under the copyright law of the UK the co-authors of a work of joint authorship are deemed to hold copyright over the joint work as 'tenants in common'.[72] This means that the exploitation of the work by a co-author or the licensing of such exploitation to a third party requires the authorization of *all* co-authors.[73] The same principle applies in French copyright law where the exploitation of the joint work is required to take place in accordance with the principle of unanimity *(accord commun).*[74] This would mean that in the UK and France (unless the POCC work has been made available to the public under an open public license such as CC or GPL) any downstream author who wishes to engage in the sequential creation process in relation to a particular portion of content belonging to the POCC work would need to identify all authors who have copyright over that portion of the content and to individually obtain their authorization to use such content for the purpose of participating in the POCC authorship process.[75] The same holds true as regards derivative works, as the copyright law systems in all three jurisdictions hold that any addition to or modification of a derivative work (i.e. the creation of a further derivative version) requires authorization of the author of the derivative work as well as the authors of all pre-existing works on which the derivative work is based.

72 *Powell v Head* (1879), 12 Ch. D., 686.

73 Ibid *see also Cescinsky v. George Routledge and Sons* [1916] 2 KB 325 and *Robin Ray v. Classic FM Plc.* [1988] F.S.R. 622.

74 Article L113-3 of the French Intellectual Property Code (1992).

75 In the case of *Morris c. Goscinny* the Cour de Cassation (Supreme Court) of France went onto hold that the exploitation of a collaborative work without obtaining the proper consent of one co-owner would amount to an infringement as per Article L 335-2 of the Intellectual Property Code, « Puisqu'il n'y avait pas de véritable accord, l'opération, non autorisée, était contrefaisante par application de l'article 335-2 du Code de la propriété intellectuelle » [As there has been no valid agreement, the unauthorized action amounts to an infringement as per Article 335-2 of the Intellectual Property Code: Translated by the author]. «*M. de Bévère dit Morris; société Lucky Productions et autres c. Mme Goscinny* » Cass. 1re civ., 27 nov. 2001. Similarly in the case of *Powell v Head* (1879), 12 Ch. D., 686, the Chancery division (UK) determined that in a situation of co-owned copyright, it is not possible for a single co-owner to license a third party to represent the work without the consent of the other co-owner.

61 The fragmentation of exclusive copyright over the POCC work among a multitude of authors and the need to obtain their individual authorization prior to adding to or modifying the POCC work within the sequential innovation process can result in several problems and inefficiencies.

1. Copyright clearance

62 Firstly, it would lead to an increase in the transaction costs relating to the license clearing process and thereby create inefficiencies regarding the exploitation of the POCC work. For instance, where the POCC work is made available under an open public license (e.g. CC or GPL) any user who wishes to exploit the POCC work or any portion thereof in a manner that is *not* covered under the terms of that license will need to identify and obtain the authorization of each contributing author who holds a copyright over the work or over that particular portion. Secondly, it would mean that the authorization granted to a downstream contributor to use the content belonging to the POCC work stems from a web of licenses granted by a plurality of copyright holders. This could give rise to serious inefficiencies (e.g. holes in the web of licenses, incompatibility among licenses) in the enforcement of the license terms in the event of a possible violation.[76] Thirdly, it would allow any author to block the sequential creation process either by preventing downstream contributors from modifying or building upon the specific expression over which they hold copyright or, by granting their authorization subject to conditions that restrict the creative freedom and autonomy of downstream contributors. The capacity of an individual author to disrupt the sequential innovation process by refusing to grant authorization to downstream contributors to modify the expression contributed by them to the POCC work poses a serious risk to the sustainability of POCC process. Furthermore, it would create an asymmetry in the entitlements held by different authors over the POCC work that negates the inclusivity inherent in the POCC process. For instance, an author who has contributed a larger or qualitatively more important portion of the work would be able to exercise greater control over the work's future development process in comparison with other authors. Similarly, upstream authors would exercise greater control over the work's development in comparison with downstream authors.

63 On the other hand, while US copyright law also deems that owners of a joint work enjoy copyright as 'tenants in common', in contrast to the UK and France, each co-author is entitled to independently exploit the joint work without the need to obtain the authorization of the other co-authors. Thus, a co-author may also unilaterally grant a non-exclusive license to a third party to exploit the work without the authorization of the other co-authors, and if necessary, even overriding their objections.[77] In doing so, the co-author is not bound by any fiduciary duties to exercise their copyright in a way that is not detrimental to the ability of other co-authors to benefit from the utilities of the work.[78] While the US approach dispenses with the difficulties of license clearance and prevents the exercise of exclusive copyright by individual contributing authors to a POCC work to block the sequential creation process, it also means that any single contributing author would be able to exercise exclusive copyright over the work in a manner that impedes the others from fully enjoying the benefits of the utilities of the POCC work. It would further enable a contributing author to exploit the POCC work in a manner that is contrary to the fundamental values of sharing and openness on which the POCC authorship process is founded.[79]

2. Action for copyright infringement

64 The individualistic approach to authorship under exclusive copyright also means that any contributing author of the POCC work who wishes to bring an action for infringement of copyright over that work would be required to establish their status as an author (i.e. co-authorship of joint work or authorship of derivative work) in order to establish legal standing *(locus standi)* to bring the action. This would give rise to difficulties relating to the determination of legal standing when the copyright infringement claim is brought in relation to a specific portion of the POCC work. In such a case the question arises whether any co-author of the work would have legal standing to bring the action for infringement or if only those

76 *See* Maxime Lambrecht 'Copyleft Licensing' ERC Inclusive Report 1 (Sciences Po 2011) [Unpublished].

77 Avner D. Sofer, 'Joint Authorship: An Uncomfortable Fit with Tenancy in Common', (1988) 19 Loyola L.A. Ent. L. Rev. 18.

78 William F. Patry, *Patry on Copyright* (Thomson/West, USA 2006) 5:13;5-46.

79 For example, pursuant to a *Wikipedia* article being judged a joint work under US copyright law, a contributing author of a *Wikipedia* article who is determined to have the status of a co-author of the article would be able to exercise their own individual discretion to grant a non-exclusive license to an online for-profit encyclopedia to reproduce the *Wikipedia* article and to exploit it for commercial purposes. This would be contrary to the shared ideology of openness and sharing based on which the other authors contributed to the article.

persons who are able to establish co-authorship or derivative authorship over that specific portion would be able to establish legal standing. On the other hand, what would be the status of an author who has in fact made an original contribution to the POCC work that has since become obliterated in the course of the sequential creation process? Would they still be able to claim legal standing based on the original expression contributed to the POCC work at a certain point in its evolution, or would the obliteration of their original expression also lead to a loss or extinguishment of copyright over the POCC work, thereby precluding them from establishing legal standing?

VI. Inadequacy of open public (copyleft) licenses

65 The CC-SA (*Creative Commons* licenses with the 'Share-Alike' component) and GPL licenses constitute legal tools that can be used for securing the perpetuation of the inclusive copyright along the chain of sequential innovation. The copyleft requirement that is incorporated in these licenses ensures the sustenance of inclusivity by preventing any person from appropriating the POCC work (or any portion thereof) to their own exclusive use and by ensuring that any original expression that is added to the POCC work becomes a part of the inclusive good (or resource) that can be modified and built upon by downstream contributors.[80]

66 Open public licenses constitute standard-form royalty-free licenses that allow any member of the public to use and exploit copyright protected content in specifically defined ways, while allowing the owner of the copyright to reserve certain forms of exploitation to their own exclusive use. The licenses are irrevocable and perpetual (i.e. valid for an infinite period of time). Accordingly, any person is free to reproduce, distribute and transmit the work or any portion thereof as long as they respect the terms and conditions of the license.

67 The application of an open public license obviates the need for each potential user of a POCC work to individually obtain the authorization of each and every person who holds copyright over that content as a pre-condition to participating in the POCC authorship process. As such, it is a successful technical solution to the problem of license clearance and enables the smooth functioning of the process of sequential innovation associated with the POCC creation process.

68 Nevertheless, open public licenses rely upon the traditional copyright law framework for their own legal validity. For example, questions relating to the scope of rights granted under the license and issues relating to the legal title and ownership of rights for the purposes of enforcement will be determined within the scope of the traditional copyright law framework. Accordingly, under an open public license, each author of a POCC work will individually grant a license to a downstream contributor to use the content in which they hold a copyright in ways that are permitted under the license. This leads to the creation of a web of licenses that preserves the attendant inefficiencies relating to enforceability. Although they constitute useful legal tools for sustaining the perpetuation of inclusivity and collectiveness of the POCC process along the chain of sequential creation, open public-licenses do not offer a remedy for the inefficiencies arising from copyright fragmentation for the enforcement of copyright.

D. The case for an inclusive copyright

69 Taking into account the increasing importance of the POCC authorship model as an instrument for the creation of socially valuable content and the promotion of social dialogue, there is a need to revisit the existing exclusivity-based narrative of copyright law and to re-interpret copyright in a way that gives legal effect to the inclusivity inherent in the legal relations between persons engaged in the POCC authorship process. Such re-interpretation should be carried out especially keeping in mind the need to ensure more effective enforcement of copyright over the POCC work and the perpetuation of the quality of inclusivity along the chain of sequential creation.

70 As noted above, within the POCC authorship process, the individual contributions made by contributing authors to the POCC work become contextually inseparable and entwined with each other. The copyright held by those contributing authors over their individual contributions become similarly entwined thereby compelling authors to exercise and enjoy the copyright held by them over the POCC work in a collective manner as opposed to each author individually enjoying their copyright to the exclusion of others. Thus, the POCC authorship process demands a shift from the existing individualistic paradigm of copyright as an instrument for exclusion to a collective paradigm that is based on inclusion. It is noted that the communicational theory[81] of copyright law, which

80 This is carried out through the ''Share-Alike' elements of CC-SA and GPL licenses, ibid (n 76).

81 *See for example,* Abraham Drassinower, 'From Distribution to Dialogue: Remarks on the Concept of Balance in Copyright Law' (2009) 34 Journal of Corporation Law 991; 'Authorship

upholds the function of copyright as an instrument for advancing social enrichment through dialogic interaction and supports the creative and flexible interpretation of existing concepts and rules of copyright law to enable copyright to fulfil this function, provides a suitable normative framework for the development of such an inclusive copyright.

I. Concept of an 'inclusive' copyright

71 As discussed in section A. above, Dusollier's concept of an 'inclusive' property right is based on two key characteristics: (a) a legal right to a good that is held by a plurality of persons that is characterised by the collective enjoyment of the utilities of that good; and (b) an absence of a power or privilege on the part of the owner of the inclusive property right to exclude any other person having ownership of the same inclusive property right from benefitting from the utilities of the good. This denotes that an inclusive property right would grant each rightholder an equal and symmetrical right to collectively benefit from the utilities of the good without any single rightholder having a power or privilege to exclude any other rightholder from benefitting from those utilities.[82] Building upon this notion, I propose an 'inclusive' copyright that is held by each contributing author over a POCC work which would grant them an equal and symmetrical right to enjoy the utilities (e.g. reproduction, adaptation, distribution, communication and making available to the public) of that copyright protected work collectively with the other contributing authors, without any other contributing author having the ability to exclude them from benefitting from those utilities. The inclusive copyright holder would have the right to reproduce, distribute, adapt (including the creation of derivative works), make available and communicate to the public, the POCC work (either in whole or in part) in any manner, as long as the use of the POCC work does not have the effect of preventing any other contributing author from benefitting from those utilities of the POCC work.

72 The inclusive copyright would also grant authors the right to authorize any other third person to benefit from these utilities in accordance with the generally applicable terms and conditions (e.g. open public licenses) under which the POCC work is made available to the public.

73 The inclusive copyright is designed to include other persons in collectively enjoying the benefits of the common work. As will be discussed below in section D.II., its enforcement will be 'defensive' as its effect would be to prevent any person from appropriating the POCC work (or any portion thereof) to their own exclusive use or to prevent any person from using the POCC work in violation of the generally applicable terms and conditions under which it has been made available to the public. This is contrasted with existing exclusive copyright and its enforcement mechanism that is 'offensive' in the sense that it is aimed towards excluding any outside persons from benefitting from the utilities of the copyright protected work and for reserving those utilities to the exclusive enjoyment of the copyright holder.

II. Nature and scope

1. Who can obtain an inclusive copyright?

74 The inclusive copyright would vest in any person who contributes to the 'expression' of the POCC work at any stage of its evolution provided that the contribution has been integrated into that work. The requirement of contributing to the 'expression' of the POCC work would serve as a delimiting factor that reserves the enjoyment of the inclusive copyright to persons who have contributed to the authorship process as opposed to those whose contributions are merely of a technical (as opposed to a creative) nature (e.g. the correction of grammatical errors or spelling mistakes) or is peripheral to the authorship process without directly contributing to it (e.g. the contribution of ideas or research). Thus, in order to obtain an inclusive copyright in the POCC work, it is not required that the contribution made by a person qualifies as original expression in the sense that it is independently copyrightable. It suffices that the contribution is made towards the expression of the work and is therefore directly linked to the authorship process.

75 The term 'integrated' refers to the fact that at some point in the sequential creation process the contribution made to the expression of the POCC work has been incorporated into the work in the sense that it has been accepted by the creator community as being a legitimate step in the POCC authorship process. This would not be the case if, for example, the original expression has been removed by an editor (or other authorized person) or otherwise rejected for being an act of vandalism or for being contrary to community guidelines and platform policy. On the other hand, once the contribution has been integrated into the POCC work, its obliteration over the course of the

as Public Address: On the Specificity of Copyright vis-à-vis Patent and Trade-Mark' (2008) 1 Michigan State Law Review 199; 'Taking User Rights Seriously', in Michael Geist (ed), *In the Public Interest: The Future of Canadian Copyright Law*, (Irwin, 2005) 462.

82 Ibid Dusollier and Rochfeld (n 5).

sequential innovation process (or even its deletion or overwriting by a succeeding contributor where this is permitted under the terms and conditions of participation in the POCC process) would not result in the loss or extinguishment of the inclusive copyright held by that contributing author in the POCC work. This is because the claim to authorship of a POCC work does not stem from the individual relationship that subsists between the author and the original expression contributed to the work. Rather, it is rather based on the author's participation in the POCC process through contribution to the expression of the work at a certain point in the work's evolution. The essence of the POCC process is the incremental creation process within which contributing authors enjoy creative freedom and autonomy to build upon and modify content contributed by previous authors. The gradual obliteration of a contribution through improvements effected by succeeding contributors is a core feature of the POCC process and divesting a person of authorship status on the grounds of such obliteration would go against the rationale of POCC authorship. It would also allow space for gaming in the sense that any person who wished to divest a contributing author of copyright could maliciously delete or overwrite the contribution made by them. In addition, it would create uncertainty in the determination of copyright ownership in a POCC work. For example, imagine that the contribution made by an author of a POCC work who brings an action for the enforcement of inclusive copyright becomes obliterated during the course of the litigation process. Would this mean that they lose legal standing in the action?

2. Temporal dimension

76 In view of the evolutionary nature of a POCC work, it is necessary to recognize that the inclusive copyright extends to the entirety of the work (as opposed to the actual portion of the work in which the author's contribution was integrated). One consequence of this is that the inclusive copyright held by a contributing author would extend to the original expression that forms a part of the POCC work, both before and after obtaining inclusive copyright. Thus, when a person contributes to the expression of the POCC work at time 'X', the inclusive copyright they obtain over the work at that time should grant the ability to benefit from the utilities of any original expression contributed to the work both before and after time 'X'. This means that the inclusive copyright would extend to original expression that formed a part of the POCC work prior to the date on which they obtained inclusive copyright as well as to any contributions that have been made afterwards, including those that may be made in the future. Thus, the inclusive copyright would have a temporal dimension to it. This is based on the premise that the POCC work, although an evolving entity, constitutes a single work that is owned by all authors collectively. This would also give rise to a legitimate expectation on the part of the holder of the inclusive copyright to benefit from the value created by contributions made to the POCC work by other contributors at any point in the evolution of the POCC work, regardless as to whether that contribution has been made before the obtaining of the inclusive copyright over the work or after.

77 Nevertheless, it is necessary to make a distinction between contributions that are made to the POCC work in the sense of being integrated into the POCC work (by modifying, adding to and developing on existing content) and free-standing derivative creations that are based on the POCC work (or any portion thereof) but are meant to form separate and independent works on their own and are therefore not intended to form a part of the POCC work. Such derivative creations would not be considered as a part of the POCC work nor would their creation be considered to form a part of the POCC authorship process. Therefore, the inclusive copyright held by authors of the POCC work would not extend to such free-standing derivative works. Similarly, the author of the free-standing derivative work would not obtain an inclusive copyright over the POCC work but merely a license to use the content belonging to the POCC work in the creation of the new derivative work. The failure to make this distinction would mean that creators who wish to use the POCC work in their derivative creations, but do not wish to engage within the POCC creation process or to dedicate their original expression to the common creative endeavour, would be drawn into the POCC authorship process against their will and be forced to grant an inclusive copyright over the original expression contributed by them in creating the derivative work. This would then, serve as a disincentive to such persons from using the POCC work in the creation of new free-standing derivative works. Therefore, this limitation of the scope of the inclusive copyright is meant to incentivize persons who do not wish to participate in the POCC authorship process from creatively interacting with the POCC work in socially valuable ways, which thereby promotes the process of dialogic authorship.

3. Duration of protection

78 Determining the basis on which the duration of inclusive copyright over the POCC work is to be calculated is problematic. One approach would be to calculate the duration of protection from the date of the first publication of the POCC work (i.e. the initiation of the project). however, this would

mean that once the period of protection over the work has expired, the work would revert to the public domain and any person who contributes to the expression of the work after that date would not obtain an inclusive copyright. Another approach would be to grant an inclusive copyright over the POCC work to each person who contributes to the expression of the work that would run from the date on which that contribution was made. This would mean that the POCC work (as an evolving entity) remains under copyright protection so long as the sequential creation process continues and result in 'active' POCC works (i.e. works with regard to which the sequential creation process is continuing) remaining under copyright protection over an indefinite period of time, without falling into the public domain. I argue that, since the inclusive copyright is defensive in nature and is aimed towards the prevention of exclusive appropriation of the POCC work as opposed to the exclusion of persons from benefitting from its utilities, its protection under copyright over an indefinite period of time would not be unduly damaging to the public interest.

4. Creator Community

79 In most instances, it would be possible to identify a creator community that exists in relation to the collaborative creation endeavour within which the POCC authorship process takes place. This creator community would be formed by holders of an inclusive copyright who have engaged in the authorship process with the intention of collaborating in a common creation endeavour. This creator community would, in most instances, be a diffused community without any formal organization or identity. However, as will be discussed below, membership in the creator community could form a basis for the establishment of legal standing in an action brought against a holder of an inclusive copyright for the purpose of enforcing the terms and conditions under which the POCC work has been made available to the public.

III. Application and Effects

80 The inclusive copyright is designed as a tool for the 'inclusion' of other persons in the collective enjoyment of the benefits of the POCC work. In doing so it can be enforced at two levels.

81 At one level, the inclusive copyright can be enforced to prevent any person from excluding the holder of an inclusive copyright from benefitting from the utilities of the POCC work. For instance, if an author of the POCC work (i.e. holder of an inclusive copyright) or a third party seeks to appropriate the POCC work or any portion thereof to their exclusive private use, any other author of the POCC work would be able to enforce their inclusive copyright to prevent such exclusive appropriation on the basis that it infringes inclusive copyright to benefit from the utilities of the common work, collectively with the other rightholders.

82 At the second level, each holder of an inclusive copyright has the right to authorize or prohibit the use of the POCC work (or any portion thereof) either within the dedicated platform or outside it, within the framework of the generally applicable terms and conditions under which the POCC work has been made available to the public. For example, where the POCC work has been made available to the public subject to a CC or GPL license, each holder of an inclusive copyright over the POCC work would, by virtue of the collective nature of the inclusive copyright, qualify as a licensor of the CC or GPL license. This would mean that any holder of an inclusive copyright would be able to prevent the use of the POCC work by a third party in violation of the generally applicable terms and conditions for the public, regardless as to whether that use infringes upon an author's inclusive copyright to benefit from the utilities of the work. For instance, if the POCC work uses a public CC-BY-SA 3.0 license that requires the attribution of the creator community in any use of the work that takes place outside the dedicated platform, any holder of the inclusive copyright would, as a licensor of the CC-BY-SA 3.0 license, have legal standing to bring an action against any person who violates this condition for the breach of the CC-BY-SA 3.0 license contract.

83 Thus, in its enforcement, the inclusive copyright has both an inclusive and exclusive dimension. It is inclusive in the sense that it is designed to include any person within the common creation endeavour and to enable the enjoyment of the resulting POCC work by members of the public at large. Yet, it can also be used to prevent the exclusive appropriation of the common work and to exclude any person from enjoying the utilities of the POCC work in a manner that violates the terms and conditions.

84 It is important to note that, each author of the POCC work would not only be a licensor but would also be bound by those terms and conditions of the chosen license by virtue of having engaged in the POCC authorship process. Where the holder of an inclusive copyright violates these terms and conditions (even if such violation does not result in the exclusion of other holders of an inclusive copyright from enjoying the utilities of the work) it is necessary to recognize the right of any other holder of an inclusive right (as a member of the creator community) to bring an action based on breach of the license.

85 The symmetrical nature of the inclusive copyright that extends to the entirety of the POCC work as an evolving entity, enables any author of a POCC work to individually exercise and enforce inclusive copyright independently.

86 Given the fact that the inclusive copyright extends to the entire work as an evolving entity, the question arises as to whether an author who obtains copyright at time X could bring an action against any person (either based on copyright infringement or breach of contract) relating to an act that occurred or (in the case of an ongoing infringement or breach of contract) commenced prior to time X. The legitimate expectation held by each holder of an inclusive copyright to benefit from the value created by contributions made to the POCC work at any point in time provides a legal basis on which the author could claim legal standing in such an action. It is also noted that, in bringing such an action, the author will not be claiming legal relief on their own behalf but on behalf of all holders of an inclusive right and in the interests of sustaining and perpetuating the inclusivity of the POCC work along the chain of sequential creation. Therefore, such an author should be able to bring an action even though the cause of action arose prior to obtaining a legal claim (i.e. an inclusive copyright) over the POCC work.

E. Final observations

87 It must be reiterated that the concept of an inclusive copyright is still nascent. This paper has attempted to outline the concept of an inclusive copyright, its basic features and modalities of enforcement. Many important issues remain unresolved. For instance, how can the inclusive copyright be reconciled with moral rights that vest individually with each author as regards the original expression contributed by them, especially in jurisdictions that do not allow for the waiving of moral rights?[83] The moral right to prevent distortion is especially problematic since it could be invoked by an upstream author in order to prevent downstream authors from modifying the original expression contributed to the POCC work. A possible solution to this problem would be to substitute the individual moral rights held by various authors with a moral right that is collectively held by the community of authors, which can be exercised and enforced in accordance with the terms and conditions applicable to the POCC authorship process and community guidelines.

88 Another interesting question relates to the potential of the inclusive copyright to extend to other fields of application such as the protection of traditional cultural expression and folklore. As noted above in section B., the folkloric model of authorship as well as certain models of authorship used in oral traditions of religious discourse closely mirror the POCC authorship model. It would be fascinating to explore whether the inclusive copyright that has been devised in the context of the POCC authorship model can be also made applicable to such models of authorship.

89 Thus, the notion of an inclusive copyright opens up exciting vistas for further research. It is hoped that the concepts and arguments developed in this paper might serve to initiate a robust scholarly discussion on this issue that could lead to the introduction of a new inclusive right into copyright's legal toolbox.

83 For example, the copyright law frameworks of France and Belgium do not allow an author to waive moral rights over the original expression.

The blockchain ecosystem in the light of intellectual property law

by **Eleni Tzoulia***

Abstract: The study at hand delves into the technologies composing blockchain and designates its most significant practical applications to date. The technological ecosystem identified through this investigation is then scrutinized from the perspective of intellectual property law. It examines, in particular, under which conditions and to what extent blockchain itself as a standalone product, its individual components, and its several applications may be subject to a) copyright, b) database and trade secret protection, and c) patent law. The objective of this investigation is to identify the most suitable legal basis for raising claims against unauthorized use of the pertinent subject matter. The analysis also explores adversities posed to intellectual property law by modern technologies and contemplates their circumvention. The benchmark for this examination is the intellectual property law currently in force in the EU.

Keywords: digital timestamp; smart contract; blockchain database; crypto-patent; know-how

Recommended citation: Eleni Tzoulia, The blockchain ecosystem in the light of intellectual property law 13 (2022) JIPITEC 290 para 1

A. Blockchain's concept and operation

1 "Blockchain" is a type of distributed ledger technology (DLT). It is based on a decentralized Peer-to-Peer (P2P) network, i.e., a set of interconnected computers ("nodes") communicating directly with each other without any central server intervention. Within such networks users share computational resources and content, thus activating a common digital data repository. A particularity of blockchain is that peer nodes cannot interfere with the distributed content, e.g., amend or delete it. The following sections present the technological context behind this feature and comment upon its practical implications.

I. The pertinent technological context

2 Data in blockchain are grouped in blocks, placed one after the other in chronological order, thus forming a chain (as the name "blockchain" indicates). This chain is distributed as a single file to all nodes and each copy is updated on every new data entry. To safeguard the integrity and confidentiality of the entries, blockchain deploys cryptographic algorithms, in particular hash functions and asymmetric (public and private) key encryption.

3 In more detail, before being stored in the blockchain the submitted data get timestamped and converted into bit arrays of fixed length ("digest") by hashing algorithms. The hash output is unique for each

given input and gets adjusted to even the slightest modifications of the latter. In the blockchain pattern, moreover, hash outputs follow a sequential order from block to block. Therefore, any attempt to manipulate data stored in the blockchain shall cause inconsistencies in the hash values between the linked blocks, thus being promptly detected and invalidated.

4 The above hashing process cannot be reversed, i.e., it is not possible to recover the initial content through the corresponding hash value. To this end, a decryption process has to take place which is based on a pair of cryptographic keys. Asymmetric cryptography safeguards secure confidential correspondence between nodes. Namely, although one may anonymously join the network, the exchange of data is permitted only between trusted parties sharing the matching key-pair to lock and unlock the transmitted message.

5 According to the above, data entries in the blockchain are public but secured, in the sense that they are accessible and traceable by all connected nodes but their content can be disclosed only to authorized parties. They also acquire certified content and dates without the mediation of an outer authority or a central administrator. Therefore, it is argued that blockchain seeks "building trust with disintermediation"[1], thus constituting an appropriate tool for the digitalization of transactions that in the analog world would be subject to notarial certification, publicity formalities, and other security mechanisms under the auspices of accredited bodies.

II. Overview of the major blockchain applications

6 The simulation of "trusted surveillance and audit", which is achieved by technological means within the blockchain ecosystem, justifies the fact that the first applications based on this technology referred to "cryptocurrencies", the conclusion and execution of the so-called "smart contracts", as well as the registration and management of digital files potentially subject to intellectual property rights (IPRs). Nevertheless, blockchain is considered to have a much broader scope of application being able to provide new prospects in sectors such as healthcare[2], supply chain tracking[3], elections[4], machine learning[5], etc.

1. Cryptocurrencies

7 The first practical blockchain application has been a digital payment and value transfer system using as currency unit the so called "bitcoin". The code of this system was released in 2008 under the signature of some "Satoshi Nakamoto", a presumed pseudonymous person or team of persons remaining unidentified to date. In the context of this application, blockchain entries relate to bitcoin transactions[6] and may refer to the amount provided each time, its remitter, and the beneficiary.

8 The strong investment interest prompted by bitcoin, incited the release of competitive products with a similar function, thus establishing a category of digital value units characterized as "cryptocurrencies". This term indicates the use of encryption techniques for ensuring the validity and confidentiality of the relevant transactions. The value attributed to cryptocurrencies depends on the competition developed in the relevant market and the forces of supply and demand. Also, the production costs for each type

* Adjunct lecturer for commercial law, Aristotle University of Thessaloniki (AUTH), post-doctoral researcher for law and technology, Hellenic Open University (HOU), Greek State Scholarship Foundation (IKY) Scholar. Email: elena.tzoulia@gmail.com. This paper has been partly produced within the framework of an Austrian Standards Fellowship at the Faculty of Law of the University of Graz.

1 See European Parliament Resolution of 3 October 2018 on Distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)), (2020/C 011/03), OJ C 11, 13.1.2020, p 7–14.

2 Blockchain can host e.g. distributed patient data files, which get updated in real-time through wearables and are remotely accessible to all stakeholders (doctors, hospitals and diagnostic centers), thus facilitating telemedicine operations (smart health). See EPO, Patents and the Fourth Industrial Revolution. The inventions behind digital transformation, December 2017, p 74.

3 Traceability of goods, control of counterfeits. See European Parliament Resolution (n 1) rec. 16.

4 See on the "smart voting" issue <https://businesstech.co.za/news/it-services/237547/a-secure-online-voting-system-using-blockchain/> accessed 15 May 2022.

5 It is argued that blockchain can ensure transparency and clarity in the operation of smart software governed by machine learning algorithms which are used in automated decision-making systems. See. Kritikos, European Parliament Scientific Foresight Unit (STOA), What if blockchain could guarantee ethical AI?, PE 656.334, 2020, <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/656334/EPRS_ATA(2020)656334_EN.pdf> accessed 15 May 2022.

6 Such as purchases, sales, and payments.

of cryptocurrency, in terms of computational resources and energy consumption, are of relevance in this respect[7].

9 From a technological perspective, cryptocurrencies are data produced, exchanged, and stored through special software in the decentralized P2P network where blockchain is hosted as described above[8]. This very nature of cryptocurrencies as digital content facilitates the creation and release of unbacked copies which are devoid of any value. To prevent incidences of duplicated cryptocurrencies being used multiple times by the same user[9], peer nodes enforce "consensus protocols". The latter term refers to agreements as to how transactions submitted in the network shall be authenticated by the nodes themselves.

10 To date, the most popular protocols have been the ones known as "proof-of-work" and "proof-of-stake". In their context, nodes compete against each other to compute whether each documented transaction fits in the flow of hash values between the linked blocks.[10] The node solving the puzzle is rewarded with cryptocurrencies. Because this process entails making profits through the expenditure of computational resources and energy, it is also called "mining". Respectively, users engaging in the verification process are called "miners".[11]

2. Smart contracts

11 The term "smart contract" pertains to software programmed to execute particular tasks when certain predetermined conditions are satisfied. Consequently, it does not refer literally to contracts concluded and executed in the digital environment. The program's code rather enforces a consensus that has already taken place in the physical world.[12] For example, an agreement may dictate that in case of a flight delay of X hours, the passenger's account shall be credited with a certain amount of money. In this case, the smart contract software shall automatically launch the compensation process as soon as it receives a delay notice. In this context, blockchain is used as a storage medium for automated transactions, also safeguarding their immutability and confidentiality. Yet, for smart contracts to operate several technologies may need to be deployed, like artificial intelligence (AI), internet of things (IoT), crypto-assets, etc.[13]

12 In the above vein, nowadays self-executable statutes may facilitate the operation of digital associations/partnerships.[14] This is the case with Decentralized Autonomous Organizations (DAOs) which use the "Ethereum" blockchain for the conclusion and execution of the (smart) corporate agreement governing them. In this case, namely, the underlying software allows the establishment and operation of a digital entity resembling a legal person.[15]

3. Digital files timestamping

13 Digital files are inherently susceptible to unauthorized use and counterfeit. To certify the production date of their data and safeguard their integrity, individuals nowadays may use blockchain-based timestamping services administered by Trusted Third Parties (TTP). By being stored in the blockchain the file leaves a unique digital fingerprint, which certifies its existence at a given time and its origin from an identifiable entity. It also becomes tamper-proof and can be traced. The relevant service applies regardless of the digital file's nature as the subject matter of IPRs, i.e., whether it represents a literary, scientific, or artistic "work", an industrial design, a

7 See on the legal nature and the function of cryptocurrencies Chiara Zilioli, 'Crypto-assets: Legal Characterisation and Challenges under Private Law' [2020] E.L. Rev. 251, 266.

8 Christian Engelhardt and Sascha Klein, 'Bitcoins – Geschäfte mit Geld, das keines ist - Technische Grundlagen und zivilrechtliche Betrachtung' [2014] MMR 355 ff.

9 What is known as the "double spending issue".

10 See Daniel Kälberer, 'Blockchain-Technologie: Virtuelle Währungen aus handels- und steuerbilanzieller Sicht' [2021] BC 417, 419 ff.

11 See Matthias Terlau in Herbert Schimansky and others (eds), Bankrechts-Handbuch (5th edn, C.H.Beck 2017) paras 135-140.

12 See Thomas Söbbing, 'Smart Contracts und Blockchain-Technologie. Definition, Arbeitsweise, Rechtsfragen' [2018] ITRB 43; Andreas Börding and others, 'Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht. Praxis und Rechtsdogmatik' [2017] CR 134.

13 Martin Fries, 'Schadensersatz ex machina' [2019] NJW 901, 902 ff.

14 See Shen Wei, 'When FinTech meets corporate governance: opportunities and challenges of using blockchain and artificial intelligence in corporate optimization', [2021] J.I.B.L.R. 53; Gaspare Dori, 'Blockchain, smart contracts and mergers and acquisitions: or how to re-establish trust' [2021] I.B.L.J. 289.

15 See Maximilian Mann, 'Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp? Gesellschaftsrechtliche und kollisionsrechtliche Implikationen' [2017] NZG 1014.

trademark, trade secret, etc. However, timestamping produces evidence of priority and authorship which may be used in the context of related legal disputes. Thus, the future establishment of IPRs on the timestamped file's content may ultimately be facilitated[16].

B. Intellectual property rights on the blockchain-related subject matter

14 Evidently, a blockchain-related industry has currently emerged which hosts various activities, alongside any cryptocurrency transaction and conversion services. Entrepreneurship within the blockchain ecosystem may prove particularly profitable.[17] This potential reinforces the interest of blockchain developers and investors to protect their products against counterfeiting and unauthorized use. To this end, they need to establish exclusive ownership of these assets, enforceable against any competing undertakings. In this and the following section, the study scrutinizes EU intellectual property law as a tool to achieve the above objectives.

15 The complexity and versatility of blockchain poses normative challenges, which in the IP domain in particular manifest themselves in the form of intersections and conflicts between individual IPRs. Indeed, according to the preceding analysis, blockchain constitutes a network of peer nodes which hosts records of encrypted data administered by special software. At the same time, blockchain is a business model apt for digitalizing and decentralizing several legal acts and relationships. Each of these aspects is subject to an individual set of IPRs, which serve distinct purposes and may ensure a different level of protection in each given case. It is questionable, which sector of intellectual property law may provide the broadest and most rounded protection to the blockchain-related subject matter, as well as whether any confluent rights may be exercised conjunctively or the establishment of one right excludes the evocation of the other.

16 Primarily, however, the assumption itself that IP law is in principle applicable within the blockchain ecosystem, is negotiable. The developer of bitcoin, the first known blockchain application to date, published incognito the pertinent code in a whitepaper of 2008. "Nakamoto" continued to edit this code until 2010 and then resigned, thus allowing the free exploitation of the application by third parties. It can therefore be argued that the technologies under consideration have been dedicated to the public domain ever since, thus not being subject anymore to exclusive IPRs.

I. Blockchain-related technologies in the public domain

17 Public domain refers to material which may be used by any person without permission.[18] In the sphere of IP, the public domain comprises products of human intellect that no longer are or have never been subject to private ownership.[19] This status may be in principle attributed to limitations and exceptions of IP law. It is disputed whether the relinquishment of one's own IPRs may effectively place the subject matter concerned within the public domain. Most jurisdictions answer this question in the negative. However, unconditional licensing in the form, e.g., of free and open-source software (FOSS) and the creative commons zero (CC0) licenses, ultimately unfolds the legal effects of IP relinquishment.[20]

1. IP public domain in the EU

18 In EU law in particular, public domain dedication of IP is not regulated concretely. Industrial property law prescribes similar rights, e.g., to formally surrender one's trademarks[21], abandon patents[22], and judi-

16 See also Michèle Finck and Valentina Moscon, 'Copyright law on Blockchains: Between new forms of rights administration and digital rights management 2.0' [2019] IIC 77; Tania Kern, 'Blockchain and intellectual property rights: blockchain anchoring, a ground-breaking means of proof to the rescue of creators?', [2021] I.B.L.J. 279.

17 See for instance the case of "Coinbase", a US company engaging in the intermediation of cryptocurrency transactions <https://www.cbinsights.com/research/report/coinbase-strategy-teardown/> accessed 15 May 2022.

18 Ilanah Simon Fhima, 'The public domain' [2019] I.P.Q. 1.

19 See on the definition and the ratio of public domain in the field of intellectual property Séverine Dusollier, 'The public domain in intellectual property: Beyond the metaphor of a domain' in PL Jayanthi Reddy (ed.), *Intellectual Property and Public Domain* (Icfai University Press Hyderabad 2009) 31.

20 See Graham Greenleaf and David Lindsay, *Public Rights* (Cambridge University Press 2018) 509 ff.

21 See Art. 57 Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trademark, OJ L 154, 16.6.2017, p 1–99.

22 See Art. 87 EPC in conjunction with Rules 45 par. 3 and 162 par. 4 of Implementing Regulations, as well as Guidelines for Examination Part A, Chapter III, par. 5.2, Part B, Chapter III, par. 3.4, Part C, Chapter IX, 1.3.

cially revoke one's IPRs in case of disuse.[23] In all these cases, however, the subject matter concerned does not become communal, but rather subject to exclusive priority IPRs established by third parties. On the other hand, industrial property law and copyright alike, do not provide for the ex officio prosecution of infringements. Therefore, right-holders who waive their claims against violators of their IPRs, legitimize de facto the unauthorized use. Such tolerance, however, cannot be construed as an implicit transfer of one's IP. To this end, a written agreement or an explicit statement is required.[24] What is more, moral rights are regarded as in principle indispensable.

19 In any case, materials incorporating public domain elements may be eligible for IP protection, as long as they demonstrate, for instance, originality from the perspective of copyright, inventiveness from the perspective of patent law, etc.[25] However, the applicable IPRs do not extend to the public domain elements themselves, which shall remain available for everyone to use. In the same vein, intellectual achievements culminating from unauthorized exploitation of third-party IPRs may be eligible for IP protection. As long as the aggrieved parties refrain from raising claims against the violator, the latter can freely and exclusively exploit the secondary product comprising the non-proprietary materials.

2. Framing the blockchain-related public domain

20 According to the above, whether the bitcoin system code has been dedicated to the public domain or not, is not uniformly regulated among legal orders worldwide. The fact is that over the last decade the blockchain ecosystem has significantly evolved. Expert contributions have enriched it with new or improved technologies and new blockchain applications have been devised. No right-holder opposition has been ever expressed against this progress and no IP claims have been raised. Therefore, it appears that the person or team behind the code of bitcoin has unconditionally abandoned any relevant IPRs.

21 Consequently, it could be argued that—either legally or de facto—this primary blockchain application is encompassed by the public domain. However, ownership and individual protection of improvements thereto, as well as novel blockchain-related products and services, may be claimed. This is true, despite the fact that these achievements take advantage of the fundamental blockchain technology and concept. As a result, the abovementioned contemplations on the appropriate legal basis for IP protection must be further examined.

II. Copyright protection for blockchain-related software

22 With regards to software, which constitutes an essential blockchain component, copyright is applicable in principle. This derives in particular from Article 10 paragraph 1 of the TRIPS Agreement, as well as Article 4 WIPO Copyright Treaty (WCT), pursuant to which computer programs are subject to copyright as "literary works" within the meaning of Article 2 of the Berne Convention. These provisions have influenced software protection at an international level. In the EU in particular, the protection of electronic programs is assigned to copyright pursuant to Directive 2009/24/EC.[26]

23 Both Article 9(2) TRIPs and Article 2 WCT provide that copyright protection applies to expressions and not to ideas, procedures, operation methods or mathematical concepts as such. The ratio behind these exceptions relates to not monopolizing ideas, to the detriment of technological progress and industrial development. Accordingly, the object of the protection conferred by Directive 2009/24/EC is the expression in any form of computer programs, as well as the preparatory design material capable of leading to the reproduction or subsequent creation of a program.[27]

24 Computer programs are considered to be expressed through their source and object code.[28] Source code is the algorithm that guides the operation of the program once it is encoded in a programming language. An object code is described as the source code of the program, after being compiled in binary machine language, so that it can be executed by the computer hardware. Preparatory design work may

23 See Art. 58 Regulation (EU) 2017/1001.

24 See Art. 20 par. 3 Regulation (EU) 2017/1001; Art. 8 par. 1 Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, OJ L 361, 31.12.2012, p 1–8.

25 See Art. 14 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130, 17.5.2019, p 92–125.

26 Directive 2009/24/EK of the European Parliament and Council of the 23rd of April 2009 for the legal protection of computer programs, OJ L 111, 5.5.2009, p 16–22.

27 See article 1 par. 2 and recital 11 of the Directive 2009/24/EC.

28 See article 10 par. 1 TRIPS.

include, for example, structures or organizational charts developed by the programmer, which may be re-transcribed in source code and object code and culminate in the execution of the program.[29] On the contrary, any element comprising ideas and principles or not enabling the program's reproduction directly or indirectly, e.g., the underlying logic and algorithms, any programming languages, the format of data files used to exploit certain functions of the computer program, the graphic interface enabling users to access the program's features[30], as well as the functionality of a computer program are not subject to copyright.[31]

25 According to Article 1 paragraph 3 Directive 2009/24/EC, software in the above sense shall be protected by copyright if it is "original". Originality is regarded as an intrinsic feature of any "work" and copyright protection is in principle reserved for intellectual creations reflecting their author's individuality. In the case of software, however, the relevant threshold is arguably low. In principle, copyright may be acknowledged for any computer program provided that it is not a copy or absolutely banal.[32]

26 In view of the above, it appears that all computer programs in the blockchain ecosystem may be subject to copyright, as long as they do not copy existing software. The protection covers the program's code before and after its compilation, as well as any preparatory design material, but neither the outcome of the program's execution, nor the underlying concept.[33] Consequently, any competitor may reproduce the program's functionality by observing, studying, and testing its operation. The competing product shall not infringe the author's copyright on the model software as long as it relies on a different code. This is true, even if it uses the same programming language and data files. Therefore, it may be argued that copyright promises limited protection for blockchain-related software, so that alternative, or complementary legal bases of IP protection should be explored.

III. The legal framework for database protection and its relevance for blockchain

27 Data records constitute another fundamental feature of blockchain. Compilations of data or other material that by reason of the selection or arrangement of their contents constitute intellectual creations, are subject to copyright. This approach is prescribed on an international level by Article 10 paragraph 2 TRIPS, Article 5 WCT, and Article 2 paragraph 5 of the Bern Convention. It has been also espoused by the EU legislator as apparent from Article 3 Directive 96/9/EC.[34] The latter act complements copyright protection by prescribing a sui generis IP right of EU-limited application scope for "databases".

1. The Directive 96/9/EEC

28 The term database in Directive 96/9/EEC refers to any collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.[35] An independent material is supposed to demonstrate autonomous informative value in relation to the rest database content.[36] Moreover, database materials are systematically or methodically arranged when they are classified according to predetermined criteria, e.g., alphabetically, numerically, etc., rather than randomly accumulated.[37] A database in the above sense is also expected to include technical or other means allowing access to and retrieval of its separate materials.[38]

29 See recital 7 of Directive 2009/24/EC and Opinion of AG Bot in C-393/09 of 14.10.2010, Bezpečnostní softwarová asociace, ECLI:EU:C:2010:611, rec. 63.

30 C-393/09 of 22.12.2010, Bezpečnostní softwarová asociace, ECLI:EU:C:2010:816, rec. 37-42.

31 C-406/10 of 02.05.2012, SAS Institute, ECLI:EU:C:2012:259, rec. 29-46.

32 See Gernot Schulze, 'Geschützte Werke' in Thomas Dreier and Gernot Schultze (Eds) *Urheberrechtsgesetz* (C.H.Beck 2022) 113; Martin Vogel, '§ 87a' in Ulrich Loewenheim and others (Eds) *Urheberrecht (UrhG, KUG, VGG) Kommentar* (C.H.Beck 2020) 1470 ff. Differing view from Marie-Christine Janssens, 'The software Directive' in Irini Stamatoudi and Paul Torremans (Eds) *EU Copyright law: A commentary* (Edward Elgar Cheltenham UK, Northampton MA USA 2021) 75.

33 C-406/10 of the 02.05.2012, SAS Institute Inc., ECLI:EU:C:2012:259, rec. 39-41.

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

35 See Art. 1 para 2 Directive 96/9/EEC.

36 C-444/02 of 09.11.2004, Fixtures Marketing v OPAP, ECLI:EU:C:2004:697, rec. 33.

37 Vogel (n 32) 1940.

38 Such as electronic, electromagnetic or electro-optical processes, indexes, tables of contents, etc. See rec. 13

29 Similar to computer programs, databases are eligible for copyright protection provided that they are original, i.e., "the author's own intellectual creation".[39] Copyright covers the selection and arrangement of the database's particles and does not extend to the content itself.[40] Other criteria than that of originality, e.g., aesthetic, or quantitative standards, shall not be applied when determining the eligibility of a database for copyright protection. The originality criterion is satisfied in this case when, through the selection or arrangement of the data, the author expresses their creative ability by making free and creative choices, thus stamping a personal touch.[41] Reversely, the originality criterion is not satisfied when the setting up of the database is dictated by technical considerations, rules or constraints that leave no room for creative freedom.[42]

30 The originality benchmark may discourage ventures into modern information storage and processing systems. To circumvent this risk, in view of establishing a common information market[43], Article 7 et seq Directive 96/9/EEC prescribes a sui generis intellectual property right for the maker of a database where the obtaining, verification, or presentation of the database's contents demonstrates substantial investment in qualitative or quantitative terms. Hence, for this special kind of protection to be granted, it is decisive whether the database maker has dispensed human[44], financial[45], or technical resources[46] to find and collect the database contents, control their consistency and accuracy, classify them, and manage their individual accessibility system.[47] The substantial character of the investment is examined quantitatively, i.e., in relation to its scale, or qualitatively, i.e., in relation to its manner and impact.[48] For instance, an innovative arrangement of the collected materials may represent a considerable investment in human capital in qualitative terms.[49]

31 As long as these conditions are met, the database maker can forbid the extraction and re-utilization in total or to a substantial extent of the database contents by third parties without previous authorization. This is true, irrespective of the commercial purpose of such practices.[50] Namely, a substantial infringement in this case may not only derive from the manufacture of a parasitical competing product, but also from any other use which may cause significant detriment—in quantitative or qualitative terms—to the investment made to set up the database.[51]

32 As it follows from Article 7 in conjunction with Recital 41 of the Directive, the above right is granted to the database "maker". The latter term refers to the person who takes the initiative and bears the risk of investing in the database manufacture. Thus, the auxiliary person who performs the technical work of constructing the database as a simple representative of the person in charge, does not fall under this concept. In other respects, the database maker may equally be a natural or a legal person. More entities bearing the relevant capacity become joint owners and the relationship between them is governed by the applicable national law.[52]

33 The abovementioned right can be transferred, assigned, or granted with or without consideration under a contractual license. It may be established on any database in which either the manufacturer or the rightsholder is an EU national or has at least usual residence within the Union.[53] Copyright and a sui generis IP right can coexist on the same database.[54]

Directive 96/9/EEC and C-444/02 (n 36), rec. 30.

39 See Art. 3 para 1 and rec. 16 of Directive 96/9/EEC.

40 See rec. 26-27 Directive 96/9/EEC.

41 C-604/10 of 01.03.2012, Football Dataco Ltd and others v Yahoo! UK Ltd and others, ECLI:EU:C:2012:115, rec. 38; C-145/10 of 01.12.2011, Painer, ECLI:EU:C:2011:798, rec. 89, 92.

42 C-604/10, ibid, rec. 39; C-403/08 and C-429/08 of 04.10.2011, Football Association Premier League and Others, ECLI:EU:C:2011:631, rec. 98.

43 See rec. 9-12 Directive 96/9/EEC.

44 Man-hours, cognitive energy and expertise, etc.

45 Money in the form of, e.g., funds, salaries, expenses.

46 Equipment, infrastructure, etc.

47 See C-338/02 of 09.11.2004, Svenska Spel, ECLI:EU:C:2004:696, rec. 24-27.

48 See recital 19 Directive 96/9/EEC and C-304/07 of 09.10.2008, Direct media Publishing GmbH, ECLI:EU:C:2008:552, rec. 24; C-203/02 of 09.11.2004, British Horseracing Board, ECLI:EU:C:2004:695, rec. 69 et seq; C-444/02, ibid, rec. 44.

49 Vogel, (n 32) p 1954.

50 C-545/07 of 05.03.2009, Apis-Hristovich EOOD, ECLI:EU:C:2009:132, rec. 40 et seq; C-304/07, (n 48) rec. 29 et seq; C-203/02, (n 48) rec. 46-51.

51 See recital 42 Directive 96/9/EEC.

52 Justine Pila and Paul Torremans, *European Intellectual Property law* (Oxford University Press 2016) 513.

53 See Article 7 par. 3 and 11 Directive 96/9/EEC.

54 Article 7 par. 4 Directive 96/9/EEC.

2. The blockchain database

34 It is argued that the distributed ledger of blockchain represents a database within the meaning of Article 1(2) Directive 96/9/EEC.[55] This is correct in principle, given that the blockchain hosts a collection of data classified in blocks according to their chronological order and technical compatibility. Data entries may be conceptually independent and self-sufficient, irrespective of their intersection and correlation, as is the case with entries referring to individual cryptocurrency transactions, pieces of digital content, diagnostic test results, etc. There is also a particular mechanism in place for nodes retrieving and inspecting each entry separately, i.e., public-key encryption.[56]

35 The database established within the blockchain is potentially subject to copyright, to the extent that the selection and/or arrangement of its content is original. It can be argued that arranging data into blocks, as an inherent and distinguishing feature of blockchain, falls within the realm of the public domain. In any case, separating data in blocks is not a creative arrangement, in particular if it is performed in chronological order and justified by technical reasonings.[57]

36 As far as the sui generis right of Article 7 et seq Directive 96/9/EEC is concerned, it may be conceived as protecting blockchain in its capacity as a carrier medium for the data collection recorded within it.[58] The pertinent protection extends to any technology used for accessing the individual contents of a blockchain database, e.g., decryption keys.[59] From this perspective, all peer nodes in the relevant network shall be regarded in principle as the makers and joint owners of the blockchain database.

37 In this context, no substantial investment can be substantiated with respect to "obtaining" the contents of the blockchain database, since the contents are created rather than sought and found by the nodes. This however does not negate the sui generis protection of Article 7 et seq, as long as the "verification and presentation" of the database contents, i.e., the process of classifying them, verifying, and maintaining their integrity requires high expenditures in computing power, time, and expertise.[60] In public blockchain applications, such as cryptocurrency networks, the "substantial" investment requirement should be deemed fulfilled by only large investors and miners. Thereby, the expanding circle of potential sui generis protection co-beneficiaries shall be restricted, thus also making the exercise of the pertinent rights manageable.[61]

IV. Blockchain and trade secrets law

38 The regulatory framework for trade secrets is commonly retrieved for the protection of subject matter not covered by other IPRs, like algorithms[62], mathematical concepts, and business methods, as well as datasets ineligible for either copyright or database protection.[63] Any piece of information which is not widely known, nor directly accessible to persons operating in the relevant trading sector may be considered a trade secret. Such information is expected to have acquired commercial value precisely because of its secret character and its rightful owner must make reasonable efforts to keep it confidential.[64]

39 The rightful owner enjoys the right to prohibit any unauthorized acquisition, use or disclosure of their trade secrets.[65] However, this does not imply the establishment of an absolute right on protected information. Therefore, the independent acquisition or development of the same know-how, e.g., through research and analysis, or even reverse engineering,

55 Sebastian Pech, 'Who owns the Blockchain? How copyright law allows rights holders to control Blockchains' [2021] J. Bus. & Tech. L. 59, 69 ff.

56 Compare C-444/02, ibid, rec. 28-32.

57 Pech, (n 55) 71.

58 Vogel (32) 1945.

59 See rec. 20 Directive 96/9/EEC.

60 See C-46/02 of 09.11.2004, Fixtures Marketing Ltd v Oy Veikkaus Ab, ECLI:EU:C:2004:694, rec. 34-40; C-203/02, (n 48) rec. 31-36; C-338/02, (n 47) rec. 24-30.

61 See also the relevant contemplations of Pech (n 55) 72 ff.

62 See Katharina Scheja, 'Schutz von Algorithmen in Big Data Anwendungen – Wie Unternehmen aufgrund der Umsetzung der Geschäftsgeheimnis-Richtlinie ihre Algorithmen wie auch Datenbestände besser schützen könne' [2018] CR 485, 487 ff.

63 The legal framework under examination is considered for instance appropriate for the protection of training datasets serving machine learning purposes. See BGH of 28.01.2014, VI ZR 156/13, BGHZ 200, p 38-51.

64 See Article 39 TRIPS and 2 para 1 of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of know-how and business information which has not been disclosed (trade secret) from illicit acquisition, use and their disclosure, OJ L 157, 15.6.2016, p 1–18.

65 See Article 4 Directive (EU) 2016/943.

remains possible.[66] Moreover, non-disclosed innovations are not considered to be a part of "the state of the art" in the pertinent technological field, i.e., knowledge already conquered, that would render any future equivalent achievements "non-novel". As a result, third parties acting in good faith may acquire priority IP rights on the subject matter protected as a trade secret.[67] In any event, the protection of information as a trade secret is considered a restrictive factor on its commercialization.

40 According to the above, the various blockchain-related technologies and applications may be subject to the legal framework for trade secrets, both regarding their technical features and in terms of their character as business schemes. This presupposes, however, that whoever lawfully controls the relevant information takes reasonable steps to safeguard its confidentiality.[68] Distributed ledgers in the narrow sense of the term, like blockchain hosting cryptocurrency transactions, are decentralized P2P networks open for everyone to join by downloading the necessary software for free and entering into the pertinent consensus protocol. The legal protection prescribed for trade secrets is extraneous to the public character of such applications. On the contrary, private blockchain networks, e.g., smart contracting, smart health, timestamping applications, etc., that allow a limited number of persons — commonly whoever has been granted a license — to connect, could be protected as trade secrets.[69] This presupposes, however, that all interconnected nodes are bound by a confidentiality agreement.

V. The shift towards patent law

41 Patents are legal titles establishing IPRs on inventions. Competent authorities grant them after having scrutinized the claimed subject matter with regards to its novelty and inventiveness, i.e., its contribution to the state of the art. Patent law provides protection for entire technological achievements, as individual products delivering certain tangible outcomes. Therefore, in comparison to copyright, patents can extend the protection granted by IP law beyond the source/object code to the functionality of a program. From another perspective, patent granting presupposes the disclosure of all details related to the implementation of the claimed invention. As a result, it is supposed to contribute to the dissemination of knowledge and the enhancement of innovation by simultaneously circumventing any competitive risks associated with the confidential character of know-how.

42 In view of the aforementioned advantages, patent law is increasingly being invoked as a legal basis for protecting blockchain-related technologies and applications. However, the capacity of achievements from the IT sector to be patented is subject to certain limitations on an international level.[70] In the following section the study analyses the requirements for patenting blockchain-related subject matter, pursuant to the provisions in force within the European legal order.

C. Blockchain-related subject matter in the light of patent law

43 Patent granting is in principle administered by provisions of national reach. Accordingly, the rights deriving from a patent are territorial, in the sense that the protection granted covers the national territory where the examination authority is based. International treaties have nonetheless established unified procedures for granting patents of broader scope.

44 Such a treaty is the European Patent Convention (EPC). Based on the pertinent legal framework, an undertaking may make patents enforceable in all member states of the EPC through one single application and examination process.[71] More specifically, European patents are enforceable in all EU member states and several third countries.[72]

66 See Article 3 and recital 16 Directive (EU) 2016/943.

67 Anthoula Papadopoulou, 'Creativity in crisis: are the creations of artificial intelligence worth protecting?' [2021] jipitec 408, 416.

68 See Thomas Söbbing, 'Schutz von Algorithmen. Rechtliche Anforderungen und vertragliche Gestaltung' [2019] ITRB 192, 194.

69 Christian Hess, 'Die Blockchaintechnologie im Lichte des Geschäftsgeheimnisschutz- und Patentrechts' [2020] GRUR-Prax 251.

70 See for the United States Antonio DiNizo, 'From Alice to Bob: The patent eligibility of blockchain in a post-CLS Bank world' [2018] Journal of Law, Technology & the Internet <https://scholarlycommons.law.case.edu/jolti/vol9/iss1/2>.

71 These are not patents automatically valid in all Member States of the Convention, such as those regulated by Regulation (EU) 1257/2012 of the European Parliament and of the Council of 17.12.2012 establishing enhanced cooperation in the field of establishing a single patent protection regime, OJ L 361, 31.12.2012, pp 1-8.

72 European patents are also recognized in certain candidate countries for EU accession and in third countries (validation states).

The examination of European Patent applications is carried out by the European Patent Office (EPO). The EPO's Boards of Appeal are competent on a supranational level to revoke European patents.

I. Software and database patentability pursuant to the EPC

45 EPC does not define the term "invention" but includes a non-exhaustive list of non-inventions in Article 52 paragraph 2. Accordingly, mathematical methods, business practices, information presentations and computer programs fall foul of the invention concept, thus being in principle patent-ineligible. However, pursuant to paragraph 3 of the same Article, this is true inasmuch as a patent application refers to the excluded subject matter "as such".

46 Thus, even though achievements from the IT sector appear to be explicitly excluded from patent law protection, it is ultimately acknowledged that EPC makes their patentability conditional upon the demonstration of "technical character". Indeed, Article 27 of the TRIPS Agreement defines inventions as "products or processes, in all fields of technology", thus implicitly declaring that patent law protection is meant for creations from the technical field. This postulation was not explicitly adopted in the EPC until its amendment in 2000.[73] However, its implicit embrace has always been apparent from the repeated references to the technical realm in the provisions of the Convention itself, as well as in the implementing regulations, and the examination guidelines that complement and specify it.

47 Whether an invention from the IT sector demonstrates a technical character is examined on a case-by-case basis, in light of the EPO's "two-hurdle" approach.[74] In this context, a two-stage examination is carried out. First, it is examined whether the claimed subject matter exploits technical means or is rather confined to theoretical considerations. Accordingly, any subject matter invoking the use of hardware, e.g., an electronic device, for its operation or implementation may be patented, even if it falls in principle under the list of Article 52 paragraph 2 EPC.[75]

48 Subsequently, an examination whether the claimed invention solves a technical problem by the claimed technical means must be conducted. The invention will be ultimately deemed patentable, if it solves the technical problem in a novel way that is not obvious to the average person skilled in the art. A technical solution is in principle effectuated by software that, e.g., controls the operation of a machine or an industrial process. However, when it comes to the software controlling only the internal functions of a computer without tangible results in the external world, as is the case for the so-called system[76], application[77], and network[78] software, as well as for various kinds of utility programs[79], a "further technical effect" must be demonstrated.

49 Accordingly, the required technical character is not evident from the mere activation and operation of a computer by means of the program.[80] In this respect, it is also not sufficient that the program merely automates a process from the analog environment. On the contrary, a patentable program is expected to dictate a new structure for the computer system or a new way of functioning by adding new features or fixing malfunctions.[81]

50 Therefore, methods of processing, classifying, analyzing, distributing, etc., digital data cannot be pat-

73 See OJ EPO 2007, Special Edition 4, p 48. Accessible via: http://archive.epo.org/epo/pubs/oj007/08_07/special_edition_4_epc_2000_synoptic.pdf.

74 T 0641/00 (Two identities/COMVIK) of 26.9.2002.

75 This formula is known as "any hardware approach", having been outlined in the context of the decision T 0931/95 of 8.9.2000 (Controlling pension benefits system) and consolidated by the decision T 0258/03 of 21.4.2004 (Auction method/HITACHI). See also T 0424/03 (Clipboard formats I/ MICROSOFT) of 23.2.2006. Accordingly, it has been found sufficient that a patent application invokes, e.g., the use of a computer or a computer-readable storage medium (CD, DVD) or a smart card or an electronic communication network, etc., to successfully pass the first stage of the examination process.

76 System software manages a computer's main resources, i.e., central processing unit (CPU), memory, disk drivers, etc., and its peripherals. It mainly consists of operating systems (OS).

77 Application software refers to programs directing a computer to execute specific tasks according to the user's commands. It includes word processors, web browsers, music players, etc.

78 This software category encompasses applications facilitating the establishment and operation of networks and data sharing among electronic devices.

79 This term refers to software support, maintenance, and development tools and comprises programs like compilers, linkers, debuggers, etc.

80 T 1173/97, Computer program product/IBM, of 01.07.1998, rec. 6 et seq

81 See T 0172/03 (*Order management/RICOH*) of 27.11.2003; BGH X ZB 23/74 (*Dispositionsprogramm*) of 22.06.1976; T 1784/06 (*Classification method/COMPTEL*) of 21.09.2012.

ented, to the extent that the technical effect they generate is confined to the execution of business or administrative practices and other mental processes by technical means.[82] Any effects achieved through automation relating, e.g., to the acceleration of procedures, saving energy and time, etc., are not regarded as technical solutions. Similarly, the presentation of digital data by means of software and electronic devices does not demonstrate in principle any technical character. The fact that such presentations may achieve a more accurate or enjoyable communication of information to the user, does not constitute a solution to any technical problem.[83]

II. The blockchain patentability in the European patent system

51 Given that blockchain is based on a decentralized computer network, any blockchain-related subject matter may fall within the concept of a Computer-Implemented Invention (CIIs) in the light of the EPC. Its patentability is therefore governed by the above rules, being conditional in principle upon consolidating its technical character.[84] To this end, one must prove that the claimed invention in each given case brings about a further technical effect, i.e., a technical solution through technical means.

52 As evident from the preceding analysis, the various blockchain applications automate in principle procedures and practices from the analog environment. This is true not only for smart health, smart voting, smart contracting systems, etc. Also, the cryptocurrency blockchains simulate in essence the financial system. The idea of decentralizing monetary transactions by substituting any auditing authorities for technological safeguards and mutual consent, constitutes a business model. Such applications do not establish the technical character required for being patented.[85]

53 Nevertheless, several technological achievements within the blockchain ecosystem could successfully claim patent protection. These may relate, e.g., to software for preventing malicious attacks and data leaks, securing the accessibility, consistency, and confidentiality of data entries in the network, etc. The EPO in particular has examined applications for encryption technologies[86], data timestamping[87], etc. In the United States, where software patentability requirements resemble the ones in force within the European patent system[88], patents have been granted for, inter alia, blockchain verification technologies[89], systems for transforming traditional domain names into blockchain user addresses[90], etc.

D. Concluding remarks

54 Nowadays, humanity is experiencing the fourth industrial revolution that is arguably distinguished by the convergence of the natural, biological, and digital environment. Many technological developments confirm this observation, such as principally the rise of artificial intelligence, the internet of things and the digitalization of the economy. The latter circumstance relates roughly to the dematerialization of transactions and the emergence of new economic activities taking place exclusively online. The implementation of the contemporary digital economy has been largely facilitated by blockchain, whose im-

82 This is the case, e.g., for order management systems, T 0172/03 of 27.11.2003, (*Order management/RICOH*); supply chain management applications, BGH X ZB 23/74 of 22.06.1976, (*Dispositionsprogramm*); data analysis serving billing and scoring purposes, T 1784/06 of 21.09.2012 *(Classification method/ COMPTEL)*, etc.

83 It is exceptionally conceivable that a technical problem is solved by a presentation of information. Such an effect has been attributed for instance to a method making it easier for the user to search and select images stored on an electronic device by displaying them in low resolution and in a side-by-side order on the screen. T 0643/00 (Searching image data / CANON) of 16.10.2003. Technical character is also stipulated in relation to presentations of information that are intended to guide the user in performing technical tasks or to function as electronic signals of the conditions prevailing within a computer system. T 1741/08 (GUI layout/SAP) of 2.8.2012, para 3.3; T 0336/14 (Presentation of operating instructions/GAMBRO) of 2.9.2015; T 1802/13 (Brain stimulation/CLEVELAND) of 10.11.2016; T 2084/18 (Suspicious behavior/AIC) of 18.6.2021, para 3.2.

84 Hess (n 69) 253.

85 See T 0994/18 (Secure mobile payment/ADVANCED NEW TECHNOLOGIES) of 20.7.2021: The invention consisting in a distributed networked system exchanging encrypted and unencrypted data does not demonstrate any technical character, as long as it relates to a payment system, thus to a business method.

86 T 2327/17 (Authenticated encryption of audio data/BOSCH) of 21.2.2020; T 0556/14 (Masking a private key/CERTICOM) of 28.7.2016.

87 T 1408/09 (Group identifier/SQUARE ENIX) of 7.9.2017.

88 DiNizo (n 70).

89 Shlomit Yanisky-Ravid and Edward Kim, 'Patenting blockchain: Mitigating the patent infringement war' [2019/2020] Albany Law Review 603, 613, footnote 54.

90 US Patent No. 10,721,060 of 21.07.2020, Verisign INC.

plications have incited investments in the field, thus also spotlighting the issue of the IP law relevance for protecting any blockchain-related subject matter.

55 It is not self-evident that blockchain technologies and applications may be subject to IP rights. It has been argued that the code of bitcoin may be regarded as part of the public domain. This assumption, however, does not negate IP protection per se for achievements that develop the primary technological context and/or introduce new practical uses of blockchain. On the contrary, their pertinent eligibility shall be examined in light of the general rules of IP law.

56 What rights exactly could a business active in the blockchain ecosystem protect and on which legal basis, is an issue requiring scrutiny and meticulous justification. The preceding analysis has revealed that concepts and methods being implemented by means of blockchain, like smart contracting, can only be protected as trade secrets. This presupposes however their confidentiality, which for many reasons may be undesirable in business practice.

57 Even though blockchain functionalities do not fit easily in the IP domain, individual technologies supporting the blockchain operation, as well as the database formed within it may be subject to a wide spectrum of IPRs. Even though the conditions for their establishment differ significantly and shall be examined on a case-by-case basis, the concurrent rights may overlap on the same subject matter. In that case they may be cumulatively invoked by the right-holder, unless certain limitations posed, e.g., their duration, or any conflicts of interest, advocate for the one in lieu of the other. For instance, the confidentiality prescribed for trade secret protection and the "sufficient disclosure" requirement of patent law contradict with each other. Also, the identification of the IP right-holder may prove challenging with respect to DLTs, where all nodes contribute to the creation and arrangement of the distributed content. Indeed, this consideration precludes the IP protection of any database formed within public blockchain.

Recommenders you can rely on

A legal and empirical perspective on the transparency and control individuals require to trust news personalisation

by **Max van Drunen, Brahim Zarouali and Natali Helberger***

Abstract: This article explores the role law can play to support trust in the context of news personalisation. The need to ensure trust in the face of technological changes in information dissemination is an important aspect of both recent horizontal legislation such as the Digital Services Act, as well as context-specific specific efforts surrounding for example disinformation. In these legal discussions, however, what trust is, why law should promote it, and what concrete measures are suitable to do so often remain ambiguous. This raises suspicions over whether trust is simply a selling point of traditional legal measures, and if not, what concrete role law can and should play to promote trust. This article focuses on the role control and transparency measures can play to safeguard trust in organisations that use news personalisation. It first analyses how trust should be understood in the context of news personalisation, how media regulation has traditionally supported trust, and how it should continue to do so in the context of news personalisation. It then draws on a conceptual framework of transparency measures in the context of news personalisation to survey how important different transparency and control measures are to the individuals who place trust in organisations that use personalisation. Law's current focus on informing individuals about and empowering them to stop personalisation does not account for the importance of enabling individuals to control how news is personalised.

Keywords: trust; control; transparency; personalisation; DSA

Recommended citation: Max van Drunen, Brahim Zarouali and Natali Helberger, Recommenders you can rely on: A legal and empirical perspective on the transparency and control individuals require to trust news personalisation, 13 (2022) JIPITEC 302 para 1.

A. Introduction

1 Trust is an intuitively appealing concept. It implies individuals can rely on other parties or technologies without having to fully understand or control them. This has always been crucial for organisations that provide news to an audience that does not have the access, expertise, or time to verify this information.[1] It takes on added importance now that information is increasingly distributed with the use of algorithms that are hard even for experts to fully understand. A number of recent policy initiatives, including horizontal regulations such as the Digital Services Act (DSA) and sector-specific policies surrounding disinformation, accordingly, highlight the need to increase trust in the online environment.[2]

* Max van Drunnen and Natali Helberger are at the Institute for Information Law, University of Amsterdam, Brahim Zarouali is at the Institute for Mediastudies, KU Leuven.

1 Matthias Kohring and Jörg Matthes, 'Trust in News Media: Development and Validation of a Multidimensional Scale' (2007) 34 Communication Research 231, 238 <http://crx.sagepub.com/content/34/2/231.abstract>; Yariv Tsfati and Joseph N Cappella, 'Do People Watch What They Do Not Trust?: Exploring the Association between News Media Skepticism and Exposure' (2003) 30 Communication Research 504, 506 <https://doi.org/10.1177/0093650203253371>; Nayla Fawzi and others, 'Concepts, Causes and Consequences of Trust in News Media – a Literature Review and Framework' (2021) 45 Annals of the International Communication Association 154 <https://doi.org/10.1080/23808985.2021.1960181>.

2 High level Group on fake news and and online disinformation, 'A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and

This article focuses on a specific technology that helps individuals to navigate the online media environment, namely news personalisation. Personalisation is used by online platforms to determine what (if any) news is shown to which individual based on their characteristics, and is also one of the most important applications of automated decision-making in the traditional news media.[3]

2 The relationship between regulation and trust is complicated. Simply focusing on the need to increase trust shifts attention away from the need to ensure companies using personalisation algorithms are actually trustworthy, and puts the emphasis on the need for individuals to accept them.[4] Ensuring trustworthiness, for example by regulating the data used in personalisation or by requiring platforms to limit the risks their recommender systems pose, has accordingly been an important part of the legal debate.[5] Ensuring trustworthiness, however, does not automatically lead to trust—individuals must also be able to determine whether they can trust another party. Transparency and control, especially concerning the need for algorithmic explainability, has played a dominant role in this context.[6] Indeed, the provisions in the DSA dedicated to recommender systems focus exclusively on transparency and control.[7]

3 How the regulatory approach to trust relates to the perspective of the individuals who interact with (personalisation) algorithms remains underexplored. Legal discussions instead highlight why trust in technology is important, how technological transformations generally challenge trust, and what role legal measures should play in safeguarding trust.[8] At the same time, existing empirical literature focused on trust in personalisation remains disconnected from normative discussions over why and how regulation should enable trust.[9] In the

Online Disinformation' (European Commission 2018) 11; European Commission, 'White Paper On Artificial Intelligence - A European Approach to Excellence and Trust' (European Commission 2020) COM(2020) 65 final 11 <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf>. European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC 2020 [P9_TA(2022)0269]; Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts 2021 [COM/2021/206 final]. The analysis in this article is based on version of the DSA passed by the European Parliament on 7 September 2022.

3 Charlie Beckett, 'New Powers, New Responsibilities. A Global Survey of Journalism and Artificial Intelligence' (LSE 2019) <https://blogs.lse.ac.uk/polis/2019/11/18/new-powers-new-responsibilities/>.

4 Onora O'Neill, *A Question of Trust* (Cambridge University Press 2002); Damian Tambini, 'Media Freedom, Regulation, and Trust: A Systemic Approach to Information Disorder' (Council of Europe 2020) 18.

5 European Commission, 'White Paper On Artificial Intelligence - A European Approach to Excellence and Trust' (n 2) 2; Neil M Richards and Woodrow Hartzog, 'Taking Trust Seriously in Privacy Law' (2016) 19 Stanford Technology Law Review 431 <https://www-cdn.law.stanford.edu/wp-content/uploads/2017/11/Taking-Trust-Seriously-in-Privacy-Law.pdf>; Balázs Bodó, 'Mediated Trust: A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators' [2020] New Media & Society 1 <https://doi.org/10.1177/1461444820939922> accessed 6 July 2020; Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' 98 <https://osf.io/preprints/socarxiv/38p5f/> accessed 26 July 2021. DSA article 34, AI Act article 5.

6 Maartje ter Hoeve and others, 'Do News Consumers Want Explanations for Personalized News Rankings?' <http://scholarworks.boisestate.edu/fatrec/2017/1/8> accessed 4 November 2020; Alejandro Barredo Arrieta and others, 'Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI' (2020) 58 Information Fusion 82 <http://www.sciencedirect.com/science/article/pii/S1566253519308103> accessed 27 October 2020; Gianclaudio Malgieri, 'Automated Decision-Making in the EU Member States: The Right to Explanation and Other "Suitable Safeguards" in the National Legislations' (2019) 35 Computer Law & Security Review 1 <http://www.sciencedirect.com/science/article/pii/S0267364918303753> accessed 27 October 2020.

7 DSA articles 27, 38. DSA article 3(s) defines recommender systems as (partially) automated systems used by platforms to prioritise information. Recommender systems can be (but are not necessarily) personalised.

8 Sonia Livingstone, 'Tackling the Information Crisis: A Policy Framework for Media System Resilience' (LSE Truth, Trust & Technology Commission 2018) <http://www.lse.ac.uk/media-and-communications/assets/documents/research/T3-Report-Tackling-the-Information-Crisis-v6.pdf> accessed 15 June 2020; Brian O'Neill, 'Trust in the Information Society' (2012) 28 Computer Law & Security Review 551 <http://www.sciencedirect.com/science/article/pii/S0267364912001409> accessed 19 June 2020; Helen Nissenbaum, 'Securing Trust Online: Wisdom or Oxymoron?' (2001) 81 Boston University International Law Review 31.

9 This is at least the case within the specific context of the impact of technology on trust in news, which is the focus of

face of this disconnect between legal and empirical discussions on trust, regulation has to promote trust without taking into account the perspectives of the individuals who actually place their trust in organisations using personalisation to inform them. This limits our understanding of how law can promote trust in a manner that supports both normative objectives as well as individuals' needs.

4 This article explores, from the perspective of individuals, how trust in organisations that use personalisation should be safeguarded through transparency and control measures. It combines an analysis of the ways in which legislation can safeguard trust in the context of personalisation with a survey that explores the perceptions of the individuals who place trust. In particular, we explore how important respondents report different control and transparency measures to be to their trust in organisations that use personalisation to inform them. By focusing on news personalisation the article aims to account for the context-specific challenges which arise when decision-making is automated in a specific field such as the media. The underlying assumption is that trust in technology, and the reasons why regulation should promote it, are shaped by the specific task which technology is relied on to perform.

5 Section B defines trust in the context of news personalisation and analyses the reasons why and ways in which media regulation has been used to promote trust. Sections C and D connect this analysis to the way in which individuals form trust in technology. The sections draw on a conceptual framework of algorithmic transparency in the context of news personalisation to develop and report the results of a survey that gauges what transparency, control, and (self-)regulation individuals find important when they determine whether to trust organisations which use personalisation to inform them.[10] The article concludes by outlining how regulation can enable individuals to trust organisations that use personalisation to inform them.

this article Donghee Shin, 'Why Does Explainability Matter in News Analytic Systems? Proposing Explainable Analytic Journalism' (2021) 22 Journalism Studies 1047 <https://doi.org/10.1080/1461670X.2021.1916984> accessed 8 June 2021; Barredo Arrieta and others (n 6).

10 MZ van Drunen, N Helberger and M Bastian, 'Know Your Algorithm: What Media Organizations Need to Explain to Their Users about News Personalization' (2019) 9 International Data Privacy Law 220 <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz011/5544759> accessed 8 August 2019.

B. The relationship between law, trust, and news personalisation.

I. Trust and its role in law

6 This paper defines trust as the willingness to be vulnerable to the actions of another based on positive expectations about their actions.[11] Although it has been notoriously difficult to reach a consensus about the exact meaning of trust, this definition contains three commonly used elements which are important to understand this article's approach to trust and its relation to law and the media. First, trust is relational: it involves one party (the trustor) placing trust in another (the trustee). The exact nature of this 'another' is quite flexible. Literature on trust in the media traditionally focused on trust in the media as an institution, specific types of media (such as print or broadcasting), or a specific organisation, journalist, or message.[12] Research into the impact of the use of technology, including personalisation, on trust in media is generally incorporated into these existing approaches. Studies have for example explored to what extent individuals are willing to trust specific types of media that heavily rely on personalisation (such as social media), or how the use of personalisation impacts individuals' trust in a the organisation that uses personalisation.[13]

11 Caroline Pauwels and Ike Picone, 'The Tussle with Trust: Trust in the News Media Ecology' (2012) 28 Computer Law & Security Review 542, 543 <http://www.sciencedirect.com/science/article/pii/S0267364912001380> accessed 31 July 2020; Jesper Strömbäck and others, 'News Media Trust and Its Impact on Media Use: Toward a Framework for Future Research' (2020) 44 Annals of the International Communication Association 139, 148 <https://www.tandfonline.com/doi/full/10.1080/23808985.2020.1755338> accessed 15 May 2020; JD Lee and KA See, 'Trust in Automation: Designing for Appropriate Reliance' (2004) 46 Human Factors: The Journal of the Human Factors and Ergonomics Society 50 <http://hfs.sagepub.com/cgi/doi/10.1518/hfes.46.1.50_30392>; Lisa M PytlikZillig and Christopher D Kimbrough, 'Consensus on Conceptualizations and Definitions of Trust: Are We There Yet?', *Interdisciplinary Perspectives on Trust* (Springer International Publishing 2016).

12 Strömbäck and others (n 11).

13 Cristina Monzer and others, 'User Perspectives on the News Personalisation Process: Agency, Trust and Utility as Building Blocks' (2020) 8 Digital Journalism 1142 <https://www.tandfonline.com/doi/full/10.1080/21670811.2020.1773291> accessed 18 June 2020; Nic Newman and others, 'Reuters Institute Digital News Report 2016' (Reuters Institute for the Study of Journalism 2017) <http://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Digital%2520News%2520Report%25202016.pdf>; Robin Steedman, Helen

This article similarly approaches personalisation as another factor that can influence individuals' trust in the organisation that informs them, rather than treating personalisation algorithms themselves as a new object of trust.

7 Second, trust involves vulnerability. Trust only comes into play when something is at stake, and the possibility exists that the trustor's vulnerability will be exploited.[14] Vulnerability also tailors trust definitions to specific contexts. Trust in the media typically centres on its editorial function, that is, whether it can be expected to provide relevant and reliable information.[15] Operationalisations of trust in media capture different aspects of this editorial function, such as accuracy, comprehensiveness, and fairness.[16] Personalisation changes the way in which (some of) these editorial functions are fulfilled. Instead of an editor deciding what information the audience should see, each individual is given their own selection of articles by a personalisation algorithm controlled by editors, engineers, and/or business departments.[17] This change in the way organisations inform their audiences may particularly affect aspects of trust that concern the way the media selects what events to cover, such as trust in the comprehensiveness or diversity of the reporting.[18] Conversely, aspects of trust that are closely related to the way news is produced (such as trust in the accuracy of the reporting) may be unaffected by personalisation, at least when an organisation uses personalisation to recommend articles produced through its traditional editorial processes (as is often the case in the legacy news media).[19] It should also be noted that personalisation's impact on trust is not necessarily negative. For example, individuals may trust algorithmically delivered news more when they perceive algorithms to be more neutral than human editors.[20] As we argue below, the goal of law in this context should not be to promote trust, but to ensure individuals' trust is based on correct assumptions.

8 Vulnerability is also the element that can make trust such a hollow concept for legal literature. The need to prevent vulnerabilities from being exploited is nothing new in law, which already contains a wide range of values and mechanisms to do exactly that. These include specific values such as the right to receive information and privacy, as well as more overarching concepts such as autonomy.[21] Trust does not have any added analytical value in legal discussions if it is simply used to refer to the need to protect these values. The danger of trust being used in this way is exacerbated by the lack of a consensus

Kennedy and Rhianne Jones, 'Complex Ecologies of Trust in Data Practices and Data-Driven Systems' (2020) 23 Information, Communication & Society 817 <https://doi.org/10.1080/1369118X.2020.1748090> accessed 9 April 2020; Jannick Kirk Sørensen, Hilde Van den Bulck and Sokol Kosta, 'Stop Spreading The Data: PSM, Trust, and Third-Party Services' (2020) 10 Journal of Information Policy 474 <https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0474> accessed 15 January 2021; Andreas Graefe and Nina Bohlken, 'Automated Journalism: A Meta-Analysis of Readers' Perceptions of Human-Written in Comparison to Automated News' (2020) 8 Media and Communication 50 <https://www.cogitatiopress.com/mediaandcommunication/article/view/3019> accessed 28 October 2020.

14 Annette Baier, 'Trust and Antitrust' (1986) 96 Ethics 231 <https://www.jstor.org/stable/2381376> accessed 29 October 2020.

15 Strömbäck and others (n 11) 148; Thomas Hanitzsch, Arjen Van Dalen and Nina Steindl, 'Caught in the Nexus: A Comparative and Longitudinal Analysis of Public Trust in the Press' (2018) 23 The International Journal of Press/Politics 3 <http://journals.sagepub.com/doi/10.1177/1940161217740695>; Bernd Blöbaum, *Trust and Communication in a Digitized World* (Bernd Blöbaum ed, Springer 2016) <http://www.springer.com/it/book/9783319280578>.

16 Kohring and Matthes (n 1); Katherine M Grosser, 'Trust in Online Journalism' (2016) 4 Digital Journalism 1036 <http://dx.doi.org/10.1080/21670811.2015.1127174>; Strömbäck and others (n 11) 142.

17 Balázs Bodó, 'Selling News to Audiences – A Qualitative Inquiry into the Emerging Logics of Algorithmic News Personalization in European Quality News Media' (2019) 7 Digital Journalism 1054 <https://doi.org/10.1080/21670811.2019.1624185> accessed 14 January 2020; Neil Thurman and others, 'My Friends, Editors, Algorithms, and I' (2019) 7 Digital Journalism 447, 459 <https://doi.org/10.1080/21670811.2018.1493936> accessed 8 June 2021; Efrat Nechushtai and Seth C Lewis, 'What Kind of News Gatekeepers Do We Want Machines to Be? Filter Bubbles, Fragmentation, and the Normative Dimensions of Algorithmic Recommendations' (2019) 90 Computers in Human Behavior 298.

18 Kohring and Matthes (n 1); Thurman and others (n 17) 459; Monzer and others (n 13).

19 Jessica Kunert and Neil Thurman, 'The Form of Content Personalisation at Mainstream, Transatlantic News Outlets: 2010–2016' (2019) 13 Journalism Practice 759 <https://www.tandfonline.com/doi/full/10.1080/17512786.2019.1567271> accessed 23 November 2020; Bodó (n 17).

20 Thurman and others (n 17); Monzer and others (n 13); Newman and others (n 13) 111.

21 Sarah Eskens, Natali Helberger and Judith Möller, 'Challenged by News Personalisation: Five Perspectives on the Right to Receive Information' (2017) 9 Journal of Media Law 259.

on its precise definition. This ambiguity makes it possible to use trust as a rhetorical tool to refer to the need for technology, individuals, or institutions to act in line with an undetermined set of values every reader can fill in for themselves.

9 Trust is not only about one party being vulnerable to another, however. The third element of the definition above captures that trust is about an individual's willingness to be vulnerable based on a positive expectation about the trustee's actions. Trust thereby allows individuals to deal with the uncertainty on whether their vulnerability will be exploited. It does not require that every vulnerability is removed from an interaction, or that individuals engage in a fully rational cost-benefit analysis.[22] Instead, trust functions as a heuristic that allows individuals to avoid such a complex analysis. Affective approaches to trust emphasise the role of emotion in this process, such as a feeling of security, while cognitive approaches highlight that individuals can also more consciously draw on information in their trust judgments, such as a website's presentation. It is important to note that these two approaches are not mutually exclusive; like many other decisions, trust is likely influenced by both affective and cognitive factors.[23]

10 In here also lies trust's added value for law. Trust captures an essential manner in which individuals determine whether they will interact with those around them—in this case organisations that use personalisation to inform them. Trust facilitates these interactions by giving individuals a fast way to assess whether their vulnerability will be exploited if they rely on another party. Simply reducing the level of vulnerability, for example through rules which require organisations to address risks posed by their personalisation algorithms or limit how organisations can use the data they collect to personalise the news, is not necessarily enough to enable individuals to trust.[24] Individuals must also be able to assess an organisation's trustworthiness or be able to limit their vulnerability if they are not able to trust another party completely. Legal debates that ignore the function that trust plays in daily life, create the risk that individuals are not able to trust other individuals, organisations, or technologies, and are less able to interact with them as a result. This creates an issue when law aims to promote public values that enable individuals to interact with others, for example by receiving information from the media or privately informing themselves about controversial issues. From a legal perspective, trust accordingly functions as a bridge between regulatory efforts, which aim to secure public values (such as privacy or freedom of expression), and the actions which these regulatory efforts intend to enable individuals to take (such as receiving information which shapes their opinions or interacting with others without chilling effects).

II. Why media regulation is used to promote trust

11 At the most basic level, trust is relevant to legal discussions because of its ability to facilitate interactions. Societies are built on cooperative relationships, and individuals interact more easily when they are able to trust each other.[25] However, law's interest in facilitating interactions is of course selective. There is no legal value in promoting individuals' trust in actors who will exploit that trust, nor the kind of trust that leads to interactions that run counter to public values, such as that which is necessary for cartels or criminal organisations to function.[26] In the technological and media context of news personalisation, two goals in particular shape the kind of trust law aims to promote.[27]

12 The necessity of trust in media law discussions is primarily driven by arguments that focus on the media's role in democratic society. The media's ability to play this role is not only based on its ability to collect and distribute information, but also on the audience's willingness to absorb and act on this information. In an information environment where individuals are not able to determine which organisations they can trust, the media cannot fulfil its function as a public watchdog or source of information.[28]

22 Guido Möllering, *Trust: Reason, Routine, Reflexivity* (Elsevier 2006).

23 Möllering (n 22).

24 DSA article 34-35; AI Act article 5, GDPR Chapter IV.

25 Robert D Putnam, 'Bowling Alone: America's Declining Social Capital' in Lane Crothers and Charles Lockhart (eds), *Culture and Politics: A Reader* (Palgrave Macmillan US 2000) <https://doi.org/10.1007/978-1-349-62965-7_12> accessed 29 October 2020.

26 Maria Bigoni and others, 'Trust, Leniency, and Deterrence' (2015) 31 The Journal of Law, Economics, and Organization 663 <https://academic.oup.com/jleo/article/31/4/663/2492478> accessed 29 October 2020.

27 Mark E Warren, 'What Kinds of Trust Does a Democracy Need? Trust from the Perspective of Democratic Theory' in Sonja Zmerli and Tom WG van der Meer (eds), *Handbook on Political Trust* (Elgar 2017) <https://www.elgaronline.com/view/edcoll/9781782545101/9781782545101.00013.xml>; O'Neill, *A Question of Trust* (n 4).

28 Tambini (n 4); Thomas Gibbons, 'Building Trust in Press Regulation: Obstacles and Opportunities' (2013) 5 Journal

Similarly, citizens cannot fulfil their role in the democratic process unless they are able to trust media organisations. Citizens rely on the media to provide them with information which they do not have the time, resources, or access to obtain themselves. Conversely, a lack of trust severely limits the information that citizens can use to take part in the political process. In other words, the media's ability to fulfil its role in society presumes that citizens are able to trust the media.[29]

13 Economic goals feature particularly prominently in the broader legal discussion on the need for trust in Artificial Intelligence. In the words of the Commission, "lack of trust is a main factor holding back a broader uptake of AI."[30] A lack of trust is thereby framed as an economic inefficiency preventing individuals from using AI that is able to provide valuable services. Trust's role as a precondition for acceptance has a long history. Some of the earliest research into trust in the media focused on the impact of perceived trustworthiness on the acceptance of a message.[31] Literature on trust in personalisation systems often continues to take a rather short-term approach to promoting trust, sometimes simply operationalising trust as the acceptance of the system or its recommendations.[32] AI policy emphasises the need for a more long-term acceptance of AI, for which the technology needs to earn trust and be consistently trustworthy.[33]

14 Democratic and economic perspectives on trust in the media can complement one another. Both focus on ensuring that a media organisation earns the trust of its audience by doing what it is relied on to do. Economic perspectives focus on the financial value of this interaction. Although this aspect is not the focal point of media law discussions, the need to create a media system in which quality journalism is financially sustainable and disinformation is not, is increasingly emphasised.[34] Trust has a part to play in this context, given the relationship between trust and media use—as well as media scepticism and use of non-mainstream sources.[35] The broader literature on media transparency accordingly highlights the importance of trust for the financial health of the media.[36]

15 Regulation's ability to secure trust in the context of news personalisation is limited precisely because of the centrality of trust to the ability of media organisations to fulfil their democratic role. Regulations that require media organisations to act in a trustworthy way would allow for political interference in the manner in which the media and citizens interact. Wijermars, for example, has analysed how Russian legislation passed to preserve the "truthfulness and trustworthiness of the information that our citizens receive" enables the state to control the output of news recommenders by limiting the kinds of sources they can recommend.[37]

of Media Law 202, 210 <https://www.tandfonline.com/doi/full/10.5235/17577632.5.2.202> accessed 30 May 2020; Benjamin Toff and others, 'What We Think We Know and What We Want to Know: Perspectives on Trust in News in a Changing World' (Reuters Institute for the Study of Journalism 2020) 5.

29 CoE, 'Recommendation of the Committee of Ministers to Member States on a New Notion of Media' (Council of Europe 2011) CM/Rec(2011)7 para 53 <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2c0>.

30 European Commission, 'White Paper On Artificial Intelligence - A European Approach to Excellence and Trust' (n 2) 9.

31 Carl I Hovland and Walter Weiss, 'The Influence of Source Credibility on Communication Effectiveness*' (1951) 15 Public Opinion Quarterly 635 <https://doi.org/10.1086/266350> accessed 16 June 2021.

32 Jonathan L Herlocker, Joseph A Konstan and John Riedl, 'Explaining Collaborative Filtering Recommendations', *Proceedings of the 2000 ACM conference on Computer supported cooperative work* (ACM 2000); Ingrid Nunes and Dietmar Jannach, 'A Systematic Review and Taxonomy of Explanations in Decision Support and Recommender Systems' (2017) 27 User Modeling and User-Adapted Interaction 393.

33 High-Level Expert Group on Artificial Intelligence, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) 4 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419>; European Commission, 'White Paper On Artificial Intelligence - A European Approach to Excellence and Trust' (n 2) 1.

34 European Commission, 'Tackling Online Disinformation: A European Approach' (European Commission 2018) COM(2018) 236 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236> accessed 20 February 2020; CoE, 'Declaration by the Committee of Ministers on the Financial Sustainability of Quality Journalism in the Digital Age' (Council of Europe 2019) Decl(13/02/2019)2 <https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168092dd4d> accessed 9 June 2019.

35 Strömbäck and others (n 11) 146.

36 B Vanacker and G Belmas, 'Trust and the Economics of News' (2009) 5 Journal of Mass Media Ethics 110.

37 Mariëlle Wijermars, 'Russia's Law "On News Aggregators": Control the News Feed, Control the News?' [2021] Journalism 1, 2944 <https://journals.sagepub.com/doi/

EU media regulation has therefore traditionally established only limited minimum norms regarding editorial responsibility, concerning among others an obligation to protect children from harmful content and a prohibition on subliminal advertising.[38] As the next section explores further, regulation aims to create the conditions under which individuals can form trust in the media instead, for example through transparency norms that allow individuals themselves to evaluate the trustworthiness of media organisations or media content.

III. How media regulation promotes trust through transparency and control options

16 Transparency and control can make it easier for individuals to determine whether they will trust another party by allowing them to be less uncertain and vulnerable. At least from a conceptual perspective, this could prevent individuals from placing as much trust in others as they otherwise would. After all, transparency and control reduce the level of uncertainty and vulnerability that make trust possible. A similar argument is sometimes made with regard to the general relationship between law and trust. By requiring individuals and companies to (for example) not violate individuals' privacy, law arguably takes away their ability to demonstrate their trustworthiness voluntarily.[39]

17 The concern that legal measures displace trust inherently only applies when individuals would have placed trust even without e.g. transparency or control. However, as the above argued, regulation is used to enable individuals to trust precisely in situations where they would otherwise feel too uncertain or too vulnerable to do so. That is, media regulation lowers the bar for trust, making it easier for individuals to place trust in a wider variety of actors. Although this may limit the trust individuals would have placed in trustworthy actors even without legal measures being in place, this limitation must be seen in the context of the wider group of actors. Furthermore, the empirical evidence (at least in the context of the media) indicates transparency and generally does have a positive (albeit small) impact on trust.[40] There are a wide variety of potential reasons for this, including the possibility that individuals see transparency as a signal that a company is trustworthy or are unaware of the fact that a company is only transparent because it is legally required to do so.[41]

18 The first way in which media regulation promotes trust is by aligning expectations. By forcing parties to make their assumptions explicit and clarify how they fulfil their roles, media regulation can prevent unintended trust violations.[42] In the context of the media, this way of promoting trust is strongly intertwined with the right to receive information, and more specifically its focus on enabling individuals to seek out a wide range of information. Regulation has traditionally facilitated the exercise of this right by ensuring the availability of information about the media organisation itself, thereby allowing individuals to evaluate how a media organisation fits into their media diet.[43] Article 5

abs/10.1177/1464884921990917> accessed 15 February 2021.

38 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (AVMSD 2018) 2018 articles 6a, 9(1)(b), 28b. Public Service Media have a special (and for certain public service media organisations such as the BBC, legal) obligation to act as a trusted source of information. Ofcom, 'Operating Licence for the BBC's UK Public Services' (2020) s 1.24.3 <https://www.ofcom.org.uk/__data/assets/pdf_file/0017/107072/bbc-operating-licence.pdf>.

39 See on these arguments e.g. Nissenbaum (n 8) 121.

40 Caroline Fisher and others, 'Improving Trust in News: Audience Solutions' (2020) 0 Journalism Practice 1, 12, 14 <https://doi.org/10.1080/17512786.2020.1787859> accessed 8 July 2020; Donghee Shin, 'User Perceptions of Algorithmic Decisions in the Personalized AI System:Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability' (2020) 0 Journal of Broadcasting & Electronic Media 1 <https://doi.org/10.1080/08838151.2020.1843357> accessed 7 January 2021; Monzer and others (n 13).

41 See e.g. Fisher and others (n 40) 7; Toff and others (n 28) 16; Bernadette Uth, Laura Badura and Bernd Blöbaum, 'Perceptions of Trustworthiness and Risk: How Transparency Can Influence Trust in Journalism' in Bernd Blöbaum (ed), *Trust and Communication: Findings and Implications of Trust Research* (Springer International Publishing 2021) <https://doi.org/10.1007/978-3-030-72945-5_3> accessed 9 July 2021.

42 CoE, 'Declaration on the Financial Sustainability of Quality Journalism' (n 34) 5; Daryl Koehn, 'Should We Trust in Trust?' (1996) 34 American Business Law Journal 183 <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-1714.1996.tb00695.x> accessed 30 June 2020.

43 Eskens, Helberger and Möller (n 21); CoE, 'Recommendation of the Committee of Ministers to Member States on Media Pluralism and Transparency of Media Ownership' (Council of Europe 2018) CM/Rec(2018)1 <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e13>.

of the EU's Audiovisual Media Services Directive (AVMSD), for example, intends to make it easier for individuals to determine who is responsible for the content of the media service that shapes their opinion.[44] Personalisation can reduce the usefulness of this information, given that a media organisation shows each individual a different collection of news items. At the same time, personalisation creates the opportunity to better suit the expectations of the individual who places trust in the media. Not only is it possible to show each individual which (types of) articles have been shown to them specifically, personalisation also allows individuals to control the news they receive more directly and ensure that personalisation functions in a way that better aligns the goals of the media organisation with their own. Article 27 DSA, which regulates the recommender systems used by online platforms, aims to engage with these factors by better enabling individuals to understand and influence the parameters of the recommender systems that determine how information is prioritised for them.[45]

19 Secondly, transparency can enable and channel scepticism. By providing additional information and contextual cues, media regulation enables news consumers to assess for themselves whether they can trust reporting.[46] Although this can involve explanations of individual editorial decisions, media regulation has generally focused on higher level explanations. Concretely, it involves information on the organisation providing the information, and whether editorial content is actually an advertisement.[47] In doing so, regulation enables trust judgments regarding specific content or sources. Yet, key from a trust-perspective is that individuals are thus not expected to discount or doublecheck everything which they read, but rather that they can make broader trust judgments and rely on reporting until explanations trigger their scepticism.[48]

20 Scepticism is at first glance incompatible with trust. However, media regulation prevents individuals from having to adopt generalised scepticism to the media as a whole by enabling individuals to distinguish between the trustworthiness of different pieces of media content.[49] For example, the distinction between commercial and editorial content allows individuals to accept that while a media organisation may be influenced by external commercial pressures, these pressures are limited to the types of content labelled as advertising.[50] Distinctions in self-regulatory ethics codes, such as the duty to clearly separate news and opinion, fulfil a similar function. Without such distinctions, individuals would be forced to adopt a more generalised scepticism to all reporting by a media organisation. Explanations of the different forces behind different content channel this scepticism, and thereby safeguard trust in the media organisation as a whole.[51]

21 Finally, media regulation can enable trust repair. As citizens increasingly question journalists' authority, it is not enough to put out responsibly produced content and assume that it will earn the trust of readers. It is also necessary to address questions as to journalistic authority by highlighting the accountability mechanisms with which the media organisation tries to prevent, detect, disclose, and address (perceived) violations of individuals' trust.[52] At the most basic level, this includes transparency on the norms to which media organisations consider themselves held, and acknowledgments when their reporting fails to live up to such norms. More recent work also emphasises the importance of providing the audience with a way to act on these explanations by providing criticism and feedback.[53] Through these accountability processes, a more responsible media system can be incentivised.[54] Going a step further, individuals could also be given the option to (temporarily) assume more control over the manner

44 AVMSD 2018 recital 16, article 5.

45 European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (n 2) articles 25, 29, recital 62. Very large online platforms are defined as online platforms with 45 million or more EU users.

46 O'Neill, *A Question of Trust* (n 4).

47 Onora O'Neill, 'Trust and Accountability in a Digital Age' (2020) 95 Philosophy 3 <https://www.cambridge.org/core/journals/philosophy/article/trust-and-accountability-in-a-digital-age/ADBDD9EEF4426590D5A60AF87611240D> accessed 31 October 2019.

48 Fisher and others (n 40) 7.

49 Lara Fielden, *Regulating for Trust in Journalism: Standards Regulation in the Age of Blended Media* (University of Oxford, Reuters Institute for the Study of Journalism 2011) 117.

50 L Hitchens, 'Commercial Content and Its Relationship to Media Content: Commodification and Trust' in Monroe E Price and Libby Verhulst, Stefaan G. Morgan (eds), *Routledge handbook of media law* (Routledge 2013) 102 <https://www.routledge.com/Routledge-Handbook-of-Media-Law/Price-Verhulst-Morgan/p/book/9780415683166>.

51 Warren (n 27).

52 O'Neill, 'Trust and Accountability in a Digital Age' (n 47).

53 Monzer and others (n 13).

54 High level Group on fake news and and online disinformation (n 2) 25.

in which a media organisation recommends news to them to create a space in which trust can be repaired. In this way, the media can limit the negative impact of (perceived) trust violations by giving the audience the opportunity to voice their scepticism and showing how these concerns are taken into account.[55]

22 News personalization challenges the way in which existing legal transparency and control measures can enable trust by changing the way news is delivered. As argued above, the increasing use and importance of news personalization impact trust by changing the way in which organizations select what news their audience should be informed about. However, transparency or empowerment measures tailored to the traditional media system do not necessarily enable individuals to assess the trustworthiness of the algorithmic tools that increasingly determine how they are informed. In this context, factors such as the way a personalization algorithm impacts an individuals' news diet, the (editorial) values it is designed to promote, or the type of content it can recommend are relevant as well. These factors generally fall outside the scope of traditional transparency and empowerment measures, however, as they focus on the content that is published (for example by requiring that any commercial content is clearly identified, and a wide variety of content is available) or publishers themselves (for example by requiring the disclosure of the identity of the media organization or commercial party influencing content, and ensuring the media system contains a variety of sources of content with which individuals can engage).[56] As personalization algorithms increasingly mediate how individuals are exposed to content or sources, it becomes more important to adapt and expand on traditional transparency and empowerment measures in media regulation to allow individuals to assess the trustworthiness of the way information is algorithmically selected for them.

IV. Surveying individuals' perspective on trust and law

23 Increasingly, policy efforts, such as the DSA as well as the various EU disinformation codes, begin to reinvent the role that law can play to safeguard trust in the light of the technological changes in the online media environment. What remains unclear, however, is to what extent regulatory initiatives aiming to promote trust in the media in the context of technological change are in line with the way in which individuals form trust. This aspect is crucial because it is ultimately the individuals themselves who determine whether they do or do not trust. If regulation is expected to actually promote the trust necessary for individuals and the media to fulfil their role in democratic society, it needs to take into account the perspective of the individuals who place this trust in the media.

24 To that end, Sections C and D report on the methodology and results of the survey exploring the transparency and control items that individuals find significant when it comes to their trust in organisations using personalisation to inform them. The items (see 2) were developed from a conceptual framework of algorithmic transparency obligations in the context of news personalisation. The framework combines algorithmic transparency and media transparency literature to distinguish between disclosures concerning the organisation that operates the personalisation algorithm, the sources shown, the data used, the algorithm itself, and the output.[57] For the purposes of this survey, the framework was expanded with a number of control options serving as counterparts to the transparency items,[58] as well as recent regulatory measures put forward in the context of trust in platform and disinformation discussions.[59] The first set of research questions explores how important these transparency and control measures are to individuals when it comes to their trust in organisations which use personalisation to inform them.

RQ1a: how important are legal transparency measures to individuals' trust in organisations that use news personalisation to inform them?

RQ1b: how important are legal control measures to individuals' trust in organisations that use news personalisation to inform them?

55 Gibbons (n 28) 212; European Commission, 'White Paper On Artificial Intelligence - A European Approach to Excellence and Trust' (n 2) 23.

56 van Drunen, Helberger and Bastian (n 10); Monzer and others (n 13); CoE, 'Recommendation on Pluralism' (n 43) para 2.2, 2.7, 4.5; AVMSD 2018 recitals 15-16, article 5.

57 van Drunen, Helberger and Bastian (n 10).

58 This is sometimes referred to as interactive transparency in media transparency discussions Michael Karlsson, 'Rituals of Transparency' (2010) 11 Journalism Studies 535 <http://www.tandfonline.com/doi/abs/10.1080/14616701003638400>; David Domingo and Heikki Heikkilä, 'Media Accountability Practices in Online News Media', *The Handbook of Global Online Journalism* (Wiley-Blackwell 2012) <http://doi.wiley.com/10.1002/9781118313978.ch15>.

59 High-Level Expert Group on Artificial Intelligence (n 33); European Commission, 'Tackling Online Disinformation: A European Approach' (n 34); CoE, 'Declaration on the Financial Sustainability of Quality Journalism' (n 34).

RQ2: is there a difference between the importance of transparency and control measures to individuals' trust?

25 News personalisation has the potential to impact individuals' trust in the organisations that use it because it changes the way in which the audience is informed.[60] This would mean that the use of personalisation further limits the media's ability to fulfil its role in society by reducing the number of individuals with high trust in the media. It is therefore important to know how news personalisation can be explained to or made controllable for individuals who already trust the media. At the same time, considerable policy and research attention is devoted to the need to prevent a decrease in trust. Research into analogue media indicates transparency is unlikely to restore the trust of individuals who have already lost trust in the media, given that the transparency is provided by an untrustworthy party.[61] Conversely, control options may not face the same challenge because they allow an individual to limit the media's influence over their news diet.[62] In order to explore to what extent the tested transparency and control measures are suitable to enable individuals with high and low trust in the media respectively to trust organisations that personalise their news, the research asks the following questions:

RQ3a: is the extent to which individuals find transparency measures important related to their existing trust in the media?

RQ3b: is the extent to which individuals find control measures important related to their existing trust in the media?

26 Similarly, the importance attached to transparency of and control over personalisation algorithms may depend on an individual's existing level of algorithmic literacy. Individuals first have to know what personalisation is and how it might affect them to gain an interest in better understanding or controlling a personalisation algorithm.[63] Knowing what information and control measures (if any) are important to individuals with high algorithmic literacy may indicate which types of measures will become more important as public awareness of the personalisation algorithms used by platforms grows.[64] This article thus aims to explore the following questions:

RQ4a: is the extent to which individuals find transparency measures important related to their algorithmic literacy?

RQ4b: is the extent to which individuals find control measures important related to their algorithmic literacy?

27 Finally, law's ability to safeguard trust entails more than empowering individuals to protect themselves through transparency and control measures. An important way in which law protects trust is by prohibiting certain forms of behaviour, effectively reducing individuals' level of vulnerability. The AI Act, which prohibits the use of certain AI systems deemed to be high risk, is an important recent example of this approach. Along similar lines, (self)-regulation of the media can limit unacceptable practices and provide individuals with further protection and certainty.[65] In other words, there can also be a role for further-reaching measures, either in the form of legal obligations or self-regulation to protect the legitimate interests and rights of users and society.

RQ5a: how important are measures in (self-) regulation to individuals' trust in organisations that use news personalisation to inform them?

RQ5b: is there a relationship between the importance of self-regulation and the importance of transparency to individuals' trust in organisations that use news personalisation to inform them?

RQ5c: is there a relationship between the importance of self-regulation and the importance of con-

60 Monzer and others (n 13).

61 Michael Karlsson, 'Dispersing the Opacity of Transparency in Journalism on the Appeal of Different Forms of Transparency to the General Public' (2020) 21 Journalism Studies 1795 <https://doi.org/10.1080/1461670X.2020.1790028> accessed 26 July 2021.

62 Monzer and others (n 13) 1153.

63 Motahhare Eslami and others, 'I Always Assumed That I Wasn't Really That Close to [Her]', *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15* (ACM Press 2015) <http://dl.acm.org/citation.cfm?doid=2702123.2702556>; Emilee Rader, Kelley Cotter and Janghee Cho, 'Explanations as Mechanisms for Supporting Algorithmic Transparency', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (ACM Press 2018) <http://dl.acm.org/citation.cfm?doid=3173574.3173677> accessed 4 November 2020.

64 Rader, Cotter and Cho (n 63); Brahim Zarouali, Sophie C Boerman and Claes H de Vreese, 'Is This Recommended by an Algorithm? The Development and Validation of the Algorithmic Media Content Awareness Scale (AMCA-Scale)' (2021) 62 Telematics and Informatics <https://www.sciencedirect.com/science/article/pii/S0736585321000460> accessed 7 July 2021.

65 CoE, 'New Notion of Media' (n 29) para. 53; Gibbons (n 28) 216.

trol to individuals' trust in organisations that use news personalisation to inform them?

C. Methodology

28 The survey (Annex A) was distributed among a representative sample of the Dutch population. The total sample size was $N = 1009$. Representativeness was achieved based on age, gender, education, and region. The data collection was carried out by the research company IPSOS. The overall response rate was 27 per cent. The data collection took place between 15 and 20 April 2021 (5 days). The mean age of the sample was 48.17 (SD = 16.68 years), ranging from 18 to 89 years old. Half of the sample consisted of women (50 per cent). All respondents who successfully completed the survey received an incentive from the research company. A demographic overview of the sample is presented in Table 1.

D. Results

29 To answer RQ1a and RQ1b, we asked respondents to indicate how important a number of concrete transparency and control measures were to their trust in media organisations that use news personalisation to inform them. Answer options ranged from 1 (*not important at all*) to 7 (*very important*). The measures and associated mean values and standard deviations can be found in Table 2. In addition, we also provide the Cronbach's alphas as estimates of internal consistency (which are all very high). It can be concluded that all transparency and control measures are perceived to be important by the respondents. The mean scores are relatively high (all between 5-6, with 7 being the maximum score). This highlights that people find all the transparency and control measures in the context of the media organisation, the data, the algorithm, and the output to be relatively important.

	Percentage (%)	*Frequency (N)*
Age categories (M_{age} = 48.17, SD_{age} = 16.68)		
18-34 years	26.76	270
35-54 years	32.80	331
55+ years	40.44	408
Gender		
Women	50.45	509
Men	49.55	500
Education		
Low	16.65	168
Moderate	39.94	403
High	43.41	438
Region		
North	8.52	86
East	22.60	228
South	25.77	260
West	29.83	301
Three large cities (Amsterdam, Rotterdam & The Hague)	13.28	13.28

Table 1. Demographic characteristics of the sample.

30 To provide an answer to RQ2, we calculated the average score of all the transparency and control items from Table 2. The average mean score of all the transparency items together is M = 5.47, SD = 1.09; the average mean score for control was 5.54, SD = 1.07. A t-test shows that there is a significant difference between these two values, meaning that people find control to be slightly more important than transparency: t(1008) = -4.46, p <.001. In addition, a Pearson correlation test shows that transparency and control are strongly correlated to each other (r =.90, p <.001). This means that the importance of transparency goes hand in hand with the importance of control measures.

31 To answer RQ3a and RQ3b, we conducted correlation analyses between individuals' existing media trust and perceived importance of transparency and control measures. Results indicate a weak positive correlation between media trust and control (r = 0.10, p < .01). The exact same pattern for transparency: a weak positive relationship with media trust (r = .12, p < .001). These findings mean that people who have a higher media trust, also find control and transparency to be slightly more important.

32 To answer RQ4a and RQ4b, we ran correlation tests between people's algorithmic literacy and perceived importance of transparency and control in news personalisation. Algorithmic literacy was measured based on items derived from a study of Zarouali, Boerman, and de Vreese.[66] The correlation between algorithmic literacy and transparency was r = .39 (p < .001); between algorithmic literacy and transparency r = .35 (p < .001). These correlation coefficients indicate a moderate positive relationship. This means that people with a higher algorithmic literacy tend to perceive transparency and control measures as more important as well.

33 To answer RQ5a, we asked respondents to indicate the importance of (self-)regulation at each of the five stages of the model. The average mean score of the importance of (self-)regulation to individuals' trust is M = 5.33. Finally, in answering RQ5b and RQ5c, we again ran correlation tests. We found that there is a strong positive relationship between the importance of (self)regulation and the importance of control measures (r = .78, p < .001); the exact same strong positive corelation was also found between regulation and transparency (r = .78, p < .001). This indicates that the perceived importance of (self-) regulation is very much associated with people's perceived importance of transparency and control measures in news personalisation.

66 Zarouali, Boerman and de Vreese (n 64).

Items	Mean	SD
The media organisation		
Transparency		
It is clear to what extent journalists and editors determine the way news is personalised.	5.36	1.41
It is clear whether commercial parties such as advertisers influence the way news is personalised.	5.48	1.50
It is clear to what extent the media organisation uses algorithms from other companies to personalise the news.	5.38	1.42
Control		
The ability to choose between the personalisation algorithms of different companies on a website.	5.25	1.46
The source of the articles		
Transparency		
It is clear what the identity of the source of a recommended article is.	5.62	1.37
It is clear whether the source of a recommended article adheres to journalistic norms established by traditional media companies.	5.53	1.35
It is clear whether a recommended article comes from a government institution.	5.60	1.38
It is clear whether a recommended article is produced automatically or written by a human.	5.53	1.39
Control		
The ability to choose from which sources you will receive news.	5.64	1.33
The ability to choose to only receive news from sources that adhere to journalistic norms established by traditional media companies.	5.56	1.37
The data		
Transparency		
It is clear what data is collected about you to personalize news.	5.75	1.37
It is clear for which other goals the collected data is used.	5.77	1.36
It is clear whether the collected data is shared with other parties.	5.80	1.37

Control		
The ability to choose what data about you is used to personalise the news.	5.85	1.34
The ability to delete the data used to personalise news for you.	5.87	1.36
The algorithm		
Transparency		
It is clear why a specific article is recommended.	5.31	1.40
It is clear which factors have the most impact on the way news is personalised.	5.27	1.38
It is clear what goal the media organisation tries to achieve by personalising the news.	5.35	1.37
Control		
The ability to turn news personalisation off.	5.94	1.32
The ability to indicate that a specific type of news article should be recommended more or less.	5.39	1.41
The ability to choose which factors have the most influence on the way news is personalised.	5.36	1.38
The ability to choose which goals the personalisation algorithm aims to achieve.	5.39	1.36
The output		
Transparency		
It is clear which parts of the site are personalised.	5.42	1.39
It is clear what type of news (for example, entertainment, politics, sport) has been recommended to you more often.	5.23	1.41
It is clear which important articles have not been recommended to you.	5.24	1.43
Control		
The ability to choose to always see important articles.	5.68	1.40
The ability to see which sources or articles have not been recommended.	5.37	1.41
The ability to give feedback on the way news personalization works.	5.22	1.52
Overall Cronbach's alpha		
Transparency: .96		
Control: .93		

Table 2: overview of all transparency and control items with their respective mean values.

E. Discussion

34 Trust is a psychological process that law aims to enable for normative purposes. This article has argued that doing so successfully in the context of news personalisation first requires us to determine what kind of trust law should promote in this context. Section B has therefore argued that aligning expectations, facilitating scepticism, and enabling trust repair promotes the kind of trust is necessary for individuals and the organisations informing them to fulfil their role in democratic society. However, knowing why and how media regulation should promote trust is not sufficient. To actually promote trust, media regulation must also account for the perspective of the individuals that decide whether an organisation that uses personalisation is trustworthy. Sections C and D therefore report the results of a survey, developed from a conceptual framework of algorithmic transparency obligations in the context of news personalisation; it explores different transparency and control items that individuals find significant when it comes to their trust in organisations using personalisation to inform them.

35 This research reveals that individuals find the transparency and control items that are suitable for the kind of trust media regulation aims to promote important when they decide whether to trust an organisation using news personalisation to inform them. Moreover, there is only a weak relationship between respondents' existing trust in the media, and the importance of transparency and control measures to their trust. Though transparency about and control over personalisation are slightly more important to individuals who already trust the media, individuals with lower trust in the media also find these measures important to be able to trust organisations using personalisation to inform them.[67] Enabling individuals to trust organisations that use personalisation to inform them is important to both individuals who already trust the media as well as those with low trust in the media.

36 The differences between the value individuals attach to the various transparency and control items that we tested are relatively small. EU legislation that aims to improve the transparency of personalisation (and automated decision-making more generally) has traditionally focused on explaining the algorithms themselves. In particular, the General Data Protection Regulation (GDPR) requires that the logic and envisaged consequences of automated decision-making are communicated to individuals, while Article 27 DSA requires online platforms to inform users about the main parameters of their recommender systems. Our results indicate that information about the functioning of personalisation algorithms is only a small (and slightly less relevant) portion of the information that is important to individuals' trust. Also information beyond the functioning of personalisation algorithms, including transparency about the data or the source of the content used in personalisation, is important to individuals' trust. The former, information about data processing, is regulated extensively in data protection law. The latter, information about the source of the content individuals see, has traditionally been an important aspect of media regulation.[68] Measures adapting such information obligations to the online media environment are beginning to emerge in a fragmented fashion in self-regulation as well as EU and national law. Among others, the proposed AI Act and German Medienstaatsvertrag require that automatically generated content is labelled as such.[69] In addition, self-regulation and soft law increasingly include transparency measures intended to inform individuals that content was produced by a government institution or by a media organisation that adheres to journalistic norms. The results indicate such transparency about the recommended content is also important to enabling individuals to judge the trustworthiness of the organisation that uses personalisation algorithms to recommend content to them, such as online platforms. This finding is also relevant to legacy media organisations, which often only recommend articles produced through their own editorial processes and exercise more traditional editorial control over the design of personalisation algorithms.[70]

67 Fisher and others (n 40) 12.

68 AVMSD 2018 recital 16, article 5; 'Recommendation of the Committee of Ministers to Member States on Media Pluralism and Transparency of Media Ownership' (2018) CM/Rec(2018)1 <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680790e13> accessed 10 June 2019; O'Neill, 'Trust and Accountability in a Digital Age' (n 47) 15.

69 Medienstaatsvertrag 2020 article 18(3); Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts (n 2) article 52(3); European Commission, 'EU Code of Practice on Disinformation' (2018) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454> article I, II.D.

70 Bodó (n 17); Mariella Bastian, Natali Helberger and Mykola Makhortykh, 'Safeguarding the Journalistic DNA: Attitudes towards the Role of Professional Values in Algorithmic News Recommender Designs' (2021) 9 Digital Journalism 1 <https://doi.org/10.1080/21670811.2021.1912622> accessed 6 August 2021.

37 However, individuals are not merely interested in knowing more; this research demonstrates that the ability to exercise control over the way in which news is personalised, is strongly correlated with and even slightly more important to individuals' trust than transparency. In particular, half of all respondents indicate that the ability to stop personalisation is very important to their trust in organisations using the technology to inform them.

38 On an abstract level, individuals' demand for control is in line with the goals that law aims to achieve by establishing algorithmic transparency obligations. The goal is not simply to provide more information to individuals, but also to enable individuals to choose what news to read, to hold organisations accountable, or to trust the use of news personalisation.[71] Control options let individuals act on the information with which they are provided more directly. At the same time, research shows that individuals gain a better understanding of the manner in which a system functions by seeing how their control results in different outcomes.[72] Our research similarly indicated a strong relationship between the importance individuals attach to transparency and control. In short, control and transparency are intertwined.

39 In practice, legislation focuses on transparency, and offers individuals few options to act on the information made available to them. On the positive side, the control option most important to individuals' trust, the ability to stop personalisation, is also the central focus of EU regulation that addresses individuals' control over personalisation algorithms. Article 38 DSA now requires very large online platforms to give users at least one option for their recommender system that is not based on profiling. Article 27 DSA moreover requires that users can choose between different options for recommender systems in the section of the platforms' interface where recommendations are provided.[73] Article 38 DSA is complemented by Article 22 GDPR, which regulates automated decision-making and profiling in general and similarly focuses on enabling individuals to reject personalisation by creating a right not to be subject to decisions solely based on automated processing.[74] However, individuals' ability to use this right to stop personalisation is subject to multiple exemptions relating to for example whether news personalisation is based on consent or a contract, or involves decisions with legal or similarly significant effect.[75] Moreover, the GDPR does not regulate how the option to stop news personalisation should be offered to users, only requiring organisations to facilitate the exercise of the right provided under Article 22.[76] Conversely for very large online platforms, the DSA makes it easier to exercise the control the respondents in our sample found to be most important for trusting organisations that use news personalisation, namely to stop personalisation.

40 The results also indicate that it is important to look beyond simply stopping personalisation. Though the ability to stop personalisation was the control option our respondents indicated was most important to their trust, it was by no means the only control option they valued. However, the DSA does not require platforms to offer users any other option than to stop personalised recommendations—it only requires that any options platforms offer voluntarily are easily accessible.[77] The GDPR offers individuals few other options to exercise control over personalisation, most of which are focused on

71 van Drunen, Helberger and Bastian (n 10).

72 S Shyam Sundar, 'Rise of Machine Agency: A Framework for Studying the Psychology of Human–AI Interaction (HAII)' Journal of Computer-Mediated Communication 82 <https://academic.oup.com/jcmc/advance-article/doi/10.1093/jcmc/zmz026/5700811> accessed 22 January 2020.

73 As it is an option to influence the parameters. See also DSA recital 94.

74 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 1995 article 15.

75 Sarah Eskens, 'A Right to Reset Your User Profile and More: GDPR-Rights for Personalized News Consumers' (2019) 9 International Data Privacy Law 153 <https://academic.oup.com/idpl/advance-article/doi/10.1093/idpl/ipz007/5525264> accessed 1 July 2019; Natali Helberger and others, 'Regulation of News Recommenders in the Digital Services Act: Empowering David against the Very Large Online Goliath' [2021] Internet Policy Review <https://policyreview.info/articles/news/regulation-news-recommenders-digital-services-act-empowering-david-against-very-large> accessed 21 July 2021.

76 Article 12(2) GDPR; Mariella Bastian and others, 'Explanations of News Personalisation across Countries and Media Types' (2020) 9 Internet Policy Review 1 <https://www.econstor.eu/handle/10419/225645> accessed 7 October 2021; Luciana Monteiro Krebs and others, 'Tell Me What You Know: GDPR Implications on Designing Transparency and Accountability for News Recommender Systems', *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (ACM 2019) <http://doi.acm.org/10.1145/3290607.3312808> accessed 21 May 2019.

77 Article 27 DSA.

removing the data used for personalisation.[78] As a result of regulation's narrow focus on the ability to stop personalisation, users are faced with a take-it-or-leave-it choice: either they have to trust personalisation with the parameters and goals platforms choose, or they reject personalisation altogether in favour of a non-personalised offer. This option is made all the less attractive by the fact the DSA does not impose any requirements on the non-personalised option it requires very large online platforms to offer.

41 According to our results, EU law's current focus on enabling individuals to stop personalisation misses the importance individuals attach to control options that allow them to influence *how*, rather than only *if* their news is personalised. Moreover, it disregards the central role personalisation algorithms fulfil in the online media system.[79] By prioritising information for individuals based on their characteristics, personalisation algorithms make the overwhelming amount of content that is available online accessible. They can do so not only by providing individuals those news items they are most likely to engage with, but also by providing news that allows individuals to more deeply inform themselves about specific topics they are interested in or offer them diverse perspectives they do not normally encounter.[80] The importance of personalisation algorithms for navigating the online media environment, as well as the different ways in which they can do so in support of users' needs and public values, is neglected by EU law's narrow focus on stopping personalisation. Instead, regulation that empowers users could enable them to ensure personalisation algorithms do what they trust them to do by giving them more control over how their news is personalised. The results surfaced a number of control options that individuals perceive to be important to their trust, such as the option to always see important articles, determine the sources from which news is received, choose what data is used to personalise their news, or choose which goals the personalisation algorithm aims to achieve.[81]

42 Neither control nor transparency are sufficient. The existence of (self-)regulatory norms regarding the way in which personalisation functions, is also critical for trust. The need for such regulation is an essential part of the criticism against individual-oriented transparency and control measures. A focus on empowering individuals can shift policy attention away from the responsibilities that organisations using personalisation bear themselves.[82] This creates the risk that individuals' involvement replaces rather than complements platforms' and the media's responsibility for the use of news personalisation. The results above indicate that empowering individuals is not enough to create the conditions that can lead to trust. Instead, there was a strong relationship between a demand for more transparency and control, and a demand for (self-) regulation in order to support trust. Determining whether technology is trustworthy is therefore not only an individual concern, or individuals' responsibility. Indeed, policymakers need to both enable individuals to ensure that organisations using news personalisation do what they trust them to do and adapt the regulatory mechanisms with which regulation has traditionally safeguarded trust.[83] In that process, attention should be paid to the factors that individuals have indicated to be relevant to their trust, including information about the influence of

78 See for a full overview of the ways in which the GDPR can be used to influence personalisation Eskens (n 75).

79 European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (n 2) recital 62; CoE, 'Declaration on the Financial Sustainability of Quality Journalism' (n 34) para. 10, 12; 'Recommendation of the Committee of Ministers to Member States on Media Pluralism and Transparency of Media Ownership' (n 68) para. 10, 2.3.

80 Natali Helberger, Kari Karppinen and Lucia D'Acunto, 'Exposure Diversity as a Design Principle for Recommender Systems' (2018) 21 Information, Communication & Society 191 <https://www.tandfonline.com/doi/full/10.1080/1369118X.2016.1271900> accessed 15 May 2020; Jaron Harambam and others, 'Designing for the Better by Taking Users into Account: A Qualitative Evaluation of User Control Mechanisms in (News) Recommender Systems', *Proceedings of the 13th ACM Conference on Recommender Systems - RecSys '19* (ACM Press 2019) <http://dl.acm.org/citation.cfm?doid=3298689.3347014> accessed 27 September 2019.

81 Harambam and others (n 80); Ian Brown, 'Interoperability as a Tool for Competition Regulation' [2020] OpenForum Academy <https://euagenda.eu/upload/publications/ian-brown-interoperability-for-competition-regulation.pdf>; 'The Trust Project' (*Santa Clara University's Markkula Center for Applied Ethics*, 2018) <https://thetrustproject.org/>; Reporters Without Borders, 'Journalism Trust Initiative' (3 April 2018) <https://www.journalismtrustinitiative.org/>.

82 M Ananny and K Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2016) 20 New Media & Society 973.

83 José van Dijck, Thomas Poell and Martijn de Waal, *The Platform Society : Public Values in a Connective World* (Oxford University Press 2018) 30, 159 <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1901418&site=ehost-live&scope=site> accessed 13 February 2019.

advertisers and other commercial interests on the way in which personalisation operates, or the ability of editors to exercise control over personalisation.[84]

43 Similarly, information about the data collected to make personalisation possible, and the other purposes for which it is used or actors with whom it is shared, is relatively important to individuals' trust in whether organisations will inform them appropriately. The latter two factors are not directly related to the way in which media organisations inform individuals. As a result, when individuals determine whether they can trust an organisation using algorithms to inform them, they apparently also consider whether that organisation protects them from other risks that feature prominently in the public debate on technology.[85] Ensuring that the norms in data protection law, which already entitle individuals to this information, are effectively applied is consequently also an important aspect of ensuring trust when the media uses technology to inform its audience.[86] This especially holds true for public service media, which have a special obligation to act as a trusted source of information.[87]

44 Looking forward, exploring the role that general safeguards such as data protection play in supporting trust in different contexts is particularly important. This allows us to determine what role, if any, there is for overarching safeguards, as regards trust in horizontal legal frameworks such as the GDPR or AI Act. At the same time, it enables an analysis of the extent to which regulatory safeguards for trust need to take account of the specific context in which technology is employed. This is not only important to address the contextual nature of trust, it is also necessary to explore to what extent trust-supporting measures such as individuals' control can be integrated in a way that respects values such as media freedom and editorial independence. Further exploring the differences and similarities in the relationship between trust and regulation in different contexts is therefore key to creating a comprehensive and consistent regulatory approach to trust in organisations using technology.

84 Tobias Eberwein, Susanne Fengler and Matthias Karmasin, *The European Handbook of Media Accountability* (Routledge 2019) <https://www.routledge.com/The-European-Handbook-of-Media-Accountability/Eberwein-Fengler-Karmasin/p/book/9781472457660>.

85 Steedman, Kennedy and Jones (n 13); Gaurav Bansal and Fatemeh Mariam Zahedi, 'Trust Violation and Repair: The Information Privacy Perspective' (2015) 71 Decision Support Systems 62 <https://www.sciencedirect.com/science/article/pii/S0167923615000196>.

86 Bastian and others (n 76); Paul C Bauer and others, 'Did the GDPR Increase Trust in Data Collectors? Evidence from Observational and Experimental Data' (2021) 0 Information, Communication & Society 1 <https://doi.org/10.1080/1369118X.2021.1927138> accessed 24 May 2021.

87 Sørensen, Van den Bulck and Kosta (n 13).

Annex A - Survey

The questionnaire below was translated from the Dutch version originally shown to participants.

What is news personalisation?

News personalisation is a technology that is used to automatically show a different selection of news articles to each reader. You can see a good example in the image below. Here, NU.nl uses news personalisation to show readers "recommended articles" on part of its site.

Two things are essential to make news personalisation possible: data and algorithms.

1) First, **data** has to be collected from the readers, such as their reading behaviour (preferences and interests) or location.

2) Based on that data, **algorithms** are then used to recommend articles to readers.

Questionnaire

The media organisation

We now want to learn more about your trust in news personalisation. The following questions are about the different parties that can influence the way news is personalised.

How important are the following conditions for you to trust an organisation that uses news personalisation to inform you? (1: not important at all – 7: very important)?

Transparency**:**

- It is clear to what extent journalists and editors determine the way news is personalised.
- It is clear whether commercial parties such as advertisers influence the way news is personalised.
- It is clear to what extent the media organisation uses algorithms from other companies to personalise the news.

Control**:**

The ability to choose between the personalisation algorithms of different companies on a website.

The source of the articles

An algorithm can recommend news from different sources. Nu.nl, for example, only recommends its own articles. Conversely, Google News recommends articles from multiple media outlets, and Facebook recommends the articles its users upload.

How important are the following conditions for you to trust an organisation that uses news

personalisation to inform you? (1: not important at all – 7: very important)?

Transparency:

- It is clear what the identity of the source of a recommended article is.
- It is clear whether the source of a recommended article adheres to journalistic norms established by traditional media companies.
- It is clear whether a recommended article comes from a government institution.
- It is clear whether a recommended article is produced automatically or written by a human.

Control:

- The ability to choose from which sources you will receive news.
- The ability to choose to only receive news from sources that adhere to journalistic norms established by traditional media companies.

Data

To personalize news, data about you must be collected. This data is used to determine which news articles you are shown.

How important are the following conditions for you to trust an organisation that uses news personalisation to inform you? (1: not important at all – 7: very important)?

Transparency:

- It is clear what data is collected about you to personalize news.
- It is clear for which other goals the collected data is used.
- It is clear whether the collected data is shared with other parties.

Control:

- The ability to choose what data about you is used to personalise the news.
- The ability to delete the data used to personalise news for you.

Algorithm

In addition to your data, other information is also used to recommend articles. For example, how recent an article is, or what the subject is.

How important are the following conditions for you to trust an organisation that uses news personalisation to inform you? (1: not important at all – 7: very important)?

Transparency:

- It is clear why a specific article is recommended.
- It is clear which factors have the most impact on the way news is personalised.
- It is clear what goal the media organisation tries to achieve by personalising the news.

Control:

- The ability to turn news personalisation off.
- The ability to indicate that a specific type of news article should be recommended more or less.
- The ability to choose which factors have the most influence on the way news is personalised.
- The ability to choose which goals the personalisation algorithm aims to achieve.

The news offer

Because of news personalisation you will see some articles more, and some articles less.

How important are the following conditions for you to trust an organisation that uses news personalisation to inform you? (1: not important at all – 7: very important)?

Transparency:

- It is clear which parts of the site are personalised.
- It is clear what type of news (for example, entertainment, politics, sport) has been recommended to you more often.
- It is clear which important articles have not been recommended to you.

Control:

- The ability to choose to always see important articles.
- The ability to see which sources or articles have not been recommended.
- The ability to give feedback on the way news

personalisation works.

Closing questions

Knowledge about and trust in news personalisation

The following questions are about your awareness of the use of algorithms in the media. There are no right or wrong answers, this is not a test. We are interested in your own opinion. Please indicate to what extent you are aware of the following statements:

1. Algorithms are used to recommend posts to me on Facebook.
2. Algorithms show other people different posts than the ones I see.
3. Algorithms are used to customize certain posts on Facebook.
4. Algorithms are used to prioritize certain posts over other posts on Facebook.

Likert scale from 1 (completely unaware) to 7 (fully aware).

How much do you trust the media? (1:not at all to 7: very much).

Use of information and control

- How likely is it that you will pay attention to information about news personalisation, provided it is easy to see and understand? (1: not likely at all – 7: very likely)
- How likely is it that you will exercise control over how news is personalised, provided this control is easy to exercise? (1: not likely at all – 7: very likely)

Regulation of news personalisation

- Whose job is it to make sure you can control news personalisation?
  - The government.
  - The media.
  - The platforms such as Facebook and Google
  - The organisation that personalizes news.
  - Nobody.
- Whose job is it to make sure you can get information about news personalisation?
  - The government.
  - The media.
  - The platforms such as Facebook and Google.
  - The organisation that personalizes news.
  - Nobody.
- How important are the following conditions to enable you to trust an organisation that uses news personalisation to inform you? (1: not important at all – 7: very important)
  - The existence of (self-)regulation about the parties that influence the way in which news is personalised.
  - The existence of (self-)regulation about the sources of news articles that are recommended.
  - The existence of (self-)regulation about the way in which the collected data is used.
  - The existence of (self-)regulation about the functioning of the algorithm that personalizes news.
  - The existence of (self-)regulation about the type of news that is recommended.

Deviation from Objective Requirements for Conformity With a Contract of Digital Content or Digital Service: The Assessment of Its Use

by **Vadim Mantrov, Jānis Kārkliņš, Irēna Barkāne, Zanda Dāvida, Salvis Kārklis and Kristaps Silionovs***

Abstract: Currently the European Union (EU) is taking major steps in different legal areas including consumer protection law to implement the Digital Single Market Strategy in order to ensure effective and smooth functioning of the internal market in the modern economy. The new EU policy concerning the Consumer Digital Content Directive (Directive 2019/770) lays down common rules on requirements concerning contracts between traders and consumers for the supply of digital content or digital service. At the same time, the Directive allows deviation from the objective requirements for conformity with a contract of a digital content or digital service on the basis of certain preconditions explicitly envisaged by Article 8(5) of the Directive itself. The present article aims to discuss the possibility for use of such a deviation by critically assessing the preconditions for deviation to take place in conjunction with typical examples likely to appear in practice. The article begins by discussing the applicable regulation, providing a possibility for deviation from objective requirements for conformity with the contract. The article then proceeds to critical assessment of each precondition for use of a deviation in the light of examples that might either be permitted or not permitted under the applicable regulation. Furthermore, frequently used forms for supply of digital content or digital service are discussed considering the previous discussion of these preconditions, as deviation from objective requirements for conformity of digital content or digital service are most often found in online contracts. The article finishes by summarizing the discussion in the article.

Keywords: Directive 2019/770; Deviation; Conformity with the contract; Objective requirements; Digital content; Digital service

Recommended citation: Vadim Mantrov et al, Deviation from Objective Requirements for Conformity With a Contract of Digital Content or Digital Service: The Assessment of Its Use, 13 (2022) JIPITEC 323 para 1

A. Introduction

1 The European Commission (EC) has declared its Digital Single Market Strategy[1] which influences different areas regulated within European Union (EU) law, including consumer protection law, commercial law[2] and author law (i.e., copyright).[3] In the case of consumer protection law, the European legislator implemented a major revision of consumer sale with the aim of improving existing regulation, starting in 1999 when the Proposal for the Consumer Sales Directive (CSD) 1999[4] was adopted. Simultaneously, the EC legislator considered a new regulation on supply of digital content and digital service. This reform resulted in adoption of two new directives in 2019 aimed to protect the rights of consumers in specific matters, i.e., the CSD 2019[5] and the Consumer Digital Content Directive 2019 (DCD).[6] Both these directives aim for higher protection of consumers in the modern economy and e-commerce concerning conclusion and fulfilment of either a contract of sale or a contract for supply of digital content or digital service. As the EC explicitly admitted, "[t]he general objective of the proposals [*for adoption of these directives – authors' remark*] is to contribute to faster growth of opportunities offered by creating a true Digital Single Market, to the benefit of both consumers and businesses".[7] Furthermore, it has become necessary to reorient consumer law, still focused on protection the final purchaser of consumer goods, into a system that protects the user, usually a long-term user, of various types of goods and services, especially it appears in relation to digital content.[8]

2 The DCD introduces a list of objective and subjective requirements for conformity of digital content or digital service with the contract.[9] Simultaneously, the DCD allows for a trader to deviate from fulfilling the duty to ensure conformity with the contract. However, the EU policy in the DCD allowing such a deviation from objective conformity requires fulfilment of certain preconditions. By declaring the necessity "to ensure sufficient flexibility"[10], the EU legislator expressly allowed such a deviation included in Article 8(5) DCD by formulating these preconditions as discussed in the next Section of this article.

3 Interestingly, the EC did not initially include the above provision in the Proposal for a directive itself. It was introduced to the text of the Proposal after the EC transmitted it to the Council. Lack of such a provision was viewed as a shortcoming of the Proposal in its initial wording, so a suggestion was expressed to supplement the Proposal with a provision allowing the possibility for the contracting

* Dr. iur. Vadim Mantrov, Docent at Civil Law Science Department, Director of Legal Science Institute, Faculty of Law, University of Latvia; Dr. iur. Jānis Kārkliņš, Professor and Research Fellow, Faculty of Law, University of Latvia, janis.karklins@lu.lv; Dr. iur. Irēna Barkāne, Lecturer and Researcher, Faculty of Law, University of Latvia, irena.barkane@lu.lv; Dr. iur. cand. Zanda Dāvida, Faculty of Law, University of Latvia, zanda.davida@lu.lv; Salvis Kārklis, Faculty of Law, University of Latvia, salvis.karklis@lu.lv; Kristaps Silionovs, Faculty of Law, University of Latvia, kristaps.silionovs@lu.lv.

1 European Commission, 'A Digital Single Market Strategy for Europe' (Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions) COM(2015) 192 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192> accessed 11 November 2021.

2 European Parliament and Council Directive (EU) 2019/1151 of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law [2019] OJ L186/80.

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

4 European Parliament and Council Directive 1999/44/EC of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees [1999] OJ L171/12 (CSD 1999).

5 European Parliament and Council Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28 (CSD 2019).

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

7 European Parliament and Council, 'Proposal for a Directive on certain aspects concerning contracts for the online and other distance sales of goods' COM (2015) 635 final, Chapter 1.

8 Monika Jagielska, Monika Namysłowska, Aneta Wiewiórowska-Domagalska, 'The Changing Nature of the Consumer in the Digital Reality' in Dariusz Szostek and Mariusz Załucki (eds), *Internet and New Technologies Law* (Nomos 2021) 46-47.

9 DCD, art 7-8. Similarly also for consumer sale (CSD 2019, art 6-7).

10 DCD, Recital 49. Similarly also for consumer sale (CSD 2019, Recital 36).

parties to agree on the supply of digital content or a digital service that does not meet the standards normally required.[11] In the result, Article 8(5) DCD was adopted, allowing a deviation from objective requirements. Its wording was inspired by proposals for the other two directives, namely Article 4(3) of the Proposal for the Online Sales Directive and Article 99(3) of the Proposal for the Directive on Common European Sales Law.[12] Likewise, the wording of Article 8(5) DCD resembles the regulation of the previous CSD 1999 (though the CSD 1999 was not familiar with and thus did not regulate digital content or digital service as such); it also allowed the possibility that lack of conformity cannot be imputed to the seller if the consumer was aware of that non-conformity.[13] The CSD 1999 was based on the assumption that it was not possible to easily depart from the duty to ensure conformity. In this regard, the CSD 1999 itself provided that restricting or waiving the rights granted to consumers "should apply also to clauses which imply that the consumer was aware of any lack of conformity of the consumer goods existing at the time the contract was concluded"[14]. Therefore, Article 2(3) CSD 1999 in comparable manner as Article (8)5 of DCD provides:

4 There shall be deemed not to be a lack of conformity for the purposes of this Article if, at the time the contract was concluded, the consumer was aware, or could not reasonably be unaware of, the lack of conformity, or if the lack of conformity has its origin in materials supplied by the consumer.

5 Thus, a comparison of the CSD 1999 with the DCD demonstrates that the European legislator's policy since 1999 has already allowed a deviation from the objective requirements for conformity of a purchase object with the contract. This does not mean that the aim of the DCD is to provide lesser consumer protection. The different approach of the DCD is explained by the fact that DCD regulates digital content and digital service, which by their nature are different from tangible goods.

6 As such, this article aims to provide a comprehensive analysis on preconditions of deviation from objective requirements for conformity, as well as to provide analysis on online purchase agreements (as deviation from objective requirements of conformity of digital content or digital services are most often found in online forms). Finally, it draws conclusions on whether the possibilities of application of Article 8(5) of DCD does reduce the protection of rights of consumers. In order to answer the above questions and to provide the above analysis, the article compares the views expressed by various authors in legal literature, while also providing the authors' own views on the issue under analysis.

B. Overview of Preconditions Allowing Deviation from Objective Requirements for Conformity

7 The DCD itself provides for certain preconditions that allow deviation (or a waiver as indicated in legal literature)[15] from objective conformity requirements. Indeed, as was noted before, Article 8(5) DCD (read together with the DCD's preamble, Recital 49) provides for the possibility of such a deviation:

> *[t]here shall be no lack of conformity within the meaning of paragraph 1 or 2 if, at the time of the conclusion of the contract, the consumer was specifically informed that a particular characteristic of the digital content or digital service was deviating from the objective requirements for conformity laid down in paragraph 1 or 2 and the consumer expressly and separately accepted that deviation when concluding the contract.*

8 Article 8(5) DCD contains six preconditions that could be deduced from the provision itself. These would form the basis for use of deviation from objective requirements. This provision makes clear that these preconditions should take place cumulatively. However, the provision in question is rather poor in terms of the contents of the preconditions. As a result, much of their interpretation should be carried out on the basis of the interrelation with other provisions of the Directive and, more importantly, with the Directive's preamble. The burden of proof that these preconditions have been fulfilled will generally be on the trader.[16] As it is rightly noted in European consumer law literature, these preconditions should be considered

11 European Law Institute, 'Statement of the European Law Institute on the European Commission's Proposed Directive on the Supply of Digital Content to Consumers' (2016) 19. <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf.> accessed 19 November 2021.

12 Reiner Schulze, Dirk Staudenmayer, *EU Digital Law: Article-by-Article Commentary* (Hart Publishing, Beck, Nomos 2020) 164.

13 CSD 1999, art 2(3).

14 ibid, Recital 22 of the preamble.

15 Schulze, Staudenmayer (n 12) 162-168.

16 Schulze, Staudenmayer (n 12) 164. See further discussion in Section 2.2. of this article below.

separately, one by one.[17] Therefore, the authors of the article consider these preconditions critically, while also discussing the practical implications of these preconditions by referring to typical examples that could arise in practice.

I. Deviation May Solely Concern the Objective Requirements

9 A possible deviation may only concern the objective requirements for conformity of a digital content or digital service with the contract. Such a distinction between subjective and objective criteria is made for the first time in European contract law.[18] Though justification of this distinction goes beyond the scope of this article, it is sufficient to note that it is already subject to criticism in European legal literature.[19] The DCD itself expressly envisages this condition by permitting deviation from the objective conformity requirements only. Indeed, Article 8(5) DCD contains the phrase that "[t]here shall be no lack of conformity within the meaning of paragraph 1 or 2 if [..]". The reasoning for imposing such a condition is clear. Objective requirements of conformity with the contract are based on the understanding of what the consumer could reasonably expect from a particular type of digital content or digital service (including taking into account the statutory understanding of the features that a digital content or digital service must possess). For example, it is argued in legal literature that a consumer who has purchased a digital content or digital service that he can share with their family (for example, the access to the *Netflix* streaming platform) can reasonably expect to also be able to share it with friends.[20] A prohibition put forward by the trader on sharing the digital content or digital service with friends should be seen as a deviation from objective conformity (as such a prohibition cannot be reasonably justified).[21] This means that a digital content or digital service must be of the expected quality and performance, taking into account public statements made by the trader or others in the chain of transactions; it must come with adequate accessories and instructions; and it must match any trial version or preview that the trader made available to the consumer (and, presumably, that the consumer actually examined before the contract was concluded).[22] As can be seen, objective requirements for conformity with the contract under the DCD are specified using varying degrees of generality with verifying success. This has led some authors to question how simple it is to determine the objective requirements.[23]

10 Nevertheless, it is for the contractual parties to have a possibility to deviate from the statutory standard (i.e., objective conformity requirements) if either a digital content or digital service has a lack of conformity which is known to the consumer. As it is rightly noted, such a possibility is based on the good faith principle, which would prevent the liability of the trader if the consumer knew about the lack of conformity with the contract at the moment of conclusion of the contract.[24]

11 For instance, one of the objective requirements covers the situation that the digital content or digital service must be of the quantity—and possess the qualities and performance features including in relation to functionality, compatibility, accessibility, continuity and security—normal for digital content or digital service of the same type and which the consumer may reasonably expect.[25] Suppose a consumer contracts for an phone video game that is available on consumers phone market, but when downloading the game the consumer finds that it is only compatible with certain phone models, excluding the phone model of consumer. Such a deviation would mean that it corresponds to compatibility of the digital content being one of its "qualities and performance features".

12 However, as it arises from the phrase "[t]here shall be no lack of conformity within the meaning of paragraph 1 or 2 if [..]", a potential deviation cannot concern provisions of the Directive other than objective requirements of conformity with the contract (Article 8(1) and (2) DCD). For example, a deviation cannot be applied in respect of failure to install an update in every situation outside those specifically

17 ibid, 164-167.

18 Daniëlle Op Heij 'The Digital Content Contract in a B2C Legal Relationship from a European Consumer Protection Perspective' (2022) 11(2) EuCML 53, 57.

19 Reiner Schulze and Fryderyk Zoll, *European Contract Law* (3rd edn, Nomos Verlagsgesellschaft 2021) 49.

20 Karin Sein, Liliia Oprysk, 'Limitations in end-user licensing agreements: is there a lack of conformity under the new Digital Content Directive?' (2020) 51(5) IIC 594, 615

21 ibid, 606.

22 Hugh Beale, 'Digital Content Directive and Rules for Contracts on Continuous Supply' (2021) 12(2) JIPITEC 96, 97-98 <https://www.jipitec.eu/issues/jipitec-12-2-2021/at_download/CompleteIssue> accessed 1 December 2021.

23 Paula Giliker 'Legislating on contracts for the supply of digital content and services: an EU/UK/Irish divide?' (2021) 2021(2) Journal of Business Law 143, 146.

24 Schulze, Staudenmayer (n 12) 162.

25 Article 8(1)(b) DCD.

mentioned (Article 8(3) DCD), namely liability of the trader (Article 9 DCD[26]); burden of proof (Article 10 DCD); or remedies (Articles 13-14 DCD).

13 Likewise, a deviation is not permitted from data protection requirements either. Where personal data are provided by the consumer to the trader, the trader should comply with its duties under the General Data Protection Regulation (GDPR).[27] Such duties should be complied with in cases where the consumer pays a price and provides personal data.[28] EU data protection law should fully apply to the processing of personal data in connection with any contract falling within the scope of the DCD.[29] According to Article 3 (8) CSDD, in the event of conflict between the provisions of that Directive and EU law on protection of personal data, then EU law prevails.

14 Lack of conformity of digital content or a digital service with subjective or objective requirements for conformity may, depending on the circumstances of the case, also lead to lack of compliance with requirements provided for by the GDPR, including core principles such as the requirements for data minimization, data protection by design, and data protection by default.[30] Article 3(1) DCD entitles consumers to invoke rights and remedies provided for in the CSDD even when they do not pay a fee but instead provide personal data to the trader. It is expressly recognized that the consumer will be able to proceed with the remedies provided in the event of failure to supply or lack of conformity of the service or digital content.[31]

15 It should be added that the precondition under discussion means that deviation should not cover subjective requirements because subjective requirements depend on the contract itself. Therefore, it is not necessary to deviate from the contract provisions based on an agreement between the contractual parties. It is, therefore, rightly opined that any deviation from a subjective conformity criterion can be foreseen in the contract itself.[32]

II. Consumer Must Be "Specifically Informed" about the Deviation

16 The DCD also provides the precondition that a trader is allowed to deviate from objective conformity requirements only if "the consumer was specifically informed" of the deviation in question (Article 8(5) DCD).

17 Comparing the wording of this condition with previous draft directives (i.e., Article 4(3) Commission Proposal for an Online Sales Directive and Article 99 (3) Common European Sales Law), it may be concluded that this condition is not new to EU law. A minor difference, however, was introduced, as it can be seen by comparing the wording of the above directives' proposals: The knowledge criterion—"the consumer knew the specific condition"—was replaced with the condition "the consumer was specifically informed". Therefore, the criterion that "the consumer was specifically informed" needs to be interpreted to mean that the trader must actively bring the information sufficiently clearly and transparently to the consumer's attention. A common example would be the situation when the contract contains a clause stating the deviation (though it should be subject to separate acceptance as discussed further).

18 This criterion, therefore, would not be fulfilled in cases where the consumer needs to actively search for information, for instance if the information is in a hyperlink incorporating other hyperlinks or the consumer needs to scroll and search the hyperlink on the website[33] or when consent is included in a framework agreement for purchase of digital content or a digital service as a term of the contract (discussed later in the article).

19 The authors support the opinion that Article 8 (5) DCD can only be fulfilled if information regarding specific deviations was actively and directly brought to the consumer's attention, so that a mere hyperlink would not suffice. Similarly, a mere reference to the end-user licence agreement of the right-holder in the standard terms and conditions of the trader

26 Schulze, Staudenmayer (n 12) 162.

27 European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016], OJ L119/1 (General Data Protection Regulation).

28 ibid, Recital 69 of the preamble.

29 Dominik Lubasz, Zanda Davida, 'Consumer Personal Data as a Payment – Implementation of Digital Content Directive in Poland and Latvia' (New Legal Reality: Challenges and Perspectives II, the 8th International Scientific Conference of the Faculty of Law of the University of Latvia, University of Latvia Press 2022) 521, 528 <https://www.apgads.lu.lv/konferencu-krajumi/new-legal-reality-challenges-and-perspectives-ii> accessed 11 May 2022.

30 General Data Protection Regulation, Recital 48 of the preamble.

31 ibid, Recital 24.

32 Schulze, Staudenmayer (n 12) 163.

33 Schulze, Staudenmayer (n 12) 164.

would not be sufficient either.[34] It is well known that consumers are unlikely even to look at lengthy terms and conditions, let alone read them with any care before they conclude a contract. Consumers should not be expected to read the small print of the contract to see if the express terms qualify or restrict the traders' "objective" obligations,[35] but should instead be informed sufficiently clearly and transparently regarding each deviation.

20 In this regard we can draw parallels with Article 5(1) Directive 97/7 as it regulates when the information is considered to be delivered to the consumer under EU law in regards to distance contracts.[36] In interpreting this provision, the Court of Justice of the European Union in *Content Services Ltd v Bundesarbeitskammer* (Case C-49/11) noted that, where information found on the seller's website is made accessible *only via a link sent to the consumer*, that information is neither "given" to nor "received by" that consumer within the meaning of Article 5(1) of Directive 97/7.[37]

21 It should be noted however, that Article 8(5) DCD does not specifically state that a duty to inform the consumer lies upon the trader itself. Given the nature of digital content and the nature of its distribution, it seems that there would be no violation of this provision if information about the deviation were to be provided by a third party, as rightly argued in legal literature.[38] For example, digital content may be accessed in a second hand market on the digital application distribution webpage, which became known to a consumer by visiting the webpage of the main provider of the digital content (for example, a photo correction application), if the latter webpage, before revealing second market retail web pages, specifically informs the consumer about lack of objective requirements. In this situation, it would be appropriate to conclude that the consumer was "specifically informed" about lack of conformity. However, in similar cases, where consumers would be informed by third parties about lack of conformity of the object, one could predict that it would be quite difficult for the trader to prove that such information was given. At the same time, information about lack of conformity from third parties should not come into contradiction with the next criterion to be discussed further.

22 It should be also mentioned that, according to the provision under discussion (in the light of Recital 49 and the last sentence of Recital 53 of the preamble to the DCD), it may not apply if the consumer has acquired knowledge of a particular deviation either based on their own initiative or otherwise (for instance, through information circulating in social media or the internet community). For example, the author of a popular and widely cited blog explains that a particular software program is not compatible with a certain operating system. This would mean that the consumer may be aware of that deviation concerning the compatibility of that digital content. Even if the trader can prove that the consumer knew or should have known about the blog entry, this is not enough to fulfil the "specifically informed" criterion, as positive knowledge in this regard (from information provided by the trader) is necessary—less strict variations of knowledge, as in the CSD 1999,[39] will not be considered sufficient.[40]

23 Unlike some directives which contain a specific form for providing information to the consumer,[41] the

34 Gerald Spindler, 'Digital Content Directive And Copyright-related Aspects' (2021) 12(2) JIPITEC 111, 129 <https://www.jipitec.eu/issues/jipitec-12-2-2021/at_download/CompleteIssue> accessed 1 December 2021.

35 Hugh Beale, 'Scope of application and general approach of the new rules for contracts in the digital environment. In-depth analysis' (2015) Directorate General for Internal Policies. Policy Department C: Citizens' Rights and Constitutional Affairs. Legal Affairs. Study commissioned at the request of the European Parliament's Committee on Legal Affairs (JURI) <http://www.epgencms.europarl.europa.eu/cmsdata/upload/4a1651c4-0db0-4142-9580-89b47010ae9f/pe_536.493_print.pdf> accessed 25 December 2021.

36 Article 5(1) of Directive 97/7 states: "[t]he consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Article 4 (1) (a) to (f), in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him. In any event the following must be provided: [..]".

37 Case C-49/11 *Content Services Ltd v Bundesarbeitskammer* [2012] ECLI:EU:C:2012:419, para 37.

38 Schulze, Staudenmayer (n 12) 164.

39 Article 2 (3) of Directive 1999/44/EC envisages that there shall be deemed not to be a lack of conformity for the purposes of this Article if, at the time the contract was concluded, the consumer was aware, or could not reasonably be unaware of, the lack of conformity, or if the lack of conformity has its origin in materials supplied by the consumer.

40 Schulze, Staudenmayer (n 12) 164.

41 For example, Annex II of the Consumer Credit Directive 2008 (Directive 2008/48/EC) contains a form which must be followed regarding provision of specific pre-contractual information. See European Parliament and Council Directive 2008/48/EC of 23 April 2008 on credit agreements

DCD does not provide a specific form to be used when informing the consumer, and it is therefore left to the trader's choice as long as the preconditions contained in Article 8(5) are met.

III. Information about Deviation Must Be Provided Not Later Than at the Time of Concluding the Contract

24 Another precondition deals with the time when the consumer should be informed about the deviation. The DCD requires that the consumer is informed about the deviation "at the time of the conclusion of the [..] contract" (Article 8(5) DCD). As one may observe from this provision, a trader must inform the consumer right at the moment when the contract is concluded. The usual way of fulfilling this condition would be a separate statement by the trader, delivered to the consumer, explaining the deviation. The wording "at the time of the conclusion of the [..] contract" indicates that the consumer must be informed about the specific deviation at the moment when expressing acceptance of conclusion of the contract.

25 However, the question arises whether it is permitted to inform the consumer before conclusion of the contract. It is argued in legal literature that this question should be answered in the negative because pre-contractual information will not be a basis for information about the deviation because the consumer must be informed "at the time of the conclusion of the contract, not beforehand".[42] This opinion could hardly be considered as valid. The DCD itself allows the trader to inform the consumer about the deviation "before the conclusion of the contract". Arguments in favour of the conclusion that the consumer may be informed before conclusion of the contract is twofold. Firstly, the last sentence of Recital 53 of the preamble to the DCD expressly allows for information about the deviation to be given to the consumer before conclusion of the contract. The wording of this provision does not seem to be a mere typing error as the same wording persists in the different language versions (e.g., English, Latvian, Polish, German).[43] Secondly, the wording of Article 8(5) DCD itself does not seem to prohibit informing the consumer before conclusion of the contract, as it states that "*at the time of the conclusion of the contract, the consumer was specifically informed.*" In other words, Article 8(5) DCD states only that the consumer needs to be specifically informed not later than at the time of conclusion of the contract.

26 In addition, the precondition allowing receipt of information from third parties, as previously discussed, expressly demonstrates the possibility also to inform the consumer about the deviation before conclusion of the contract. Likewise, information about a deviation may be included in the pre-contractual information submitted to the consumer as this information forms part of the contract. The obligation of information could be said to be fulfilled if the trader sends an e-mail to consumer specifically informing the consumer about deviation before the consumer has entered into the contract (for example, before a consumer has given their credit card data or pressed "buy" to complete the conclusion of an agreement). Therefore, the authors argue that Article 8(5) DCD must be read widely, not limited to the requirement to provide information at the time of conclusion of the contract.

27 At the same time, the mere possibility to inform the consumer before conclusion of a contract cannot be used as a tool to manipulate consumer choice or understanding, as other preconditions for a

for consumers and repealing Council Directive 87/102/EEC [2008] OJ L133/66.

42 Schulze, Staudenmayer (n 12) 165.

43 For example, the English version of the last sentence of Recital 53 of the preamble to the DCD states that: "The trader should only be able to avoid such liability by fulfilling the conditions for derogating from the objective requirements for conformity as laid down in this Directive, namely only if the trader specifically informs the consumer before the conclusion of the contract that a particular characteristic of the digital content or digital service deviates from the objective requirements for conformity [..]". The same sentence in the Latvian version states "Tirgotājam vajadzētu būt iespējai no šādas atbildības izvairīties, tikai izpildot nosacījumus atkāpei no šajā direktīvā noteiktajām objektīvajām atbilstības pra sībām, proti, tikai tad, ja tirgotājs pirms līguma noslēgšanas konkrēti informē patērētāju, ka digitālā satura vai digitālā pakalpojuma kāda konkrēta īpašība atkāpjas no objektīvajām atbilstības prasībām [..]"; in Polish "Przedsiebiorca powinien móc uniknać pociagniecia do odpowiedzialności wyłacznie wtedy, gdy spełni warunki umożliwiajace odstepstwo od obiektywnych wymogów zgodności z umowa określonych w niniejszej dyrektywie, a mianowicie jedynie wtedy, gdy wyraźnie poinformuje konsumenta przed zawarciem umowy o tym, że określona cecha treści cyfrowych lub usługi cyfrowej odbiega od obiektywnych wymogów zgodnośc [..]"; in German "Der Unternehmer sollte einer dementsprechenden Haftung nur entgehen können, wenn er die Bedingungen für Abweichungen von den in dieser Richtlinie festgelegten objektiven Anforderungen an die Vertragsmäßigkeit erfüllt, was konkret bedeutet, dass der Unternehmer den Verbraucher vor Abschluss des Vertrags ausdrücklich darüber informiert, dass eine bestimmte Eigenschaft der digitalen Inhalte oder digitalen Dienstleistungen von den objektiven Anforderungen an die Vertragsmäßigkeit abweicht [..]".

permitted deviation from objective requirements still apply. It is doubtful that a trader could, for example, validly allege having properly informed the consumer about a deviation if the consumer was familiar with the deviation from the objective requirements years ago and the trader can prove it, for instance, via webpage server printouts.

IV. A "Particular Characteristic" Must Be Indicated

28 The DCD pursues the specific information approach, rejecting the general information approach concerning a characteristic of digital content or a digital service that is affected by a deviation. Thus, the Directive requires that "the consumer was specifically informed that a *particular* [emphasis added – authors' remark] characteristic of the goods was deviating from the objective requirements for conformity laid down in" (Article 8(5) DCD). The rationale of the condition "a particular characteristic" prevents a trader from introducing a deviation or a set of deviations in general. For instance, such a situation could be where the contract states that the trader is not responsible for any lack of conformity, or the trader is not responsible for any non-compatibility with any existing operating system or device. These and similar clauses would therefore contradict the notion of "a particular characteristic" and would be contrary to the Directive. Therefore, it would not be sufficient, as is asserted in legal literature, if the trader expressly mentions a deviation from the objective requirements while not specifically identifying the pertinent characteristics.[44]

29 Likewise, it is not sufficient if a trader simply describes the relevant feature of the digital content or digital service. According to Article 8(5) DCD (as well as Recitals 49 and 53 of the preamble to the DCD), the consumer needs to be able to comprehend the implications of this feature and to be enabled with this information to take a reasonable and deliberate decision to enter into a contractual relationship. Therefore, the information provided by the trader should indicate that a specific feature of digital content or a digital service deviates from the objective conformity requirements. It must be clear to the consumer that the reason this characteristic is mentioned is that the digital content or digital service does not meet the standard that could otherwise be expected.[45]

30 Therefore, the contract clause must list the specific characteristic of a digital content or digital service that is deviated from. For instance, the contract clause states that a particular video game or a software program is meant to be used in a tablet only or in another device. In addition, there are applications which operate only in a particular operating system, for instance, in computers using the *macOS* operational system, and, therefore, cannot operate so easily on a computer using *Windows*. For example, the video editing application *Final Cut Pro* is specified to run only on the *macOS* operating system, with *macOS* 11.5.1 as the minimum required operating system version ("*macOS* 11.5.1 or later"). In this case, the trader must fully indicate that this application is compatible with a particular computer operating system. Simultaneously, this example highlights the specific situation. Namely, if a digital content or digital service deviates from the objective requirements only partly, then the remaining part of the digital content or service must meet the objective requirements. For example, a trader informs the consumer that a software program operates only in a particular operating system, for instance, in smartphones using *Android.* This situation would mean that the software program supplied must comply with the objective (as well as subjective) requirements for conformity with the contract if it is used in smartphones based on *Android* but if the consumer uses a smartphone with a different operating program or uses the software program in another device, such use is subject to deviation from the objective requirements for conformity with the contract.

V. The Consumer Must Expressly Accept the Deviation

31 The last two preconditions are the consumer's express (1) and separate (2) acceptance to the deviation. These preconditions arise from the phrase "the consumer expressly and separately accepted that deviation" contained in the Article 8(5) DCD, and in essence incorporate the principle that any deviation from the objective conformity requirements requires an agreement between the trader and the consumer (rather than just requiring the trader to unilaterally inform the consumer of such deviation). Moreover, as it will be described further below, the prerequisites of separate and express acceptance practically entail that this agreement is subject to a qualified form of consent, which excludes the possibility of obtaining it through the current widespread forms of agreement (such as so-called shrink-wrap, box-wrap, browse-wrap and sign-in-wrap agreements).

32 The precondition of "express acceptance" is to be interpreted in conjunction with Recital 49 of the preamble to the DCD, according to which consumer has to accept the deviation by way of active and

44 Schulze, Staudenmayer (n 12) 165.

45 Schulze, Staudenmayer (n 12) 164.

unequivocal (in other words express) conduct. The necessity for active and unequivocal conduct means that the consumer's acceptance cannot be tacit or implied, such as by statements often found in websites of traders which provide that the act of browsing the website constitutes acceptance to their general terms, or that the act of registering or signing into an account constitutes an acceptance to the terms of service described on the same webpage or available via a hyperlink. For example, a notice on a social media platform's registration form, which states that "By signing up, You agree to our Terms (hyperlink provided) and Privacy Policy (hyperlink provided)" would not meet the requirement of express acceptance even if instead of Terms and Privacy Policy, this notice would specifically describe the deviations from the objective conformity requirements.

33 As noted in legal literature, the precondition of "express" acceptance was already laid down in the EC's Proposal for an Online Sales Directive in order to prevent that acceptance could be made subject to standard terms and conditions,[46] and the phrase "expressly accepted" requires an individually negotiated contract clause.[47] In our view, however, the inclusion of deviations in the general terms of the contract, does not preclude the possibility of "express acceptance", and the necessity for "individually negotiated contractual clause" instead results from the requirement of "separate acceptance", which will be described in more detail in the next subsection.

34 Article 8(5) DCD requires that the "consumer expressly and separately accepted that [emphasis added] deviation when concluding the contract", therefore there needs to be a clear link between the consumer's acceptance and the deviation—acceptance needs to refer to, and only cover, the specific deviation from the objective conformity requirements as regards the particular characteristic of the digital content or digital service.[48] Therefore this criterion will not be fulfilled in the widespread "as is"[49] or similar clauses in the trader's terms and conditions. This aspect was already argued for Article 99(3) Common European Sales Law which provided for a similar yet lower deviation standard.[50] The authors agree with the view expressed in legal literature, namely that in order to protect the reasonable expectations of the consumer, the courts should set high standards for "express agreement" to exclude the liability of traders, especially in cases where such exclusion would come as a surprise to a reasonable consumer,[51] while "as is" clauses do not provide for a clear link between consumer's acceptance and the deviation, nor can it be concluded from them that the consumer has unequivocally agreed to accept these deviations.

35 In addition, the "express acceptance" criterion will also not be met if the trader has inferred it by using default options which the consumer is required to reject in order for deviation not to apply (for example pre-ticked boxes). A similar conclusion has already been reached by the EC Directorate-General for Justice and Consumers (JUST) regarding the phrase "if the performance has begun with the consumer's prior express consent and his acknowledgment [..]" contained in Article 16(m) of the Consumer Rights Directive (Directive 2011/83/EU).[52] Namely, it was stated that "express" consent and acknowledgement for the purposes of Article 16(m) should be interpreted as requiring the consumer to take positive action, such as ticking a box on the trader's website. A pre-ticked box or accepting the gen-

46 Schulze, Staudenmayer (n 12) 165.

47 Karin Sein, 'The applicability of the digital content directive and sales of goods directive to goods with digital elements' (2021) (30) Juridica International 23, 27.

48 Schulze, Staudenmayer (n 12) 166.

49 Under an "as is" clause, the buyer agrees that the product quality is acceptable in its present condition, when the contract is signed. An "as is" clause places all the risk on the buyer, so it would be desirable to combine it with providing the buyer an opportunity to inspect. This clause is often recognized as an argument for applying the *caveat emptor* doctrine, to exclude seller's liability for defects (*see* Robin Paul Malloy, James Charles Smith, *Emanuel law outlines. Real estate* (3rd edn, The Emanuel Law Outlines Series, Wolters Kluwer 2015) 50). For example, regarding real estate, the *caveat emptor* doctrine is recognized as a legal rule in England, but is also indirectly applied in different EU Member States (*see* Christoph Ulrich Schmid and others, 'Real property law and procedure. General Report. Final Version' (European University Institute Florence/European Private Law Forum Deutsches Notarinstitut 2005) 59 <https://www.eui.eu/Documents/DepartmentsCentres/Law/ResearchTeaching/ResearchThemes/EuropeanPrivateLaw/RealPropertyProject/GeneralReport.pdf> accessed 28 November 2021).

50 Karin Sein, Gerald Spindler, 'The new directive on contracts for supply of digital content and digital services – Conformity criteria, remedies and modifications – Part 2' (2019) 15(4) European Review of Contract Law 365, 374.

51 Sein (n 46) 27.

52 European Parliament and Council Directive 2011/83/EU of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64.

eral terms is not likely to satisfy the requirements of Article 16(m).[53]

36 Although at the outset the above-described preconditions for deviation from the objective conformity requirements and the precondition of "separate acceptance" described in the following subsection gives consumers significant protection in the digital content and services market where deviations are justified on the basis of private autonomy, the EU legislator may have indirectly encouraged Article 8(5) DCD being perceived as a simple formality by traders. Namely Recital 49 of the preamble to the DCD provides a set of examples of how the preconditions of express and separate acceptance could be fulfilled, i.e., "by ticking a box, pressing a button or activating a similar function".

37 In this regard, the authors agree with the view that: firstly, it would not be reasonable to consider Recital 49 of the preamble to the DCD detached from the conditions set out in Article 8 (5) DCD, and the examples mentioned in this Recital of the preamble such as "ticking a box, pressing a button or activating a similar function" are simply examples and their use (such as ticking a box according to which consumer accepts general terms and conditions) does not in itself give grounds for believing that the trader is exempted from ensuring compliance with objective conformity requirements[54]; and secondly, traders should follow the provision contained in Article 5 of the Unfair Contract Terms Directive,[55] according to which written contractual terms must always be drafted in plain, intelligible language.[56]

38 As noted by Professor Hugh Beale, the term "expressly" should be interpreted as requiring that the actual facts be made clear to the consumer and that application of the Unfair Contract Terms Directive is possible as well. Application of the Unfair Contract Terms Directive may provide consumers useful additional protection from the requirement that traders use plain and intelligible language. Namely, "expressly" in Article 8(5) DCD should equally be interpreted as requiring transparency.[57] Such interpretation would be desirable as non-transparent (difficult to understand) deviations would call into question whether consent was indeed given "expressly" (which requires unequivocal conduct according to Recital 49 of the preamble to the DCD).

39 In addition, the necessity to formulate agreements regarding deviations in plain, intelligible language arises indirectly from the obligation contained in Article 8(5) DCD that consumer must be "specifically informed" about each particular deviation. As explained above, this criterion requires positive knowledge from the consumer, which naturally implies the need for consumer to actually be able understand the deviation. Furthermore, it would be difficult to see how Article 8(5) DCD would be in line with the purpose of the DCD (stated in Article 1 DCD) to "contribute to the proper functioning of the internal market while providing for a high level of consumer protection" if the trader would be allowed to include deviations in a way that is not understandable to the average consumer, thereby preventing the consumer from making an informed choice as regards to acceptance to deviations.

40 The necessity to provide for deviations in plain, intelligible language perfectly fits with the aim of the EU legislator. That is, while providing for the possibility of deviating from objective conformity requirements, the EU legislator has striven to ensure that the consumer is completely and clearly aware of what and to what extent they agree to and take an active and deliberate conscious decision.[58] whenever the digital object provided deviates from the consumer's reasonable expectations. Furthermore, the whole purpose of Article 8 (5) DCD is that deviations from the objective requirements of Article 8(1) and (2) are possible only under strict conditions.

41 Article 5 of the Unfair Contract Terms Directive con-

53 European Union Commision's Directorate-General for Justice and Consumers (JUST), 'Guidance document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council' (2014) 66 <https://ec.europa.eu/info/sites/default/files/crd_guidance_en_0.pdf> accessed 20 November 2021. Essentially the same conclusion has been stated in: European Union Commission Notice 'Guidance on the interpretation and application of Directive 2011/83/EU of the European Parliament and of the Council on consumer rights' (2021) point 5.7. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021XC1229(04)&from=EN> accessed 1 May 2022.

54 Salvis Kārklis, 'Jauns digitālā tirgus regulējums: Nākamgad gaidāmās izmainas un to piemērošanas problēmas' [A New Digital Market Framework: Changes Expected Next Year and Their Application Problems] (2021) 47 (18) Jurista Vārds 18, 25.

55 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29 (Unfair Contract Terms Directive).

56 Schulze, Stadenmayer (n 12); Kārklis (n 54) 25.

57 Beale (n 21) 98.

58 Schulze, Staudenmayer (n 12) 163.

tains a "transparency requirement". Schulze and Zoll note that the principle of transparency may be viewed as a further expression of the consumer's reasonable expectations being among the central features of EU contract law. The content of the contract may only be influenced by factors that the consumer can expect. Such factors must be sufficiently clear in order to be acknowledged by the consumer. A transparency requirement is expressly included in several EU directives, for example, Articles 5(1) and 6(1) of the Consumer Rights Directive and Article 5 of the Unfair Contract Terms Directive. This principle is not merely a feature of EU consumer law, as it can also be seen in Article 3(1)(a) of the recent Platform Regulation, which states that providers of an online intermediation service shall [i.e., must] ensure that their terms and conditions are drafted in plain and intelligible language.[59] A transparency requirement is also contained in other provisions of the DCD, such as Article 19(1)(3), which requires that the consumer must be informed in a *clear and comprehensible manner* of any modification of the digital content or digital service, especially in situations where those modifications impact negatively the consumer where the obligation to inform is strengthen.[60]

42 The concept of the transparency requirement contained in Article 5 of the Unfair Contract Terms Directive has been extensively discussed in the case law of the Court of Justice of the EU. As confirmed in *Jean-Claude Van Hove v CNP Assurances SA*,[61] in order for a provision to be worded "in plain and intelligible language", it must be comprehensible not only literally (formally and grammatically) but also in substance so that the consumer can easily foresee the consequences of such a provision. A similar conclusion can also be inferred from several other European Court of Justice judgments (*Kásler,*[62] *RWE Vertrieb AG*,[63] and *RWE Bogdan Matei*[64]). In order to evaluate whether a waiver is expressed in "plain and intelligible language" we have to take into account, for example, the level of attention expected from the average consumer, who is reasonably well informed and reasonably observant and circumspect.[65] Another important aspect noted in *RWE Vertrieb AG* is that "it is clear that obligation to make the consumer aware [..] is not satisfied by the mere reference, in the general terms and conditions, to a legislative or regulatory act determining the rights and obligations of the parties. It is essential that the consumer is informed by the seller or supplier of the content of the provisions concerned".[66] This applies even if that the trader mentions mandatory statutory or regulatory provisions[67]: if there are circumstances which would allow the consumer to rely on objective conformity requirements, it would apply as well. When applying this transparency requirement to a waiver (ie, a deviation), it is insufficient to refer simply to the respective objective conformity requirement, but rather it is necessary to demonstrate how a deviation from the objective conformity requirements takes place.[68]

43 However, as noted by Oprysk, while providing clear information to consumers could theoretically help them decide on a provider, the impact is limited in practice if the supply is not diverse or a consumer is locked into using a particular platform anyway.[69] Transparency would be of greater importance if viable alternatives were available and if a consumer could choose and easily switch between them. In practice, contracts and end-user licence agreements could remain on a take-it-or-leave-it basis with no satisfactory alternatives.[70] Accordingly, the level of consumer protection in practice will most likely depend on the preferences of traders with the greatest network effects and bargaining power in the market.[71] It is therefore to be hoped that in future the EU legislator will set out more restrictions for the possibility to deviate from the objective conformity requirements, to limit the opportunity for traders to deviate from such objective conformity requirements

59 Schulze, Zoll, 9) 51.

60 Martim Farinha, 'Modifications on the digital content or digital service by the trader in the Directive (EU) 2019/770' (2021) 25 (2) Red-Revista Electronica De Direito 84, 92.

61 Case C-96/14 *Jean-Claude Van Hove v CNP Assurances SA* [2015] ECLI:EU:C:2015:262.

62 Case C-26/13 *Árpád Kásler, Hajnalka Káslerné Rábai v OTP Jelzálogbank Zrt* [2014] ECLI:EU:C:2014:282.

63 Case C-92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen e.V* [2013] ECLI:EU:C:2013:180.

64 Case C-143/13 *RWE Bogdan Matei, Ioana Ofelia Matei v SC Volksbank România SA* [2015] ECLI:EU:C:2015:127.

65 Geraint Howells and others, *Rethinking EU Consumer Law* (Routledge 2018) 27-31.

66 Case C-92/11 *RWE Vertrieb AG v Verbraucherzentrale Nordrhein-Westfalen e.V* [2013] ECLI:EU:C:2013:180.

67 ibid.

68 Schulze, Staudenmayer (n 12) 168.

69 Liliia Oprysk, 'Digital Consumer Contract Law Without Prejudice to Copyright: EU Digital Content Directive, Reasonable Consumer Expectations and Competition' (2021) 70(10) GRUR International 951.

70 ibid 952.

71 ibid 954.

that are derived from EU law.[72] Similarly, according to Article 3(8) DCD, deviations currently from the objective conformity requirements do not affect the provisions of EU law on protection of personal data.

44 Alternatively, the EU legislator could at the very least provide that the scope of the Product Liability Directive[73] will be extended explicitly to digital content and digital service, while reducing the current limitation contained in Article 9(1)(b) of the Product Liability Directive, which provides that damage amounting to at least 500 euros must be caused for application of that Directive. According to Article 12 of the Product Liability Directive (and as confirmed in its preamble), no contractual derogation is permitted as regards the liability in relation to the injured person. Applying this directive irrespective of the deviations made within the meaning of Article 8(5) DCD could ensure at least partially effective remedies if a digital content or digital service does not provide the safety which a person is entitled to expect. As mentioned by the EC, "[d]igital content, software and data play a crucial role in the safe functioning of many products but it is not clear to what extent such intangible elements can be classified as products under the Directive. It is therefore unclear whether injured parties can always be compensated for damage caused by software, including software updates, and who will be liable for such damage".[74]

45 The situation "leave or confirm deviation" should be seen together with practical analysis: For example, whether the trader offers the same non-diversion digital content or digital service to other consumers, whether offering the deviating digital content or service to the consumer would cause disproportionate difficulties or significant economic loss, or whether the deviation has an objective justification for its necessity.

46 Likewise, the precondition under discussion cannot be applied in isolation from the rest of EU law, particularly other legal acts falling within EU consumer protection law. In this way, EU law may not only affect the interpretation and application of the above preconditions that allow deviation but may be also applied in parallel to those preconditions by banning a trader from circumventing consumer protection guarantees under EU law.

47 As it is justly indicated in legal literature, a deviation from objective requirements is not likely to be individually negotiated (Article 3(2) Unfair Contract Terms Directive). Likewise, they do not fall within exceptions from application of regulations on standard contract terms: 1) they are not mandatory or otherwise prescribed; 2) they normally do not relate to the definition of the main subject matter of the contract; and 3) they do not relate to the "adequacy of the price and remuneration" (Article 1(2) or Article 4(2) Unfair Contract Terms Directive).[75] From the point of view of the possibility to use standard terms for drafting the deviation, it is possible to speak about "accusation" against the EC suggested in legal literature concerning drafting of the DCD[76] which relates to deviation because it also leaves the contract content to the parties, i.e., the trader in practice, so that the consumer is vulnerable to disadvantageous provisions in standard term contracts.[77] However, further discussion of these issues concerning the impact of the Unfair Contract Terms Directive on the drafting of the deviation from the objective requirements goes beyond the scope of this article and, therefore, should be left for further studies.

VI. The Consumer Must "Separately" Accept the Deviation

48 Finally, the DCD follows the separateness approach by requiring that a contract for a particular digital content or digital service itself be separated from the consumer's acceptance of the deviation. Indeed, Article 8(5) DCD requires that the "consumer [..] *separately* [emphasis added] accepted that deviation when concluding the contract".

49 As it can be seen from Recital 49 of the preamble to the DCD, the requirement for a "separate" acceptance of the deviation is not fulfilled if a statement containing such acceptance is contained

72 *See.* Article 8(1)(a) DCD

73 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L210/29 (Product Liability Directive).

74 European Commission. Inception Impact Assessment. Initiative 'Civil liability – adapting liability rules to the digital age and artificial intelligence' (Ref. Ares(2021)4266516 - 30/06/2021) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en> accessed 11 December 2021.

75 Schulze, Staudenmayer (n 12) 167.

76 Paula Giliker, 'Adopting a Smart Approach to EU Legislation: Why Has It Proven So Difficult to Introduce a Directive on Contracts for the Supply of Digital Content?' in Tatiana Synodinou and others (eds), *EU Internet Law in the Digital Era: Regulation and Enforcement* (Springer 2019) 311.

77 ibid 312.

in other statements or agreements, such as: 1) an agreement to standard terms and conditions; 2) an explicit acknowledgement by the consumer that the order implies an obligation to pay[78]; or 3) consent to processing data. Accordingly, the word "separate" in the above provision should be interpreted restrictively as meaning that the consumer's consent must be given separately from any other terms of the contract. However, this does not mean that consent must be included in a separate document. Thus, it is argued in legal literature that it will not be sufficient to obtain the consumer's consent to the general terms and conditions of the contract in order to fulfil this condition.[79]

50 The DCD does not provide a specific form to be used for acceptance, nor does it exclude that the consumer may give the statement of acceptance to another party than the trader.[80] Nevertheless, it can be concluded from the text of Article 8(5) DCD that for each digital content or digital service characteristic which deviates from the objective conformity requirements a separate acceptance is required. This conclusion is supported by the wording of Article 8(5) DCD according to which consumer must be "specifically informed that that a particular characteristic [emphasis added] of the digital content or digital service was deviating from the objective requirements for conformity and the consumer [..] separately accepted that deviation [emphasis added] when concluding the contract".

51 A trader who wishes to deviate from any objective conformity requirement should do so with a short, easy-to-understand list of boxes or bullets setting out precisely, unambiguously, and separately those characteristics that do not meet the objective conformity requirements, requiring separate acceptance for each of them.[81] Such an approach would indeed be preferable to listing all deviations in a single document and requesting acceptance for them as a whole. In this regard, the classical situation of conclusion of a contract depicts two parties of relatively equal bargaining power who negotiate the details of a transaction that each fully comprehends, and who then expressly agree to the resulting terms. However, in a typical consumer contract, the trader drafts a set of standard contract terms, without a consumer's input and then submits these standard terms to consumers, on a take-it-or-leave-it basis. The consumer pays attention not to the standard contract terms, but to a few primary terms, such as the product's description and its price. The consumer, who is focused on primary contract terms, almost never reads or comprehends the standard contract terms, but indicates assent to them, e.g., by signing at the bottom of a long document or clicking a button labelled "I agree".[82] If traders were to summarize all the characteristics they might consider as deviations from the objective conformity requirements in a separate document (e.g., entitled "deviation terms" or "additional terms") and ask for a consumer's acceptance at the end of that document, there is a risk that consumers might perceive these terms similarly to standard contract terms and click the "I agree" button without actually reading them. Whereas if the consumer had to give separate acceptance for each characteristic that does not meet the objective conformity requirements, this would likely lead to greater consideration of these terms and contribute to informed decision-making.

C. Assessment of the Typical Forms for Limitation of Liability Used in Practice

52 Taking into account the above discussion and conclusions regarding the preconditions for deviation from the objective conformity requirements with the contract, it is now possible to evaluate whether frequently used forms of agreements, i.e., shrink-wrap, box-wrap, click-wrap, browse-wrap, and sign-in-wrap, would fulfil these preconditions. The authors will first describe the essence of each of these forms, and then explain which of them could fulfil the preconditions contained in Article 8(5) DCD.

53 *Shrink-wrap agreements* derive their name from the clear plastic wrapping that encloses goods (such as software packages), typically including a notice saying that by opening the wrapping, the purchaser agrees to the terms and conditions enclosed.[83] Shrink-wrap agreements are most common in the market of goods (including goods with digital elements) but may also occur when purchasing digital content

78 This acknowledgement is required in the context of Article 8(2) of the Consumer Rights Directive as one of the formal requirements for distance contracts.

79 Schulze, Staudenmayer (n 12) 163; Spindler, 'Digital Content Directive and Copyright-Related Aspects' (n 33) 129.

80 Schulze, Staudenmayer (n 12) 166.

81 Kārklis (n 54) 25.

82 Gregory Klass, 'Empiricism and Privacy Policies in the Restatement of Consumer Contract Law' (2019) 36(1) Yale Journal on Regulation 45, 52 <https://openyls.law.yale.edu/handle/20.500.13051/8282?show=full> accessed 11 December 2021.

83 Lynden Griggs and others, *Commercial and Economic Law in Australia* (3rd edn, Wolters Kluwer 2018) para 662; Alan Davidson, *The Law of Electronic Commerce* (Cambridge University Press 2019) 67.

if the tangible medium supplied to the consumer serves exclusively as a carrier of digital content (Article 3(3) DCD). For example, this situation would apply where a USB or a CD (covered in a wrapping) contains an installable computer operating system or video game. Similar to shrink-wrap agreements are *box-wrap* agreements, which involve opening a box as a sign of assent to the terms of the contract. In both cases, the contract is packaged with the product,[84] and, accordingly, they would be subject to the same conclusions.

54 *Click-wrap agreements* are a method of including terms and conditions in an online contract, i.e., formed on the internet. This type of agreement differs from a shrink-wrap agreement, as in the case of a click-wrap agreement, the user assents to a list of terms by clicking an onscreen button marked, for example "Agree", "I accept", "I consent" or similar. A click-wrap agreement has the advantage of allowing the user to read the specified term(s) before consenting.[85]

55 *Browse-wrap agreements* are used by many websites and consider that the act of browsing the website constitutes acceptance of their terms.[86] These terms and conditions, placed somewhere on the website, are accessible through a hyperlink and will regulate the relationship between the parties despite consumers likely never having seen them.[87] Browse-wrap agreement is by nature a questionable form of agreement[88] and has been critically viewed by the courts, including those established in third countries. As noted by Momberg, in *Specht v. Netscape Communications Corp.* an arbitration clause included in a browse-wrap contract was declared unenforceable. In that case, the browse-wrap link stated "Please review and agree to the terms of the *Netscape SmartDownload* software licence agreement before downloading and using software", but users were not required to click on that link as a condition of downloading Netscape's software. The Court decided that users were not bound by *Netscape*'s licence because they had not viewed the licence agreement and, therefore, they had not assented to the contract. In other words, downloading a software does not mean that the user agrees to terms that they are not reasonably aware of.[89]

56 *Sign-in-wrap agreements* are similar to browse-wrap agreements. In a sign-in-wrap agreement, the user is presented with a button or link to view the terms of use. Unlike click-wrap agreements, these agreements do not have an "I accept" or similar box/button (i.e., they do not require positive action by the user). Instead, they usually contain language to the effect that, by registering for an account, or signing into an account, the user agrees to the terms of service which they can navigate from the sign-in screen.[90] Compared to browse-wrap agreements, sign-in-wrap agreements actually give consumers a chance to read the terms offered by the trader before the consumer is considered to have consented to them.

57 Out of all these forms of agreements, only *click-wrap agreements* could meet the requirements contained in Article 8(5) DCD. Firstly, the problem with *shrink-wrap agreements* (and *box-wrap agreements*) is that the terms contained in them are meant to be binding on the consumer even though they are unknown at the time the contract is entered into, thereby not fulfilling the precondition that information must be provided not later than at the time of conclusion of contract. Similarly, a separate acceptance cannot be established since the act of opening a wrapping is understood as simultaneous acceptance of all terms and conditions. Furthermore, since these terms are unknown to the consumer, it cannot be established that consumer unequivocally intended to agree to the specific deviations. Secondly, a *browse-wrap agreement* would manifestly not meet a number of preconditions envisaged by Article 8(5) DCD, including "specifically informed" (information is not sufficiently clearly and transparently brought to the consumer's attention), as well as "separate" and "express acceptance" since it requires acceptance separately from other statements or agreements and by way of active and unequivocal conduct (express acceptance under Article 8(5) DCD cannot be implied). Thirdly, a *sign-in-wrap agreement* does not meet the precondition of "express acceptance" since such acceptance cannot be implied, and consumer might already have signed in before even considering purchasing a specific digital content/service. In addition, this agreement does provide for "separate acceptance" from other

84 Rodrigo Momberg, 'Standard Terms and Transparency in Online Contracts' in Alberto De Franceschi, *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution* (Intersentia 2016) 192.

85 Davidson (n 81) 68.

86 Griggs (n 81) para 662.

87 Marco Loos, Joasia Luzak, 'Update the Unfair Contract Terms Directive for Digital Services' (Study requested by the European Parliament's Committee on Legal Affairs (JURI) European Union 2021) 17 <www.europarl.europa.eu/RegData/etudes/STUD/2021/676006/IPOL_STU(2021)676006_EN.pdf> accessed 11 November 2021.

88 Momberg (n 82) 195.

89 ibid.

90 Gordon Hughes, 'Enforceability of Contract Terms Displayed on Social Media' in Marita Shelly, Margaret Jackson (eds), *Legal Regulations, Implications, and Issues Surrounding Digital Data* (1st edn, IGI Global 2020) 9.

statements contained in the sign-in-form (such as standard terms, privacy policy, cookies policy, etc.). Additionally, the criterion "information about the deviation must be provided not later than at the time of conclusion of the contract" is to be understood so that the consumer needs to be informed before concluding a contract. This criterion would not be fulfilled by arguments that the consumer signed into the trader's website two years ago and therefore has been properly informed about deviations regarding each of the trader's products/services and the consumer has accepted these deviations by signing into the website.

58 As regards to *click-wrap agreements*, they are similar to the possible forms of deviation mentioned in Recital 49 of the preamble to the DCD "ticking a box, pressing a button or activating a similar function". It is noted in legal literature that the formerly used ways to incorporate restrictions of intellectual property law in contracts such as "click-wrap" or "shrink-wrap" contracts can no longer be used because an explicit and separate agreement is necessary.[91] In a practical sense this statement would usually be correct since end-user licence agreements are normally drafted similar to general terms and conditions—without requiring separate and express consent to author-imposed limitations/restrictions regarding the specific digital content/service. But in a theoretical sense "click-wrap" agreements could certainly be used to fulfil the conditions of Article 8(5) DCD.

59 For example, a trader may include the text below together with the following checkboxes:

> "Limited liability company 'ABC' has included in the computer program 'ABC' a system of copyright protection (technical protection measures), which prevent any reproduction or transfer of the computer program 'ABC' to a third party. By clicking on the following boxes and purchasing the computer program, the I accept that I waive my right to:
>
> **[ ]** make private copies;
>
> **[ ]** make back-up copies;
>
> **[ ]** transfer (including selling or lending) the program to third parties.

60 This purely illustrative example generally satisfies the "specifically informed", "particular characteristic", and "separately accepted" preconditions. To ensure that the "express acceptance" condition is complied with, these boxes are not previously "checked" or activated automatically by agreeing to the general terms and conditions. Pursuant to Article 8(5) DCD, the above text with checkboxes would be included not during installation phase of the computer program but before the purchase of the program is finished.

61 This way, if the consumer wants to make a private copy, back-up copy or sell the computer program to a third party (in accordance with the conditions laid down in *UsedSoft GmbH v Oracle International Corp*[92]) but is unable to do so in practice because of the technical protection measures used, no lack of conformity can be established within the meaning of Article 8(1) and (2) DCD, and the consumer is not entitled to the remedies provided for in that Directive (which would be transposed into national law). If, however, the same text was included in the trader's general terms and conditions which would need to be scrolled through with an "I accept" checkbox at the end, consumer would be entitled to remedies, as the "separate acceptance" (from other statements or agreements) precondition would not be fulfilled. Whereas if general terms (inter-alia containing deviations) were included in a hyperlink with an "I agree" checkbox next to it, the precondition "specifically informed" would also not be met.

62 Thus, although the legal literature sources do not contain a detailed assessment as to which forms of obtaining consent are in conformity with Article 8(5) DCD, the authors of this article support the view expressed by *Staudenmayer* that "clickwrap agreements could fulfil the conditions of this provision, while browse-wrap or shrink-wrap agreements would not".[93] However, it should be clarified that click-wrap agreements only allow for the possibility to fulfil the preconditions contained in Article 8(5) DCD, but *in itself* neither fulfil nor violate them (it still needs to be examined whether all the preconditions of Article 8(5) DCD are met).

63 Finally, to answer the question as to how a trader in a physical shop could provide for deviations according to Article 8(5) DCD, the essence would likely be similar to click-wrap agreements—there could be an additional agreement or a marked paragraph in the text of the contract for each deviation, which would need to be either signed or otherwise separately accepted (e.g., by checking a box, putting a "+" or "x" sign into it by hand) before the contract is concluded[94]. However, even a trader that uses such a

91 Sein, Spindler (n 49) 365, 374.

92 Case C-128/11 *UsedSoft GmbH v Oracle International Corp* [2012] ECLI:EU:C:2012:407.

93 Schulze, Staudenmayer (n 12) 166.

94 Haslinger/Nagele Rechtsanwälte GmbH, 'The New Warranty Law – Everything Clear?' (Haslinger/Nagele Rechtsan-

form must comply with the requirements of Article 8 (5) DCD (described in more detail in Section 2 above) regarding the *content* of the deviation.

D. Conclusion

64 The present article deals with the understanding of the EU policy concerning a deviation from objective requirements for conformity with a contract of digital content or digital service. This EU policy is encapsulated in Article 8(5) DCD and is considered as an exception from the general regulation for ensuring conformity with the contract of digital content and digital service. The permitted use of the discussed deviation is based on six preconditions from Article 8(5) DCD that should be established cumulatively and interpreted narrowly and strictly. These preconditions are as follows: a deviation may solely concern the objective requirement; the consumer must be specifically informed about the deviation; information about the deviation must be provided not later than at the time of conclusion of the contract; the particular characteristic of the deviation must be indicated; the consumer must expressly accept the deviation; and the consumer must separately accept the deviation. The article demonstrates that traders could easily use a permitted deviation from objective requirements in their proposed and concluded transactions as fulfilment of these preconditions in general is relatively easy. At the same time, the article argues that traders could not use the deviation in all possible instances. For instance, it would not be permitted to deviate from any other trader's duty under the DCD as well as EU data protection legal acts. There, the consumer would be able to seek remedies when lack of compliance with the requirements of Regulation (EU) 2016/679 constitutes lack of conformity with requirements of digital content or digital service. At the same time, the article raises serious concerns about possible abuse of a deviation permitted under Article 8(5) DCD by traders. In this regard, the article analyses five frequently used forms of agreements (shrink-wrap, box-wrap, click-wrap, browse-wrap, and sign-in-wrap) to evaluate whether they fulfil above preconditions, arguing that only click-wrap agreements could meet the requirements contained in Article 8(5) DCD, although not automatically. This conclusion is discussed together with a hypothetical example of a statement in the form of a click-wrap agreement that could possibly be used to satisfy the preconditions envisaged by Article 8(5) DCD. However, the potential abuse issue requires further studies analysing existing practices in respect of each precondition separately. Likewise, further studies are necessary to investigate deeper interrelation with other EU legal instruments such as regulation of unfair contract terms or e-commerce which is characterised in the present article as far as it is possible considering the theme of the article.

Note: The research reflected in this article was financed by the program of Fundamental and Applied Research Projects within the project Strengthening of High Level of Consumer Protection in the Digital and Data Age: The Transposition of the New Consumer Sale Directives Into Latvian Legal System (project No lzp-2020/2-0265) funded by the Latvian Council of Science.

wälte GmbH 2021) <www.haslinger-nagele.com/en/news/the-new-warranty-law-everything-clear/> accessed 18 November 2021.

Attention, here comes the EU Data Act!

A critical in-depth analysis of the Commission's 2022 Proposal

by **Matthias Leistner and Lucie Antoine***

Abstract: The paper outlines the main elements of the 2022 EU Commission's Data Act Proposal. The proposal is the apex of the Commission's recent regulatory initiatives in the field of platforms and the data economy. The paper provides for a critical in-depth analysis of the proposal that forms the basis for concrete recommendations to improve the current text, all guided by the aim to help this legislative initiative to reach its objectives by curbing it, where necessary, and at the same time making it more focused and efficient.

Recommended citation: Matthias Leistner and Lucie Antoine, Attention, here comes the EU Data Act! A critical in-depth analysis of the Commission's 2022 Proposal 13 (2022) JIPITEC 339 para 1

A. Introduction and general remarks

1 On 23 February 2022 the Commission has published its proposal for a "Regulation on harmonised rules on fair access to and use of data (Data Act)" [1]. The proposal is the apex of the Commission's regulatory initiatives for the data economy, with the Digital Markets Act, the Data Governance Act, the Digital Services Act and the AI Act already being adopted or close to actual final adoption.[2]

2 Although this most recent proposal of the current Commission has its main focus (and certainly the largest degree of intended regulatory impact) on the IoT sector, certain elements of this ambitious legislative project also go beyond the IoT sector specifically. The Data Act follows the objectives to

* Prof. Dr. Matthias Leistner, LL.M. (Cambridge), Professor and Chairholder for Civil Law and Intellectual Property Law with Information Law and IT-Law, Ludwig Maximilian University Munich; Lucie Antoine, Research Assistant and PhD Candidate, Ludwig Maximilian University Munich. This paper goes back to the authors' study 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022) requested by the European Parliament's Committee on Legal Affairs, published on 3 May 2022, available at <https://ssrn.com/abstract=4125503>. The following summary contains but the absolutely inevitable references; comprehensive references can be found in the study.We thank Heike Schweitzer, Josef Drexl, Wolfgang Kerber, Axel Metzger, Ansgar Ohly, Louisa Specht, Gerald Spindler, Tatsuhiro Ueno and Herbert Zech for their consistently helpful comments and valuable ideas in our various discussions of the subject.

1 European Commission, Proposal of 23 February 2022 for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final (hereinafter "Data Act").

2 Data Governance Act: promulgated in the Official Journal on 3 June 2022, OJ L152/1; Digital Markets Act and Digital Services Act: adopted by European Parliament on 5 July 2022, Council's final approval for the Digital Markets Act on 18 July 2022; AI Act: ongoing proceedings in European Parliament and Council.

open certain markets related to the IoT and cloud sector, to define explicit provisions for data sharing on contractual basis as well as to reduce technical barriers and allow B2G data access in exceptional situations (such as the recent pandemic). In order to establish "harmonised rules on fair access to and use of data" it is a remarkable achievement that the Data Act proposes *institutional, decentral structures (which from our viewpoint are typical for private law claims and should also be enforced accordingly)* for data access, sharing, portability, and use, thereby going way beyond the current legal framework focused primarily on (more centralised) data and services governance.

3 The Data Act shall introduce five new instruments: first, the *user's right* – applying in B2C and B2B relations – to *access* and *use data* generated by IoT products and to *share* such data with third parties[3]; second, an *unfairness test for B2B contract clauses* on data sharing which have been imposed on SMEs[4]; third, a framework for *B2G data sharing* based on exceptional need[5]; fourth, provisions on *switching between cloud service providers,*[6] and, fifth, safeguards against *unlawful access to non-personal data held in the Union in international contexts*[7].

4 Some of these proposed instruments (data sharing, mandatory unfairness control of B2B contracts, cloud and edge service provider switching), in particular because of their *sweeping scope* (B2C as well as B2B), their *mandatory character*, and the *central role of the user* concerning the access and sharing rights, require fundamental scrutiny in light of the involved *impact on the principle of contractual freedom* as well as with regard to their impact on *free competition* and their *prospective efficiency*. Also, certain "fine-tuning" is necessary with particular regard to the objective to *reduce market entry barriers for newcomers* (or at least not to erect new or heighten existing barriers to market entry), in the markets for IoT products and cloud services.

5 In the following, we summarise some analytic and critical remarks on the proposal which to us seem to be most imminent for the further legislative discussion that is meanwhile well underway. On that basis, we provide for a list of recommendations to improve the current text of the proposal.

3 Articles 3–12.

4 Article 13.

5 Articles 14–22.

6 Articles 23–26.

7 Article 27.

B. Overlaps, balances and consolidation

6 As a general remark on legislative technique, concerning the entirety of the currently planned instruments of the "*data package*"[8], the relation between the different existing and in particular the newly proposed instruments, their purposes and their content *needs to be* further clarified and *consolidated*. If the involved intricate *overlap, consolidation* and *balancing* issues remain unsolved or unclear, they will be a major factor causing legal uncertainty (chilling effects) as well as possibilities for opportunistic behaviour in the upcoming years.

7 Elsewhere we have made several proposals concerning such overlap, consolidation and balancing issues which we have addressed mainly by proposing certain changes to the substantive provisions of the Data Act and by proposing certain avenues for adequate contextual delineation.[9] Also, we have made proposals in regard to necessary institutional consolidation in the area of public enforcement and its relation to *necessary private rights and enforcement mechanisms*, as otherwise there will be a manifest danger of overlapping and contradicting enforcement decisions of different competent authorities in different sectors, concerning both the level of the Member States and the level of the Union.

I. Relation to the GDPR

8 In particular, concerning the *processing of personal data*, the Data Act takes into account the entire "toolbox" of the GDPR by referring to any legal basis foreseen in Article 6 GDPR (or Article 9 GDPR) instead of relying solely on the data subject's consent. Requiring consent in the sense of Article 6 (1) (a) GDPR – or under the even stricter standards of Article 9 (2) (a) GDPR – in each case would indeed considerably reduce the practical efficiency of the new data access and sharing rights due to the high standards, legal uncertainty and practical difficulties with the GDPR's concept of consent[10], in particular

8 In particular the Data Governance Act, the Digital Markets Act and the Digital Services Act.

9 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 73 et seq.

10 See for instance Andreas Sattler, 'Autonomy or Heteronomy – Proposal for a two-tier interpretation of Art. 6 GDPR' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?*

in regard to dynamically involving use scenarios as well as for uses based on relevant sensitive data. However, Article 6 (1) (f) GDPR as the obvious main alternative route to legal processing of IoT data in private settings, poses equally problematic issues concerning the *lacking legal certainty* with regard to the balancing of interests.[11] In this overall context it should always be borne in mind that the GDPR expressly pursues two – equally important – objectives consisting in the protection of natural persons with regard to the processing of personal data *and* the free movement of personal data.[12]

9 In the context of the proposed Data Act, the broad definition of personal data in Article 4 (1) GDPR – which at the same time entails a *negative* definition of *non-personal* data – should be put under scrutiny.[13] Large parts of the data processed in the data-driven economy relate (at some point) to an identifiable natural person or at least cannot always be clearly distinguished from non-personal data when larger or combined datasets are concerned.[14] The same applies for data generated by IoT products: Location data (e.g. connected cars), use data (e.g. smart home devices) or search queries "asked" to a virtual assistant can qualify in many cases as personal data in the sense of the GDPR.[15] It seems necessary to *fundamentally specify the scope and impact of the GDPR in the sector*,[16] i.e. to at least consider *amendments to the definition of personal data* in such scenarios in a way which is in line with the objective to improve the *free flow of sufficiently anonymised or manifestly publicly available data*, as well as to specify and clarify the specific possibilities to *balance* the legitimate objectives behind the Data Act with the fundamental right to protection of personal data by interpreting the respective heads for lawfulness of processing in Article 6 GDPR in accordance with the legal duties set out in the Data Act.

10 In this regard, first, we propose certain ways to achieve the necessary and proportional balance, while preserving effective protection of personal data, and which can be implemented by *certain clarifications in the Data Act proposal* and without changing the text of the GDPR, e.g. by recognising Article 4 (1) and Article 5 (1) of the Data Act as "legal obligation" in the sense of Article 6 (1) (c) GDPR. Second, apart from these detailed proposals, one more fundamental aspect will be central to genuinely improve the conditions for businesses in the internal market in that regard in the future. As the Data Act aims at reducing the practical and technical barriers for data sharing by introducing standards for interoperability and other relevant technical features, in the context of the GDPR this could also be an occasion to further implement legally reliable *technical and organisational standards for the sufficient anonymisation of data* – ideally by complementing this with at least a rebuttable presumption of sufficient anonymisation when businesses comply with such established anonymisation standards.[17]

II. Relation to intellectual property rights and trade secrets protection

11 As regards the necessary balance with IP protection and trade secrets, the proposed provisions of the Data Act consequently and rightly focus primarily on potential overlaps with trade secret protection (particularly Chapter II, III) and with the sui generis right of database makers.[18]

(Nomos/Hart 2020) <https://www.jura.uni-muenchen.de/personen/s/sattler_andreas/veroeffentlichungen/autonomy-or-heteronomy.pdf>.

11 Andreas Sattler, 'Autonomy or Heteronomy – Proposal for a two-tier interpretation of Art. 6 GDPR' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Data as Counter-Performance – Contract Law 2.0?* (Nomos/Hart 2020), 16; see further Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data* (Mohr Siebeck 2021), 275 et seq.

12 See title of the GDPR; Article 1 GDPR and Recital 13 GDPR.

13 Already Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10 Law, Innovation and Technology 40.

14 See e.g. European Commission, Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, COM(2019) 250 final, 4 et seq.

15 Acc. to Article 4 (1) GDPR "personal data" refers to any information relating to an identified or identifiable natural person.

16 See also Inge Graef, Martin Husovec and Jasper van den Boom, 'Spill-Overs in Data Governance: Uncovering the Uneasy Relationship Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes' [2020] Journal of European Consumer and Market Law 14 et seq.; Inge Graef, Raphael Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation' [2019] European Law Review 605 et seq.

17 See further Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 65. The German Data Ethics Commission has proposed to introduce a respective system, see its 'Opinion' (2019), 131 <https://www.bmi.bund.de/EN/topics/it- internet-policy/data-ethics-commission/data-ethics-commission-node.html>.

18 See already Matthias Leistner, 'The existing European IP

12 In principle, from the viewpoint of legal technique, the *relation to trade secrets* is satisfyingly addressed in Article 4 (3) and Article 5 (8).[19] In the context of new access, sharing, and use rights we propose however to distinguish between (more sensitive) business information pertaining to specific market information or information about the very parameters of competition as such on the one hand and general technical or creative know-how on the other hand in order to strike a *more precise balance* between access and use interests on the demand side and the interest of protection on the rightholders' side taking into account the public interest in free and undistorted competition.[20]

13 From our viewpoint – for the sake of legal certainty – it should also be *clarified that the FRAND "licences" (as they are foreseen in Article 8) will also have to define and cover necessary and justified use acts in regard to trade secrets*. This would be of mainly clarifying character as the necessary justification already follows from Article 4 (3) and Article 5 (8). However, it would also allow to take the character of certain data as trade secrets into account when further specifying the terms and range of FRAND compensation.

14 As a tool for complementing the Data Act, *(non-mandatory) model contract terms* for the licensing of trade secrets and for allocating the "ownership" of trade secrets in cooperative data sharing networks should be developed in order to reduce legal uncertainty.[21]

III. Database sui generis right (Article 35)

15 The database sui generis right has a difficult role in the context of data access, use and sharing as it has the potential to intensify de facto control over data, to aggravate existing access problems and to lead to hold-up issues in certain situations.[22]

16 These issues are addressed (in a rather limited, cautiously delineated sector specific way) by Article 35. Pursuant to Article 35, the sui generis right "does not apply to databases containing data obtained from or generated by the use of a product or a related service".

17 While the explicit clarification that machine-generated databases do not fulfil the conditions of the sui generis right seems acceptable as a bright line rule to reduce the significant legal uncertainty concerning the conditions for protection in the sector,[23] the wording and legal technique of Article 35 should be refined: Apart from certain necessary technical clarifications of the provision's wording[24] it is recommended that it should be clarified (in the sense of a *Union law pre-emption doctrine*) that within the scope of the Database Directive, if a given database does not fulfil the conditions for protection, Member States shall be precluded to protect such a database on different grounds[25] (such as *parasitisme* or unfair competition protection against misappropriation, unless additional factors, such as consumer confusion, warrant such additional unfair competition law based protection).

18 In fact, the restatement that machine-generated databases do not qualify for protection under the sui generis right solves some of the problems in regard to the conditions of protection by providing

rights system and the data economy' in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data access, consumer interests and public welfare* (Nomos 2021), 209, 222 et seq. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3625712>.

19 More sceptical Weizenbaum Institute for the Networked Society, 'Position Paper regarding Data Act' (2022), 12 et seq. <https://www.ssoar.info/ssoar/handle/document/79542>.

20 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 64.

21 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 64.

22 Comprehensively, Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 59 et seq.

23 With a rather critical view, Estelle Derclaye and Martin Husovec, 'Why the sui generis database clause in the Data Act is counter-productive and how to improve it?' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4052390>.

24 In detail Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 120. See also Max Planck Institute for Innovation and Competition, 'Position Statement of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022), paras. 258 et seq.; European Copyright Society, 'Opinion of the European Copyright Society on selected aspects of the proposed Data Act' (2022), 2 et seq. <https://europeancopyrightsocietydotorg.files.wordpress.com/2022/05/opinion-of-the-ecs-on-selected-aspects-of-the-data-act-1.pdf>.

25 Estelle Derclaye and Martin Husovec, 'Why the sui generis database clause in the Data Act is counter-productive and how to improve it?' (2022), 2 et seq.

for a bright line non-conflict rule for certain cases. However, many of the problems we have identified in our study[26] and in earlier publications[27] are not addressed by this very targeted provision. In this regard there is *still need for action.*[28]

19 With regard to the *Database Directive*, we therefore *propose* (beyond the Proposal for a Data Act)[29]

- to substantially *shorten the term of protection*;
- to *exclude* databases of *public bodies* from sui generis protection;
- to *reform the exceptions and limitations;*
- to introduce a *compulsory licencing regime*;
- to develop (non-mandatory) *model contract terms* for the allocation of sui generis rights in the context of data related bilateral and/or network contracts.

C. The role of private law enforcement

20 In general, the Data Act is characterised by broadly formulated standards ("general clauses") and many new legal concepts and terms. These provisions, terms and concepts will have to be further clarified and specified in the upcoming years. Since the Data Act – in particular in its central part on the introduction of new data access and sharing rights for users of IoT devices – assigns an important role to private agents' requests and bilateral or tri-lateral (contractual) agreements as a private law institution,[30] the task to specify the proposed provisions should centrally lie with *private law courts*, thus should be addressed within *private law enforcement* and by private law courts instead of by a system of different intersecting public authorities.[31] Therefore, in the interest of effective and proportionate enforcement it is *recommended to lay down express rules on private rights and litigation* and, more generally, on the substantive and procedural relationship between the public enforcement mechanisms, foreseen in Articles 31 et seq., and private litigation as the main pillar of putting this new regulatory framework into practice.[32]

D. The proposed rules on B2C and B2B data access and sharing

21 From our viewpoint, the new system of proposed B2C and B2B data access, sharing and use in Chapter II and III is the central element of the Data Act. Besides the already mentioned necessity of *instruments for private enforcement*, our main concerns relate, first, to the *horizontal scope* and *generalising mandatory law character* of the proposed data access and sharing system, secondly to certain *inherent limitations* of that system, and thirdly to the *central role assigned to the users* in that new proposed system.

I. Scope and objective

22 The provisions proposed in Chapter II and III granting access and use rights for users and the right to share

26 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 49 et seq.

27 Matthias Leistner, 'Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), Trading Data in the Digital Economy: Legal Concepts and Tools (Nomos 2017), 27 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3245937>; Matthias Leistner, 'The existing European IP rights system and the data economy' in German Federal Ministry of Justice and Consumer Protection and Max Planck Institute for Innovation and Competition (eds), *Data access, consumer interests and public welfare* (Nomos 2021), 209; Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data* (Mohr Siebeck 2021), 410 et seq.

28 See also Max Planck Institute for Innovation and Competition, 'Position Statement of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022), para. 265.

29 Comprehensively Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 59 et seq.

30 Also highlighting the private law character, Dirk Staudenmayer, 'Der Verordnungsvorschlag der Europäischen Kommission zum Datengesetz' [2022] Europäische Zeitschrift für Wirtschaftsrecht 596.

31 Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022] Gewerblicher Rechtsschutz und Urheberrecht 953, 960 et seq.

32 Similarly, Max Planck Institute for Innovation and Competition, 'Position Statement of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022), paras. 8, 240 et seq.; Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022] Gewerblicher Rechtsschutz und Urheberrecht 953, 960 et seq.

data with third parties in regard to data "generated" by IoT products and related services are designed to constitute generally applicable, basic rules for all sectors in this field.[33] Due to this *horizontal character covering the entire "sector" of IoT products*, the proposed provisions, on the one hand, have a very broad scope of application – from industry to private use of connected products (*B2C and B2B alike*). On the other hand, in regard to the relevant data, the scope of the Data Act is limited to "data generated by the use of products or related services" and thus does not substantially cover any *inferred or derived data*.[34] Furthermore, the access to, use and sharing of these data is limited to uses *which do not compete* with the IoT product from which the data originate.

23 Consequently, these provisions can neither be consistently construed as addressing specific situations of abuse of dominant market positions (or other situations of specific market failure) nor as addressing specific situations of information asymmetry, imbalances in negotiation power (or other situations of specific contract failure). This is because under the perspective of situation-specific market failure or situation-specific contract failure, the scope and structure of these mandatory provisions would be at the same time both, too broad as well as too narrow. The scope of *mandatory law regulation is too broad* as these provisions obviously also apply in situations where no information or market power asymmetry can be identified at all. This is because, in particular *in B2B settings*, the user of the IoT product might as well be better informed and more experienced than the IoT product provider and data holder, and might also have a relatively stronger market position resulting in a relatively stronger negotiation position. In such a setting, broadly applicable, *sector-wide mandatory* provisions on data access and sharing cannot be justified as a corrective for a specific situation of market or contract failure. On the contrary, in some of these situations they might outright interfere with efficient, contract-based allocation of data, as because of their mandatory character, they prevent any reservation of data-related aftermarkets based on factual data control or contracts, even in situations, where this would be the efficient solution (e.g. a small newcomer (not a dominant undertaking) in the IoT producers' market could otherwise not enter the market at all) and would therefore benefit both parties to a respective contract.[35] At the same time, the *scope is too narrow*, as we have identified situations of potential market failure in regard to the access to aggregated data, and, namely structured data, i.e. *contextualised, standardised data*, as the genuine main bottleneck for the development of many data oriented services at the moment.[36] However, for such situations, the new provisions do not really provide a comprehensive remedy, because their *field of application is limited to volunteered and observed data* and their fundamental structure is oriented towards the access to and sharing of individual-level data[37] (which at best indirectly and inefficiently helps to remedy situations where access to aggregate, contextualised datasets would be necessary and justified).[38]

24 Instead of remedying specific situations of market or contract failure, the newly proposed provisions on data access, use and sharing in the Data Act are based on the general assumption that access to and use of IoT data in order to provide new products or services (in particular, but not only, maintenance, repair and other aftermarket services or products) will liberate aftermarkets and other new markets through the provision *and* commodification of data access rights, and will thus, in their total effect, create more benefits through enhanced dynamic efficiency than costs[39] (through the undoubted interference with static and dynamic efficiency in certain situations, in particular B2B situations). The objective is thus to provide an *institutional framework*

33 Data Act, Explanatory Memorandum, 5.

34 Recital 14, 17.

35 In B2B relationships, situations in which – due to particular investments etc. – a limitation of the user's access and use rights (by means of an agreement) may seem reasonable to both of the parties are undoubtedly conceivable, see Heike Schweitzer and Martin Peitz, 'Ein neuer europäischer Ordnungsrahmen für Datenmärkte?' (2018) Neue Juristische Wochenschrift 275, 280.

36 Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 25; from a competition law perspective Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era' (2019), 75 et seq.

37 First case group as defined by Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era' (2019), 75.

38 See also Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 12 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4080436>.

39 Cf. European Commission, 'Impact Assessment Report, Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' (2022), Staff Working Document, SWD(2022) 34 final, 43 et seq.; Deloitte and others, 'Study to support an Impact Assessment on enhancing the use of data in Europe' (2022), 270 et seq. <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act>.

for the development of certain new markets, in particular in regard to new products or services in markets related to the distribution of *IoT products* (such as repair, maintenance and other related markets), through generally opening and institutionally structuring hypothetical or actual upstream markets for the access to the necessary data generated by such products. This new regulatory approach, which goes way beyond the existing, comparably problem-specific approaches in competition law, consumer protection law and sector-specific regulation is at the same time limited in scope to IoT products and related (after)markets as well as in regard to upstream markets for volunteered or observed) data generated by the use of such products. Thus, while the regulated sector (use of any IoT product, B2C and B2B) is very broad and unspecific (*broad horizontal field of mandatory regulation*), the affected data categories (only volunteered and observed data, i.e. no inferred data) as well as the statutorily enabled uses (use for developing competing products is expressly excluded) are remarkably limited (*limited vertical depth of regulation*).

25 However, even in light of these crucial limitations, it has to be borne in mind that the sectors in which data-collecting IoT products are used, *vary widely*, and thus, the conditions on the relevant markets, the relationship between the actors and the amount and categories of the co-generated data differ significantly. Also, the aspect of possible new *barriers to market entry* (or at least chilling effects) for original producers which have not yet implemented IoT components in their products at all (and the general aspect of not chilling potential competition), should not be lost out of sight. General competition law by and large only sanctions market dominant firms for exclusionary conduct by leveraging their dominance on a primary market to a secondary market (although of course recent reforms, such as the most recent reform of the German Competition Act, have already cautiously departed from this approach inter alia in the context of the data economy[40]). By contrast, the Data Act might be interpreted as a decision for generally opening (hypothetical) markets in the IoT sector through a *general ex-ante (market design) approach*, since from the viewpoint of the Commission the existing, competition law-based case-by-case analysis has turned out not to be effective enough to generally foster the development of certain data-driven markets. Even following this assumption, it would however also have to be shown, whether a generalised *mandatory law* framework (extending to all B2B-situations) is indeed required to reach this objective throughout the entire sector, whether solely opening secondary markets (by excluding data access, use or sharing in order *to compete* with the data holder) is sufficient and in particular, how such secondary markets shall be defined and delineated from situations of (direct) competition with the data holder in borderline cases. In that latter regard, the Data Act remains rather cautious, thus at the same time significantly limiting the impact of this new regulatory instrument for crucial case groups.

26 From our viewpoint, all this has three main general consequences resulting in two main policy recommendations. First, given the diversity of their field of application, the new provisions have to be re-evaluated with particular attention to their *scope* and necessary *flexibility* in particular through the use of flexible open-ended standards in the legislative text. Related to this on an instrumental level is the important question which institutional players shall specify these standards in the future as this will be crucial for the necessary balance between flexibility through the use of open-ended standards and fostering sufficient legal certainty through the specification of these standards in case law (this particularly also concerns the question of *private* and/or public *enforcement* and their relationship to each other).

27 Secondly, it has to be kept in mind that none of these new provisions should be designed, construed or applied in a way which puts disproportional *new cost burdens on newcomers* in the very markets the Data Act intends to open and incentivise (this particularly at least concerns necessary lenience in regard to SMEs as well as – again – the issues of the necessity of mandatory law, efficient enforcement and necessary legal certainty which might be endangered if overlapping, multi-institutional public law enforcement causes significant additional administrative and information costs, e.g. because of resulting legal uncertainty and additional bureaucracy). As a *policy recommendation*, these two aspects lead to a need to *reconsider the broad scope* of the proposed mandatory framework (possibly in favour of a more sector-specific approach) and/or to re-evaluate whether *mandatory rules* are indeed needed in those B2B constellations, where no manifest imbalance exists between the parties to the contract

28 Thirdly, one has to remain aware that *potential additional access problems* that have been identified and systematised in recent literature, go way beyond the specific field of certain data co-generated by IoT products and the opening of related aftermarkets for products or services which are not in direct competition with the data generating IoT product itself. This is especially true for access needs of competitors to complete datasets for competing in

40 Max Planck Institute for Innovation and Competition, 'Position Statement of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022), para. 36.

secondary markets (which might include inferred data), and access to large aggregated datasets (e.g., training data and other *inferred data*) of big data conglomerates for innovation purposes which might even lead to products or services which are in direct competition with the data generating product or service.[41] Due to the strict *exclusion of services*, data generated by the use of (online) services or platforms are not covered by the proposed Data Act. This sector is therefore hitherto only covered in the 'data package' by the proposed Digital Markets Act, albeit limited to data held by gatekeepers (i.e. the GAFAM companies plus presumably less than a handful of other gatekeeper platforms) and to specific market situations. Therefore, it will be necessary to design and construe the new provisions in the Data Act in a way which allows the Act to at least indirectly contribute to the solution of some of these (partly related) data access problems. Also, it has to be kept in mind that the mentioned *access problems*, in particular in regard to aggregated, contextualised or standardised data and *in regard to certain larger (not purely data-processing, but data-driven) services*, might need to be addressed, going beyond the limited data related rights vis-à-vis Big Tech companies in the proposed Digital Markets Act. By contrast, the Data Act proposal is primarily designed to enable data access and use by third parties in a particular sector and in regard to but one central use scenario (aftermarket services for IoT devices). This leads to the *policy recommendation* to reconsider the *limitation of the scope* of the Data Act's proposed access and sharing regulation to IoT-products and related services, to re-evaluate the exact extent of the principled *exclusion of inferred data*[42] as well as to reconsider the principled requirement of *non-competing use*.[43]

II. The proposed central role of the user

29 Generally, and in particular for B2B constellations, it also needs to be justified why the *user* should be in a *central role*. Whereas protecting *personal data* by means of strong subjective rights (as provided by the GDPR) is mandated by the fundamental right to protection of personal data, the need for allocating mandatory access, use and sharing rights in regard to non-personal data to the users as suggested by the Data Act, is less self-evident.[44] Allowing access to and use of data generated by IoT products and related services for *B2C relations* can also be seen as an expression of guaranteeing data sovereignty and "empowering" of private consumers in regard to perceived information asymmetries or other reasons for an assumed weaker bargaining position of private consumers.[45]

30 However, *in B2B constellations*, such allocation of non-personal data to the customers/users of IoT devices needs genuine justification. As we have explained, in B2B constellations, where the customer/user is not a consumer, such mandatory allocation of data access, use and sharing rights, cannot across the board be justified by the identification of specific situations of market or contract failure[46] – this would at best be possible for SME users vis-à-vis large IoT companies or for certain very specific sectors where empirical data clearly suggest the general actual or potential existence of such imbalanced situations. The Data Act goes beyond this, covering all B2B relations, where IoT products are used by businesses on the basis of sales, rental or lease contracts, alike. Thus, it seems that the mandatory allocation of data access, use and sharing rights to business users of IoT products is based on the perceived co-initiative and co-investment of such business users in the generation of the resulting use generated data through their actual use.[47] As for the allocation of exclusive rights in such data, it has been

41 Second and third case group as defined by Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era' (2019), 75 et seq.

42 Max Planck Institute for Innovation and Competition, 'Position Statement of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022), paras. 24 et seq.; Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022] Gewerblicher Rechtsschutz und Urheberrecht 953, 961.

43 Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 12; cf. Inge Graef and Martin Husovec, 'Seven Things to Improve in the Data Act' (2022), 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4051793>.

44 Max Planck Institute for Innovation and Competition, 'Position Statement of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' (2022), para. 49.

45 Data Act, Explanatory Memorandum, 13.

46 Similarly, Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 25.

47 Cf. Recital 6. The aspect of "co-generation" is also core element of the ALI-ELI Principles for a Data Economy, see particularly Principle 18 and the flexible factors proposed therein (American Law Institute and European Law Institute, 'ALI-ELI Principles for a Data Economy – Data Transactions and Data Rights', ELI Final Council Draft, (2021) <https://www.principlesforadataeconomy.org/fileadmin/user_upload/p_principlesforadataeconomy/Files/Principles_for_a_Data_Economy_ELI_Final_Council_Draft.pdf>).

decided by the ECJ in the context of the database sui generis right, that the mere generation of data in the course of another main business activity (i.e. as a spin-off of such a main business activity), shall not give rise to exclusive rights based on such more or less incidental generation of data.[48] As for B2B situations under the Data Act proposal, the crucial (and somewhat different) question is whether the contribution to the generation of data through use of IoT products in the context of another main business activity, should give rise to certain limited and non-exclusive access, use and sharing rights for the user.

31 Whereas certain contextual elements in the *acquis communautaire* (in particular the conception of minimum use rights of the lawful user in the Computer Programs[49] and the Database Directive[50]) can serve as a tentative model for the access, use and sharing rights for business users in the Data Act,[51] the crucial question remains whether the *initial allocation of such rights to the users* of the devices is efficient, when assessed in light of one of the main objectives of the Data Act, i.e. to create new markets for such data as a necessary precondition for the offer of new products and services in aftermarkets related to the originally distributed IoT product or its use. To answer this question, it will have to be considered, whether the users of such devices are sufficiently informed and incentivised to actually make use of their new rights, in particular also to share (and effectively market) them. In a rather limited field, i.e. the provision of specific new or at least cheaper or better services in aftermarkets, one might assume that the users as prospective customers of such services, might indeed be the best informed agents and might have sufficient incentives in order to initiate the necessary sharing of data by the data holder. At the same time effects, such as switching costs and inertia bias as well as the associated transaction costs, might well reduce the incentives of the users to effectively initiate data sharing. To make this envisaged regulatory system work, first, the relevant provisions of the Data Act must allow for *broad, non-static and transferrable as well as monetisable sharing claims* at least where trade secrets are not affected. Secondly – and more importantly – it will have to be considered whether the central (and to a certain extent "proto-exclusive") role of the users in regard to initiating and authorising upstream data sharing is indeed as such justifiable and sufficient to effectively foster the emergence of dynamic and diverse new data markets as a precondition of new data related products or services.[52]

32 In this context, it should also be kept in mind that the very generating, obtaining and observing of data generated by the use of a product or related service at the same time requires substantial ex-ante and continuous organisational, technical and financial efforts by the *data holders*. Also, in many situations, the data holders might be in a better situation to assess, negotiate and implement efficient data contracts, whereas the users' respective initiative and role seem less central and functional in that regard. In order to effectively incentivise data sharing, the role and legal as well as practical position of the *data holders (IoT producers and related companies) should therefore be equally taken into consideration, when regulating the sharing of such data on a non-exclusive basis* with third parties. In accordance with our analysis, we have made several proposals to achieve this goal in our study some of which we also list in our following main policy recommendations.

III. Necessary flexibility

33 *Article 41 foresees an ex-post evaluation of the Data Act* by the Commission *two years* after the date of its application with a particular view to certain adaptations of the central instruments of the Data Act. Indeed, such clause as well as any other provision injecting necessary flexibility and adaptability into the legal instrument seem highly recommendable in light of the very dynamic development of the regulated market sector. Article 41 in principle provides a coherent basis for the evaluation of the Data Act and possible future adaptation although one might consider, in the interest of increased flexibility, whether in addition the Commission should also be empowered to make certain necessary mere specifications of open standards in the Data Act by way of delegated acts. As for possible ex-post evaluation and data collection, we have noted certain essential aspects in our study which we have summarised at the end of our following list of main

48 C-203/02 *British Horseracing Board v Hill* [2004], ECLI:EU:C:2004:695, paras. 30 et seq.; C-46/02 *Fixtures Marketing v Oy Veikkaus* [2004], ECLI:EU:C:2004:694; C-338/02 *Fixtures Marketing v Svenska Spel* [2004], ECLI:EU:C:2004:696; C-444/02 *Fixtures Marketing v Organismos prognostikon*, ECLI:EC:C:2004:697.

49 Articles 5 and 6 Computer Programs Directive. Further on this aspect Matthias Leistner and Lucie Antoine, 'IPR and the use of open data and data sharing initiatives by public and private actors' (2022), 60.

50 Article 8 Database Directive.

51 Cf. Matthias Leistner, Lucie Antoine and Thomas Sagstetter, *Big Data* (Mohr Siebeck 2021), 65 et seq., 444 et seq.

52 Cf. Wolfgang Kerber, 'Governance of IoT Data: Why the EU Data Act will not fulfill its objectives' (2022), 2 et seq.; Rupprecht Podszun and Clemens Pfeifer, 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission' [2022 Gewerblicher Rechtsschutz und Urheberrecht 953, 961.

policy recommendations.

E. Recommendations

34 In sum, we propose with regard to the *Data Act in general*,

- to *clarify and strengthen the role of private law enforcement*;
- to make the proposed public enforcement structures *optional* to the Member States and to streamline them, at best by a *one-stop shop* approach including a European "meta-authority"[53] for data related topics;
- to thoroughly assess the *coherence of the Data Act with the entire "data package"* and the existing legal framework;
- to include provisions on the applicability of the Data Act in *multipolar settings* (e.g. data sharing networks) and to re-evaluate whether the current regulatory approach is well equipped to cover such situations;
- to *develop accompanying non-mandatory model contract terms*.

35 With regard to the proposed rules on *B2C and B2B data access, sharing, and use* we propose

- to *reconsider their broad scope of application and/or to critically evaluate the necessity of the mandatory character of the proposed system in B2B constellations* where no imbalance of the parties is present;
- complement the central role of the user with a *regulation of the position of the data holders*;
- to assess whether access to data generated by the use of *services* is already comprehensively covered by the proposed Digital Markets Act and to consider the *extension of the scope of the new data access, sharing and use rights to certain larger (not purely data-processing, but data-driven) services* which are not gatekeepers under the comparatively strict thresholds of the proposed Digital Markets Act;
- to re-evaluate the exact extent of the principled *exclusion of inferred data*;
- to reconsider or at least to specify the conditions of the prohibition to use the respective data for developing a *competing product*;
- to consider whether the obligations to make data available set forth in the Data Act *could qualify as "legal obligation" in the sense of Article 6 (1) (c) GDPR*, and, in the future, to consider further delineating the notion of "personal data", at best by developing *technical and organisational standards for anonymisation* and by introducing a *rebuttable presumption* of anonymisation when the respective standards are met;
- to clarify that *FRAND "licences" will cover necessary and justified use acts in regard to trade secrets*.

36 With regard to the *unfairness test for B2B contract terms* on data sharing we propose

- to specify that the fairness test does not apply to constellations in which a *micro or small business* is the imposer of a contract clause;
- to add the condition that a *gross imbalance* in the parties' rights and obligations arising under the contract must be the result of the unfair term.

37 With regard to *B2G data sharing* based on exceptional need we propose

- to reconsider whether the provisions should be *extended to small and micro-sized enterprises*.

38 With regard to the provisions on *switching between cloud and edge services* we propose

- to foresee an *exception for SMEs as providers*, at least for B2B relations;
- to revise the *relation to the proposed Digital Markets Act*;
- to *clarify the concept of "functional equivalence"*.

39 With regard to the provisions on *interoperability* we propose

- to *extend the scope of the general principles* applicable to the operators of European data spaces to also guide future general standardisation processes in regard to cloud portability, data access and data sharing.

40 With regard to *Article 35 on the database sui generis right* we propose

- to primarily "refine" the wording of the provision in order to clarify that databases which fall into the scope of the Database Directive but

53 Weizenbaum Institute, 'Position Paper concerning Data Act – Inception Impact Assessment' (2021), 12 <https://www.weizenbaum-institut.de/media/News/Statement/Weizenbaum_Institute_Data_Act_IIA_Position_Paper_final.pdf>.

which do not fulfil the substantive conditions of protection shall generally not be protected by other instruments of Member States' national law either, absent any additional objectives entirely unrelated to the investment protection objective of the Database Directive (*Union law pre-emption doctrine*).

41 With regard to an *ongoing and ex-post evaluation* of how legal instruments proposed in the Data Act are implemented and if they are efficient and effective, we propose

- to carefully *choose certain very specific, carefully limited and representative industry sectors* for possible evaluation of central instruments of the Data Act and possibly associated data collection as otherwise the very broad scope and generalising character of the Data Act will prevent the emergence of conclusive results.

JIPITEC

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

www.jipitec.eu