jipitec

3 | 2021

Volume 12 (2021)
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 12 Issue 3 July 2021
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

by **Miquel Peguera**

Recommended citation: Miquel Peguera, Editorial, 12 (2021) JIPITEC 271 para 1.

1 This is the first regular issue of JIPITEC in 2021. It has been preceded by two special issues, numbers 12(1) and 12(2), which dealt monographically with specific topics. Special issue 12(1) presented the "Kyoto Guidelines on Intellectual Property and Private International Law" of the International Law Association (ILA) with extended comments. While special issue 12(2) focused on the Directives on Digital Content and Services and on Consumer Sales, and more generally, on consumer contracts and new technologies. This third issue, 12(3), resumes the thread of JIPITEC regular issues, covering a variety of timely and relevant topics, which range from tackling online misinformation to competition law, from intermediary liability to data protection, and from IP rights to Covid-19 tracing applications.

2 Online political advertising is the topic addressed in the first article, authored by Natali Helberger, Tom Dobber, and Claes de Vreese. Online political microtargeting is increasingly adopting the practices of sophisticated online commercial advertising, particularly in the context of social media and data-driven platforms. The article shows that, in practice, both commercial and political online advertising have many elements in common, particularly the use of data-driven persuasion strategies, which may impact the ability to make free and informed political decisions. The authors explore whether the way in which the law approaches fairness in commercial advertising may provide valuable lessons for future regulation of political advertising. They find that, indeed, the experience in the field of commercial advertising could serve as a conceptual frame to build on and point to a number of specific takeaways from that legal tradition that could be taken into account when devising a legal framework for political advertising.

3 Maryam Pourrahim examines in the following article to what extent EU competition law can foster patent pools as a mechanism for licensing Standard Essential Patents while avoiding anti-competitive practices. The article underscores the significant pro-competitive effects of patent pools and offers a substantive comparative analysis between the US and EU approaches. It suggests some ways for the EU to improve its patent pool legal framework.

4 In the next piece, Folkert Wilman addresses the evolution and current status of the liability exemption for internet intermediaries that store and disseminate content uploaded by their users set forth in the e-Commerce Directive. While the author identifies some shortcomings in terms of ineffectiveness in tackling serious illegal content and risks of over-removal, he argues that there are nonetheless good reasons for retaining the key features of the system, as the Digital Services Act choses to do. The author puts forward that the noted shortcomings should be addressed by enacting complementary requirements and explores to what extent the Digital Services Act proposal contributes to this end.

5 In the following article, Bluetooth-based apps for tracing proximity contacts in the fight against Covid-19 provide a case-study for dealing with the more general issue of joint controllership in EU data protection law. Stephanie Rossello and Pierre Dewitte examine the ambiguities of the notion of joint control, combining them with those related to the notion of identifiability of personal data and exploring the scope of the household exemption as well. Applying the theoretical analysis to the case-study, the authors argue that a broad understanding of joint controllership may lead to unexpected results, apparently regardless of whether the architecture of the software system is centralized or decentralized, and note that further clarification from the EDPB, National Supervisory Authorities, the CJEU and domestic courts is needed.

6 Competition issues on the availability and use of non-personal machine data, specifically in the field of agricultural data, are tackled in the contribution authored by Can Atik and Bertin Martens. The

authors argue that data-driven agricultural business models lock farm data into machines and devices that reduce competition in downstream agricultural services markets. The article highlights the need for neutral platforms as intermediaries so that farmers can achieve the benefits from applications that depend on economies of scale and scope in data aggregation. While the authors point to regulatory intervention as the last resort to overcome data lock-in and monopolistic market failures, they also underscore the difficulties in designing data access rights.

7 Covid-19 is again considered in this issue, now from the point of view of Intellectual Property Law, in a contribution by Emmanuel Kolawole Oke. The author explores to what extent states can realistically invoke the national security exception set forth in Article 73(b)(iii) of the TRIPS Agreement to suspend the protection and enforcement of IP rights in order to facilitate the importation and production of vaccines and medicines to fight against the pandemic. The author considers how this provision has been interpreted and applied so far and while he acknowledges that states may indeed be able to invoke the national security exception in this case, he also argues that such an invocation may not be actually helpful to states lacking local manufacturing capacity.

8 Finally, IP rights are also considered in the realm of Artificial Intelligence. Anthoula Papadopoulou examines how copyright law and patent law may interact with AI technology, and particularly whether AI outputs deserve IP protection. Considering legal but also moral and social aspects, the author suggests that the attribution of a sui generis right could be the best option for fostering innovation and competition.

I do hope you will enjoy the issue!

Miquel Peguera

Towards Unfair Political Practices Law: Learning lessons from the regulation of unfair commercial practices for online political advertising

by **Natali Helberger, Tom Dobber and Claes de Vreese***

Abstract: Online political advertising operates in a tense forcefield between political and commercial practices. It thus presents regulators with a difficult conundrum: because online political advertising is political rather than commercial speech, it is destined to follow an entirely different regulatory tradition than commercial advertising. And yet many of the tools used, players involved and concerns triggered by modern online political advertising strategies very much resemble the tools, players and concerns in online commercial targeting. Commercial advertising is subject to consumer law and unfair advertising regulation, including rules about unfair commercial practices. Unfair commercial practices law, and other rules about commercial advertising, however, are explicitly not applicable to forms of non-commercial political or ideological advertising. An important reason is the different level of protection of political and commercial speech under fundamental rights law standards. And yet with the ongoing commercial turn in advertising, the traditional division between forms of commercial and political advertising is no longer that self-evident. Also, it cannot be denied that commercial advertising law has a long tradition of thinking of where and how to draw the line between lawful advertising and unlawful persuasion through withholding or misleading consumers about the information they need to take informed decisions, or abusing superior knowledge, exerting undue psychological pressure and engaging in other forms of unfair behaviour. The question this article explores is whether there are lessons to be learned from the regulation of commercial advertising for the pending initiatives at the national and the European level to regulate online political advertising, and online political targeting in specific.

Keywords: online and commercial political targeting; fundamental rights; platforms; unfair commercial practices; regulation

Recommended citation: Natali Helberger, Tom Dobber and Claes de Vreese, Towards Unfair Political Practices Law: Learning lessons from the regulation of unfair commercial practices for online political advertising, 12 (2021) JIPITEC 273 para 1

A. Introduction

1 "Hold political ads to the same standard as other ads" was the first recommendation made by hundreds of Facebook employees in an open letter to the Facebook leadership.[1] The letter criticised Facebook's policy of excluding political ads from its fact-checking

* Prof. Natali Helberger, Institute for Information Law (IViR), University of Amsterdam; Tom Dobber, Amsterdam School of Communication (ASCoR), University of Amsterdam; Prof. Claes de Vreese, Amsterdam School of Communication (ASCoR), University of Amsterdam. The authors thank Sander Kruit and Ljubisa Metikos for valuable research assistance. This project was funded by the Research Priority Area Information & Communication in the DataSociety of the University of Amsterdam and the Dutch Organisation for Scientific Research, grant no. MVI.19.019 (Safeguarding democratic values in digital political practices).

1 The New York Times, 'Read the Letter Facebook Employees Sent to Mark Zuckerberg About Political Ads' *The New York Times* (28 October 2019) <https://www.nytimes.com/2019/10/28/technology/facebook-mark-zuckerberg-letter.html> accessed

programme that is intended to identify false or misleading content, including advertising. Facebook cites freedom of expression concerns and respect for the democratic process as reasons for the different treatment of political versus commercial ads.[2] The fundamental right to freedom of expression and the importance of political speech for the democratic process are more generally important reasons why commercial advertising also in law follows a different path than the regulation of political advertising. And yet with the advent of digital technology, social media and new forms of political advertising, elements of political and commercial advertising are increasingly intertwined. Online political targeting in particular raises new issues of voter protection and challenges a number of regulatory assumptions and path-dependencies that we have taken for granted for too long.[3]

2 Political campaigns still rely on the mass media to send campaign messages that appeal to a large part of the electorate,[4] but in addition to that, digital technology has enabled new forms of personalised political advertising, whereby political campaigns can target increasingly small segments of the electorate with tailored messages. Students, for example, no longer see political ads about pensions; instead, they see ads about student debt or student housing in the city where their university is located. Political campaigns can personalise these messages to a considerable degree, as long as the political campaign has 1) vast amounts of data about the electorate, 2) the skills and tools to analyse the data and to make meaningful advertisements and 3) the infrastructure (and money) required to spread those ads.[5] The advent of online political targeting has given rise to both new hopes and concerns about the fairness and governance of these practices.[6] There are concerns about the opacity and lack of accountability of these practices,[7] the danger of

19 March 2021.

2 https://www.facebook.com/business help/315131736305613 (last visited on 2 March 2021).

3 The focus of this article is on online political targeting as a specific form of online political advertising. Since online political targeting is a form of political advertising, at some places in the article we used the notions interchangeably. We depart from the definition of Zuiderveen et al that describe political targeting as "a type of personalized communication that involves collecting information about people, and using that information to show them targeted political advertisements, Frederik J Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14 Utrecht Law Review 82, 82.

4 John R Petrocik, William L Benoit and Glenn J Hansen, 'Issue Ownership and Presidential Campaigning, 1952-2000' (2003) 118 Political Science Quarterly 599; Lynn Vavreck, *The Message Matters: The Economy and Presidential Campaigns* (STU-Student edition, Princeton University Press 2009) <https://www.jstor.org/stable/j.ctt7t1g4> accessed 19 March 2021.

5 Zeynep Tufekci, 'Engineering the Public: Big Data, Surveillance and Computational Politics' [2014] First Monday <https://journals.uic.edu/ojs/index.php/fm/article/view/4901> accessed 19 March 2021; Daniel Kreiss and Christopher Jasinski, 'The Tech Industry Meets Presidential Politics: Explaining the Democratic Party's Technological Advantage in Electoral Campaigning, 2004–2012' (2016) 33 Political Communication 544; Daniel Kreiss, *Taking Our Country Back: The Crafting of Networked Politics from Howard Dean to Barack Obama* (Oxford University Press) <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780199782536.001.0001/acprof-9780199782536> accessed 19 March 2021; Bruce Bimber, 'Digital Media in the Obama Campaigns of 2008 and 2012: Adaptation to the Personalized Political Communication Environment' (2014) 11 Journal of Information Technology & Politics 130; Colin J Bennett, 'Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America?' (2016) 6 International Data Privacy Law 261.

6 Normann Witzleb and Moira Paterson, 'Micro-Targeting in Political Campaigns: Political Promise and Democratic Risk' in Uta Kohl and Jacob Eisler (eds), *Data-Driven Personalisation in Markets, Politics and Law* (CUP, Forthcoming 2021) <https://papers.ssrn.com/abstract=3717561> accessed 19 March 2021; Frederik J Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14 Utrecht Law Review 82; Jeff Chester and Kathryn C Montgomery, 'The Role of Digital Marketing in Political Campaigns' (2017) 6 Internet Policy Review; Solon Barocas, 'The Price of Precision: Voter Microtargeting and Its Potential Harms to the Democratic Process', *Proceedings of the first edition workshop on Politics, elections and data* (Association for Computing Machinery 2012) <https://doi.org/10.1145/2389661.2389671> accessed 19 March 2021; European Commission for Democracy Through Law, 'Joint Report of the Venice Commission and of the Directorate of Information Society and Action Against Crime of the Directorate General of Human Rights and Rule of Law (Dgi) on Digital Technologies and Elections" (CoE 2019) CDL-AD(2019)016 <https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2019)016-e> accessed 19 March 2021>.

7 Witzleb and Paterson (n 6); Varoon Bashyakarla and others, 'Personal Data: Political Persuasion – inside the Influence Industry' (Tactical Tech 2019) <https://cdn.ttc.io/s/tacticaltech.org/methods_guidebook_A4_spread_web_Ed2.pdf>; Kathleen Jamieson, 'Messages, Micro-Targeting, and New Media Technologies' (2013) 11 The Forum.

polarisation,[8] filter bubbles[9] and the ability of voters to engage in a shared discourse.[10] Related to this are more general concerns about the way political power is shifting from political parties to platforms,[11] and instances of voter exclusion, discrimination and the ability 'to sidestep less sympathetic audiences' or invest time in voters who are unlikely to vote.[12] In response, countries around the world are increasingly devising ways to regulate political microtargeting. Devising new rules for online political targeting is also a priority for the European Commission (EC). The Commission's European Democracy Action Plan announced legislative proposals on the transparency of political advertising and possible further restrictions on microtargeting and forms of psychological profiling.[13] The regulation of online political targeting, however, presents regulators with a difficult conundrum.

3 The existing rules on political advertising are intended to strike a careful balance between respecting the status of political advertising as the highest protected form of speech and the need to lay down some ground rules in the interest of fair elections and the protection of voters.[14] Most of these rules focus on the traditional mass media that have long been the primary vehicle to disseminate political advertising to voters.[15] Online political targeting is different from the traditional forms of advertising via the mass media. There is, first of all, the far more central role of data, in combination with powerful data analytics tools that allow for predictive modelling and the increasingly precise targeting of content and delivery of political messages, than in the traditional mass media.[16] The combination of detailed knowledge about voters, their behaviours, fears and preferences with data-driven profiling (i.e. adjusting message and distribution strategy to individual or group profiles) provides entirely new levels of persuasion knowledge and therefore has heightened concerns about voter manipulation and unfair forms of subconsciously undermining voter autonomy.[17] Data-driven tools provide advertisers and platforms with a much more detailed view of the target audience than traditional forms of advertising do (information asymmetries). The advertisers and platforms learn information about the citizen, while the citizen has a limited understanding of the data machinery operating behind the scenes, leading to their exposure to a (micro)targeted political ad.

4 A second important difference is the prominent role of new players, primarily social media platforms that serve as both new sources of data (both disclosed and inferred, e.g. in the form of look-a-like audience matching and data modelling) and new advertising infrastructure. Unlike traditional mass media, social

8 Judit Bayer, 'Double Harm to Voters: Data-Driven Micro-Targeting and Democratic Public Discourse' (2020) 9 Internet Policy Review; Daniel Kreiss, 'Yes We Can (Profile You)' (2012) 64 Stanford Law Review <https://www.stanfordlawreview.org/online/privacy-paradox-yes-we-can-profile-you/> accessed 19 March 2021; Dobber, Ó Fathaigh and Zuiderveen Borgesius (n 45).

9 Borgesius and others (n 6); Axel Bruns, 'Filter Bubble' (2019) 8 Internet Policy Review.

10 Ira Rubinstein, 'Voter Privacy in the Age of Big Data' (2014) 2014 SSRN Electronic Journal; European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Securing Free and Fair European Elections' (2018) COM(2018) 637 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0637> accessed 19 March 2021; Committee of Ministers, 'Declaration by the Committee of Ministers on the Manipulative Capabilities of Algorithmic Processes' (Council of Europe 2019) Decl(13/02/2019)1 <https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b> accessed 19 March 2021.

11 Witzleb and Paterson (n 6).

12 Barocas (n 6) 33.

13 European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – European Democracy Action Plan' Ares(2020)3624828 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AAres%282020%293624828>.

14 Jacquelyn Burkell and Priscilla M Regan, 'Voter Preferences, Voter Manipulation, Voter Analytics: Policy Options for Less Surveillance and More Autonomy' (2019) 8 Internet Policy Review 3.

15 Lynda Lee Kaid and Christina Holtz-Bacha, *The SAGE Handbook of Political Advertising* (2006) <http://sk.sagepub.com/reference/hdbk_politicaladvert> accessed 19 March 2021.

16 Zuiderveen Borgesius and others (n 6); see also the extensive comparison in Julian Jaursch, 'Rules for Fair Digital Campaigning, What Risks Are Associated with Online Political Advertising and What Reforms Are Necessary in Germany' (Stiftung Neue Verantwortung 2020) <https://www.stiftung-nv.de/sites/default/files/rules_for_fair_digital_campaigning.pdf>; Katharine Dommett, 'Data-Driven Political Campaigns in Practice: Understanding and Regulating Diverse Data-Driven Campaigns' (2019) 8 Internet Policy Review.

17 Burkell and Regan (n 12); Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8 Internet Policy Review <https://policyreview.info/node/1410> accessed 27 November 2020; William A Gorton, 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy' (2016) 38 New Political Science 61.

network sites with their highly connected structure allow entirely new and far more interactive means of communication with individual voters. As powerful controllers of both economic and communication power, their ability to change power balances and affect fair competition in the marketplace of ideas is the source of much scholarly concern,[18] especially because these actors fall outside the scope of traditional media regulation and the applicable rules in e-commerce and consumer protection law are ill suited to deal with their commercial and political power.[19]

5 This leads us to a third major difference between traditional forms of political advertising and online advertising, and the one that is most central to this article: the degree of professionalisation and commercialisation of political advertising. As political campaigns increasingly rely on the tools developed for commercial targeting practices and the same commercial parties (in particular the Google and Facebook duopoly) to spread their messages,[20] commercial strategies and motives are increasingly shaping political campaigning strategies. The consequence is that political advertising is turning, at least from the perspective of platforms, into 'just another form of advertising', and it is becoming difficult to distinguish the citizen from the consumer. Or in the words of Brad Parscale, digital director of the former Trump campaign: 'It's the same shit we use in commercial, just has fancier names.'[21]

6 It is this tension between the political and the commercial that creates new challenges for the regulation of political advertising, an issue that this article is particularly interested in. Because online political advertising is political and not commercial speech, it is destined to follow an entirely different regulatory tradition than commercial advertising. Commercial advertising is subject to consumer law and unfair advertising regulations, including rules about unfair commercial practices. The provisions about unfair commercial practices are intended to protect consumer autonomy and fairness in the commercial marketplace, and to find the right balance between legitimate and illegitimate forms of persuasion.[22] Increasingly, the rules about unfair commercial practices are also discussed in the context of behavioural commercial targeting, as a potential response to concerns about data-driven forms of commercial advertising.[23] Unfair commercial practices law, and other rules about commercial advertising (e.g. rules about unfair comparative advertising), however, are explicitly not applicable to forms of non-commercial political or ideological advertising.[24] An important reason why this is so are

18 Martin Moore, 'Tech Giants and Civic Power' <https://kclpure.kcl.ac.uk/portal/en/publications/tech-giants-and-civic-power(b8e837ec-abd8-4838-b8e7-f0059f0de550).html> accessed 19 March 2021; Natali Helberger, 'The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power' (2020) 8 Digital Journalism 842; Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OXFORD UNIV PR 2020); Urs Gasser and Wolfgang Schulz, 'Governance of Online Intermediaries: Observations from a Series of National Case Studies' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2566364 <https://papers.ssrn.com/abstract=2566364> accessed 19 March 2021.

19 Helberger (n 18;. Victor Pickard, 'Restructuring Democratic Infrastructures: A Policy Approach to the Journalism Crisis' (2020) 8 Digital Journalism 704.

20 Joseph Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (Yale Univ Press 2011); Michael Trusov, Liye Ma and Zainab Jamal, 'Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting' (2016) 35 Marketing Science 405; Anastasia Siapka, 'The Ethical and Legal Challenges of Artificial Intelligence: The EU Response to Biased and Discriminatory AI' (Social Science Research Network 2018) SSRN Scholarly Paper ID 3408773 <https://papers.ssrn.com/abstract=3408773> accessed 26 February 2021.

21 Cited in: John Miglautsch, 'Did Direct Marketing Swing the Election?' (*LinkedIn*, 22 December 2016) <https://www.linkedin.com/pulse/bigdata-fail-vs-trump-win-john-miglautsch/> accessed 19 March 2021.

22 Geraint Howells, 'Aggressive Commercial Practices' in Hans-W Micklitz and Thomas Wilhelmsson (eds), *European fair trading law: the unfair commercial practices directive* (Ashgate 2006); Hans-W Micklitz, 'The General Clause on Unfair Practices' in Geraint Howells and Thomas Wilhelmsson (eds), *European fair trading law: the unfair commercial practices directive* (Ashgate 2006).

23 Marijn Sax, Natali Helberger and Nadine Bol, 'Health as a Means Towards Profitable Ends: MHealth Apps, User Autonomy, and Unfair Commercial Practices' (2018) 41 Journal of Consumer Policy 103; Ryan Calo, 'Digital Market Manipulation' (2013) 82 University of Washington School of Law Research Paper nr 2013-27 995; Autoriteit Consument & Markt (ACM), 'Guidelines on the Protection of the Online Consumer' (11 February 2020) <https://www.acm.nl/en/publications/guidelines-protection-online-consumer> accessed 19 March 2021; BEUC, 'The Report of the Consumer Law Enforcement Forum CLEF and of the Consumer Justice Enforcement Foirmum COJEF' <https://www.beuc.eu/general/consumer-justice-enforcement-forum-cojef>.

24 Art. 2 (d), art. 3 (1) of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/

differences in the level of protection of political and commercial speech under fundamental rights law standards. And yet, with the ongoing commercial turn in advertising, the traditional division between forms of commercial and political advertising is no longer that self-evident. Also, it cannot be denied that commercial advertising law has a long tradition of thinking of where and how to draw the line between lawful advertising and unlawful persuasion through withholding or misleading consumers about the information they need to make informed decisions, or by exploiting information asymmetries, exerting undue psychological pressure and engaging in other forms of unfair behaviour.

7 The question that this article therefore explores is: "Are there valuable lessons to learn from the way the law approaches fairness in commercial advertising for the future regulation of political advertising?" It is explicitly *not* the goal to discuss a possible extension of unfair commercial advertising regulation (as most notably laid down in the Unfair Commercial Practices Directive)[25] to online political advertising. This article also does not explore to what extent data protection law imposes regulatory constraints on online political advertising, a question that has been discussed extensively elsewhere.[26] Instead, we explore the nexus between online commercial and political advertising, and possible inspiration for regulatory tools or instruments that can inform the future regulation of online political advertising.

B. The commercialisation of political advertising

8 In the following section, we scrutinise in more depth the ongoing commercialisation of political advertising and of voters, and the main factors that drive it, namely data and data-driven platforms.

I. Merging data on voters and consumers

9 Collecting personal data on voters is not new to political campaigning and political parties were collecting such data long before the widespread proliferation of the internet, for example in the form of public voter registries and data that political parties collect directly from their voters. In their history of political data in the United States, Kreiss and Howard (2010) pinpoint the origins of campaign data practices in the 1960s, but also show how the arrival of the internet offered political campaigners new ways to use the data they had collected to directly interact with voters and amplify their messages. Already then they were aided in their efforts by early commercial platform services as well as the use of commercial data brokers (such as "Adobe, Oracle, Salesforce, Nielsen, and IBM")[27] and other sources of commercial data about the behaviour of voters, as consumers, online. In both the United States and Europe, data brokers gather data from public sources, through surveys, promotional actions, purchased data sets (also from offline behaviour, such as magazine subscriptions or loyalty card programmes), and they add value by cleaning the data, combining datasets and keeping them up to date. The arrival of social media platforms in the late 1990s unlocked another wealth of personal data, as well as the ability to purchase data that users disclose on these platforms and the data that social media platforms inferred from the behaviour of users (often in their role as consumers), as well as look-a-like audience matching and custom audience services.[28]

II. Data-driven advertising as a business model

10 Today, social media platforms (such as Google and Facebook) are the most important actors in online advertising, because of their size and infrastructure and the wealth of new data sources that they unlock. The size of the bigger platforms allows them to collect a lot of information about users and to subsequently use that information to infer or predict behaviour. The platforms' easy-to-use infrastructure then allows advertisers to cheaply microtarget voters. Social media platforms offer their services to commercial and political advertisers alike. Facebook, for example, offers its advertising

EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') 2005 [32005L0029].

25 Ibid.

26 ICO, 'Investigation into Data Analytics for Political Purposes' (6 October 2020) <https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/> accessed 19 March 2021; Bennett (n 5); Witzleb and Paterson (n 6).

27 Daniel Kreiss and Philip N. Howard, 'New Challenges to Political Privacy: Lessons from the First U.S. Presidential Race in the Web 2.0 Era', (2010) 4 Int'l J. Comm. 1032.

28 Dommett (n 16).

services to commercial and political campaigners via a centralised ads manager,[29] as do Google[30] and Twitter.[31] Commercial and political advertisers can even compete with each other by placing a bid into the platforms' auction systems in the hope of being allowed to show their ad to a specific audience. Oftentimes, there are many different parties—political *and* commercial—seeking to display an ad to the same specific audience.

11 More recently, and in response to scandals such as Cambridge Analytica and increasing concerns about the role of social media in elections, social media platforms have been adjusting their service offers. For example, Twitter banned the promotion of political content altogether, based on a belief that 'political message reach should be earned, not bought'[32], while Google limited 'election ads audience targeting' to some more general categories, not offering more granular microtargeting and committed to more transparency.[33] Facebook suspended running ads about social issues, elections and politics only temporarily in the run-up to the United States 2020 elections,[34] and continued to offer outside the United States the ability to target ads at custom audiences and look-a-like audiences or to define an audience "based on criteria such as age, interests, geography and more", including interest and behaviour.[35] The more recent adjustments to the range or reach of their advertisement services, however, do not change the general business proposition. As Witzleb and Paterson observe, "the same personal data gathered by online platforms is as valuable to platforms and other businesses seeking to sell goods and services, as it is for political parties and political interest groups seeking to 'sell their programs, ideas and ideologies.'"[36] Thus, social media platforms are important drivers behind the increasing commercialisation of political advertising and are blurring the lines between commercial and political advertising.[37]

III. The same tools and strategies to rule them all

12 Social media platforms also sell their sophisticated skills and tools for data analysis. Advertisers do not necessarily have the in-house knowledge and tools to turn vast amounts of data into something meaningful. Platforms, therefore, actively offer their services to political campaigns in the United States[38] and in Europe.[39] Additionally, commercial and political advertisers can outsource their big data analysis to consultancies.[40] The 'meaningful information' resulting from such analyses can just as easily be employed for political as for commercial purposes, and is the source of a range of new forms of online and political advertising, ranging from programmatic advertising and targeting across different devices, through targeting based on location (geolocation targeting), demographic or personal information, to forms of psychographic targeting or neuromarketing that are driven by intimate insights into the emotions, desires, personalities, attitudes and behavioural biases of users and informed by the insights of cognitive psychology.[41]

29 https://www.facebook.com/business/ads/pricing.

30 https://ads.google.com/home/.

31 https://ads.twitter.com/onboarding/18ce5478v4d/welcome.

32 https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html.

33 https://blog.google/technology/ads/update-our-political-ads-policy/.

34 https://www.facebook.com/business/help/167836590566506?id=288762101909005.

35 https://www.facebook.com/business/ads/ad-targeting.

36 Witzleb and Paterson (n 6).

37 Chester and Montgomery (n 6) 4; Daniel Kreiss and Shanon McGrogor, 'Technology Firms Shape Political Communication: The Work of Microsoft, Facebook, Twitter, and Google With Campaigns During the 2016 U.S. Presidential Cycle' (2018) 35 Political Communication 155, 155–177.

38 Kreiss and McGrogor (n 37).

39 From personal talk with Facebook and interview with the Dutch party D66's campaign leader; 'Facebook In Person Marketing Training' (*Facebook for Business*) <https://www.facebook.com/business/learn/in-person>.

40 Barbara Thau, 'Consumer Goods Industry Trends: How Companies are Driving Product' (*IBM Big Data & Analytics Hub*) <https://www.ibmbigdatahub.com/blog/consumer-goods-industry-trends-how-companies-are-driving-product-sales-big-data>; 'Capgemini Invent UK: BRINGING TO LIFE WHAT'S NEXT.' (*Capgemini UK*, 10 September 2018) <https://www.capgemini.com/gb-en/service/invent/>.

41 Burkell and Regan (n 14) 3; Chester and Montgomery (n 6).

IV. Similar concerns of users and voters

13 The use of online targeting strategies and psychological targeting strategies in commercial advertising has given rise to a number of concerns about the rights of consumers. For commercial targeting, the Dutch Consumer Authority observed that as a result of profiling strategies, "businesses can steer consumers' behavior very effectively, potentially affecting the autonomy of consumers".[42] The European Consumer Protection Organisation (BEUC) states that under certain conditions behavioural advertising can have "undue influence" in the sense of the Unfair Commercial Practices Directive, notably if there is a situation of power due to information asymmetries, and targeting strategies are used to exert pressure on the consumer or 'prevent the display of other advertisements and reduce consumer choice'.[43] In its Guidance on the application of the Unfair Commercial Practices Directive, the EC concedes that when profiling strategies violate the data protection rights of consumers, doing so can also constitute an unfair commercial practice, particularly if that practice is not transparent or hides the commercial intent,[44] or is designed to exert undue influence through psychological pressure.[45] Scholars have also pointed to the possibilities to identify and target individual vulnerabilities and more generally influence the taking of autonomous decisions.[46]

14 Some of the concerns regarding the use of commercial targeting are echoed in the literature about online political targeting. An example are concerns related to the inability of users to judge political advertising on its value and take well-informed, autonomous decisions. This can be because of the deceptive or misleading content of the political message itself,[47] a lack of transparency[48] or using microtargeting to make divergent promises to different voters.[49] The information asymmetry – where the political advertiser has a detailed profile of the voter, while the voter has no idea about the mechanics and information behind the targeted advertisement she receives[50] – enables the political advertiser to not only stay under the radar, but also to lie, mislead, pressure or leverage fears more effectively. And as in behavioural commercial targeting, also for political targeting practices the use of 'psychographics' or persuasion profiling and knowledge of biases and political concerns and views on particular political topics to exercise undue influence over voters is another key concern in the discussions about online political advertising, and microtargeting in particular.[51] Other concerns therefore relate to the way the political message is delivered, for example by developing rich voter profiles that reveal preferences, fears, beliefs and other characteristics and combining them with psychological insights to

42 Autoriteit Consument & Markt (ACM) (n 23).

43 Emilie Barrau, 'DATA COLLECTION, TARGETING AND PROFILING OF CONSUMERS ONLINE BEUC Discussion Paper' (BEUC 2010) <https://www.beuc.eu/publications/2010-00101-01-e.pdf>.

44 European Commission, 'COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES Accompanying the Document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Comprehensive Approach to Stimulating Cross-Border e-Commerce for Europe's Citizens and Businesses, SWD/2016/0163 Final'.

45 Calo (n 23); Sax, Helberger and Bol (n 23); Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Nomos 2016) <http://www.nomos-elibrary.de/index.php?doi=10.5771/9783845273488-135> accessed 27 November 2020; Bram van Duivenvoorde, *The Consumer Benchmarks in the Unfair Commercial Practices Directive* (2014) <https://dare.uva.nl/search?identifier=1519cbfb-a08a-4132-a207-af6355e53bcd> accessed 19 March 2021; European Commission, 'COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES Accompanying the Document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Comprehensive Approach to Stimulating Cross-Border e-Commerce for Europe's Citizens and Businesses, SWD/2016/0163 Final' (n 42).

46 Susser, Roessler and Nissenbaum (n 17).

47 Tom Dobber, Ronan Ó Fathaigh and Frederik J Zuiderveen Borgesius, 'The Regulation of Online Political Micro-Targeting in Europe' (2019) 8 Internet policy review; Borgesius and others (n 6); Witzleb and Paterson (n 6).

48 Barocas (n 6) 34 , pointing to the fact that secrecy of the campaign is often considered an important success factor, limiting the incentives for political advertisers to share campaign strategies with voters or third parties.

49 Julian Jaursch (n 16) 22.

50 Tufekci (n 5).

51 Martin Moore and Damian Tambini (eds), *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford University Press 2018); Gorton (n 17); Chester and Montgomery (n 6).

tailor content and form of the message,[52] or identify and exploit individual vulnerabilities and biases.[53]

15 To conclude, the fusion of political and commercial players, along with tools and data sources is accompanied by a number of important implications for political advertising, as well as the protection of users thereof. Both commercial and political advertisers use similar data, similar tools and similar infrastructures to target their audiences. As the tools and strategies are the same, it stands to reason that also some of the concerns regarding the commercial use of some profiling strategies (unfair forms of manipulation, loss of autonomy, data protection and surveillance, the potential to exploit individual vulnerabilities)[54] arise in the context of political targeting. Users for their part are potential voters and consumers alike and are confronted with the difficult task of having to process and distinguish between commercial and political messages. Perhaps one of the most obvious consequences is the central role of and dependency on social media platforms that can leverage the data, tools and infrastructure that they developed to both political and commercial advertisers. Unlike political parties, these are commercial players that are essentially driven by commercial interests to increase revenues and are accountable not to voters but to shareholders. If political advertising is yet another form of advertising, should we not offer users the same level of protection vis-à-vis unfair forms of commercial and political advertising? This is the question that the next section investigates.

C. Regulation of commercial and political advertising – different regulatory traditions

16 So far, the regulation of commercial speech and that of political speech have followed separate paths. An important reason why this is so lies in fundamental rights law, and the differences in the margin of appreciation that national governments have to regulate commercial vs political speech. From the perspective of fundamental rights law, commercial and political speech are not the same, though both enjoy freedom of expression protection.[55] Government restrictions on political speech receive a far higher level of scrutiny regarding their compatibility with Art. 10 ECHR. The European Court of Human Rights has indeed consistently held that the margin of appreciation that states have in deciding whether or not to regulate speech is "is essential in commercial matters and, in particular, in an area as complex and fluctuating as that of unfair competition,"[56] which gives states more room to interfere with commercial speech than political speech. Elsewhere, the Court explained: "For the citizen, advertising is a means of discovering the characteristics of services and goods offered to him. Nevertheless, it may sometimes be restricted, especially to prevent unfair competition and untruthful or misleading advertising. In some contexts, the publication of even objective, truthful advertisements might be restricted in order to ensure respect for the rights of others or owing to the special circumstances of particular business activities and professions."[57] As a result, commercial advertising is subject to a range of advertising regulations that can include scrutiny of both the fairness of the message (e.g. whether or not it is misleading) and the way the message is delivered (e.g. in a way that amounts to exerting pressure on consumers).[58]

52 Tal Z Zarsky, 'Privacy and Manipulation in the Digital Age' (2019) 20 Theoretical Inquiries in Law 157; Julian Jaursch (n 16); Burkell and Regan (n 10) 9; Susser, Roessler and Nissenbaum (n 17).

53 Shaun B. Spencer, 'The Problem of Online Manipulation' [2020] Illinois Law Review <https://illinoislawreview.org/print/vol-2020-no-3/the-problem-of-online-manipulation/> accessed 19 March 2021; Muhammad Ali and others, 'Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes' (2019) 3 Proceedings of the ACM on Human-Computer Interaction 199:1; Lisa Maria Neudert and Nahema Marchal, 'Polarisation and the Use of Technology in Political Campaigns and Communication.' (European Parliament Directorate General for Parliamentary Research Services 2019) <https://data.europa.eu/doi/10.2861/167110> accessed 19 March 2021.

54 Sax, Helberger and Bol (n 23); Calo (n 23).

55 *CASE OF MARKT INTERN VERLAG GMBH AND KLAUS BEERMANN v GERMANY* [1989] ECHR 10572/83 [26], stipulating that information of a commercial nature cannot be excluded from the scope of Art. 10 ECHR.

56 ibid 33; *X and CHURCH OF SCIENTOLOGY VS SWEDEN* [1979] ECHR 7805/7 7.

57 *CASE OF CASADO COCA v SPAIN* [1994] ECHR 15450/89 [51].

58 *CASE OF MARKT INTERN VERLAG GMBH AND KLAUS BEERMANN v. GERMANY* (n 55) para 35. observing that even the publication of items that are true may under certain circumstances be prohibited, e.g. if they fail to respect the privacy of others, the duty to respect confidentiality, but also regarding any false impressions that a message can invoke and that these are factors that national courts can take into account to decide whether statements are permissible or not.

17 Commercial advertising regulation serves at least three goals: (1) the protection of consumers and their ability to make informed, rational choices, (2) the protection of competitors against unfair competition and (3) the protection of a broader public interest in information,[59] on the one hand, and a fair and functioning marketplace on the other hand.[60] Over the course of time, the legal order has developed a range of instruments to concretise these objectives, including rules intended to:[61]

- *Protect consumers against particular products (the regulation concerning tobacco advertising is an example)[62] or protect particular groups of consumers (e.g. the rules with regards to the protection of minors in the AVMSD).[63]*
- *Protect consumers (and indirectly public information interests and fair competition) against misleading or otherwise unfair advertising (and here, in particular the provisions of the Unfair Commercial Practices Directive and its implementation into national laws).[64]*
- *Protect competitors (and fair competition) against particular forms of unfair advertising, including comparative and denigrating advertising (the Directive on misleading and comparative advertising),[65] as well as under national, non-harmonised rules on torts, libel and defamation[66].*

18 At the heart of the regulation of commercial advertising is the standard of fairness and good faith in advertising.[67] Under the Unfair Commercial Practices Directive, for example, commercial practices are unfair where they are either contrary to the requirements of professional diligence, or can or do "distort the economic behaviour" of consumers (Art. 5 (2) UCPD),[68] through misleading or aggressive practices. The main objective behind the ban on misleading practices is to provide consumers with the correct information they need to take informed and autonomous decisions.[69] The provisions about aggressive practices go beyond transparency and are concerned with forms of exerting pressure or other forms of undue influence on the actual decision-making, as well as on consumers' fundamental rights, such as privacy.[70]

19 While the function of commercial advertising is primarily linked to the economic marketplace,

59 Roger A Shiner, *Freedom of Commercial Expression* (Oxford University Press) <https://oxford.universitypressscholarship.com/view/10.1093/acprof:oso/9780198262619.001.0001/acprof-9780198262619> accessed 19 March 2021; Reto M Hilty and Frauke Henning-Bodewig (eds), *Law Against Unfair Competition: Towards a New Paradigm in Europe?* (Springer-Verlag 2007) <https://www.springer.com/gp/book/9783540718819> accessed 19 March 2021.

60 Rogier de Vrey, *Towards a European Unfair Competition Law: A Clash Between Legal Families* (Brill Nijhoff 2005) <https://brill.com/view/title/12739> accessed 19 March 2021.

61 Since advertising regulation in Europe has to a large extent been harmonised, we will concentrate in the following on the relevant European regulatory acts.

62 Directive 2003/33/EC of the European Parliament and of the Council of 26 May 2003 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products [2003] *OJ L 152.*

63 See article 6a of the 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 audio-visual media services (Audiovisual Media Services Directive; AVMSD) in view of changing market realities, OJ L 303, 28.11.2018, p. 69–92.

64 In particular, note that the national provisions on unfair competition in a number of Member States have traditionally had a double function of protecting consumers as well as competitors (e.g. in the context of the German UWG), but also that, as Henning-Bodewig has pointed out, over the course of time and under the influence of European law a shift in focus on consumer protection has taken place, Henning-Bodewig, 2007.

65 Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising (codified version) (text with EEA relevance) (henceforth: Directive on misleading and comparative advertising) [2006] OJ L 376/21.

66 Rules that again make a distinction between truthful and untruthful, fact and opinion, and typically include the possibility for competitors to lodge a complaint, file for an injunction (stop or prevent from doing so in the future) or damages, De Very, 2005, 287 (n 60).

67 Hugh Collins, 'The Unfair Commercial Practices Directive' (2005) 1 417.

68 Such economic behaviour of consumers can include a broad range of activities along the entire lifecycle of a commercial relationship, from processing advertising and deciding to buy or not buy a product, to using and ceasing to use it, or exercising any contractual rights a user may have, such as compliance with contractual agreements, maintenance, and after sales services.

69 Thomas Wilhelmsson, 'Misleading Practices' in Geraint Howells and Hans-W Micklitz (eds), *European fair trading law: the unfair commercial practices directive* (Ashgate 2006).

70 Howells (n 22) 200.

political advertising is associated with the marketplace of ideas. Paid advertising can be a means for political parties to convey a message to the public, and particularly for smaller political parties it can even be a means to compensate for the relative lack of media coverage compared to what larger political parties might receive.[71] According to the European Court of Human Rights, '[f]ree elections and freedom of expression, particularly freedom of political debate, together form the bedrock of any democratic system'.[72] Moreover, as the Court has stated elsewhere, "[t]here is nothing to prohibit a political party or wealthy individual or organisation from spending money on publicity in support or opposition to a political party or tendency generally, at national or regional level, provided that there is no intention to promote or prejudice the electoral chances of any particular candidate in any particular constituency'.[73] Accordingly, "there is little scope under Art. 10 (2) of the Convention for restrictions on political speech or on debate on questions of public interest".[74] Freedom of expression protection also applies to contributions to the public debate that represent a minority opinion and are not a generally accepted idea, at least in "a sphere in which it is unlikely that any certainty exists",[75] as well as to information that offends and shocks.[76] Contributing to the high level of protection for political speech is the fact that the regulation of political advertising affects not only individual freedom of expression rights, but also—and even more so—the integrity of the political process and societal interest in political debate and fair elections.[77] In VgT, for example, the court made explicit that the margin of appreciation of whether regulatory interventions are permissible can be further reduced in situations in which what is at stake is not an individual's purely commercial interests, but their participation in a debate that affects the general interest.[78]

20 This is not to say that it is impermissible to regulate political advertising, at least in Europe.[79] The ECHR acknowledged also in cases concerning political speech that the rights and freedoms granted by Art. 10 ECHR can be subject to restrictions, provided those restrictions are "construed strictly, and the need for any restrictions must be established convincingly, particularly where the nature of the speech is political rather than commercial".[80] At times, the right to freedom of expression and that to free elections can also conflict. In such a situation, restrictions on free speech rights that are normally inacceptable can be justified if such restrictions are necessary to "secure the free expression of the opinion of the people in the choice of the legislature."[81] For example, the Court acknowledged that a public interest in protecting the democratic debate during election times from distortion and unfair competition between candidates can be a legitimate reason to restrict political speech.[82] The Court also considered legitimate "certain formalities, restrictions or penalties ... during an election period, for instance to *ensure a level playing field*, for example by way of regulating and controlling *campaign expenditure*."[83] The same is true for rules regarding the transparency of campaign finances, and "enforcing the voters' right to impartial, truthful and balanced information via mass media outlets and the formation of their informed choices in an election" are legitimate aims that can justify regulatory interference,[84] as are spending limits and rules with

71 TV *VEST AS & ROGALAND PENSJONISTPARTI v NORWAY* [2008] ECHR 21132/05 [73].

72 *Bowman v the UK* [1998] ECHR 141/1996/760/961) [42].

73 ibid 47.

74 TV Vest AS & Rogaland Pensjonisparti v Norway [2008] ECHR 21132/05 (11 December 2008).

75 *CASE OF HERTEL v SWITZERLAND* [1998] ECHR 59/1997/843/1049 [50].

76 HANDYSIDE v THE UNITED KINGDDOM [1976] ECHR 5493/72 [49].

77 Justice Oftedal Broch of the Norwegian Supreme Court, cited in para. 20 of the TV Vest decision.

78 *VEREIN GEGEN TIERFABRIKEN SCHWEIZ (VgT) v SWITZERLAND* [2009] ECHR 32772/02.

79 In the United States, under the First Amendment the barriers to regulation are arguably higher, see e.g. Cohen 2020 (n 18), p. 51: "To regulate those activities would go to the core of the free speech guarantee, by establishing regulations that control viewpoint and are unduly burdensome. Moreover, it would defeat the point of political discussion." From a US First Amendment perspective,

80 *VEREIN GEGEN TIERFABRIKEN SCHWEIZ (VgT) v. SWITZERLAND* (n 78) para 66.

81 *Bowman v. the UK* (n 72) para 43.

82 *Erdoğan Gökçe v Turkey* [2014] ECHR 31736/04 [40]. In a similar vein, Burkell and Regan argue that there are arguments to be made to convey less freedom of expression protection for manipulative speech. Maybe one could argue that also less protection for commercial-political speech, see ECHR Verein gegen Tierfabrieken.

83 *CASE OF ORLOVSKAYA ISKRA v RUSSIA* [2017] ECHR 42911/08 [102] (emphasis added).

84 Ibid, para. 104.

the goal of "securing equality between candidates".[85] Similarly, regulation of political speech to protect the diversity and inclusivity of the public debate was considered a legitimate interest to restrict political speech under certain circumstance.[86] Moreover, in situations in which there was not yet a European consensus on how to regulate political advertising, states can enjoy a greater margin of appreciation.[87]

21 In response to the conditions for interference with political speech as defined by the ECHR, the existing rules that regulate political advertising in Europe[88] have as an important objective the creation of a level playing field between political parties—for example in terms of campaign financing rules, spending limits and transparency obligations—as well as the regulation of the role of the mass media (predominantly public broadcasting) in disseminating information and party standpoints while serving the 'voter's right to impartial, truthful information'. [89] Examples are the regulation of allocating equal time for political parties or even free airtime: political parties can buy broadcasting time or sponsor political ads, but each political party should be entitled to an equal share of broadcasting time. Other countries have banned paid political advertising in the media altogether, coupled with exceptions in election times or the entitlement to free airtime. Similarly, the obligations to provide fair, balanced and impartial coverage in the media, to exercise restraint in the publication of opinion polls or to enforce quiet periods, all depart from the idea of the media as a central actor whose task is to guarantee fairness in political advertising, with the national media authorities responsible for enforcing the rules. Importantly, unlike in commercial advertising law, and flowing directly from the reduced margin of appreciation of states to regulate political speech, common to all the regulations is it that it is not so much the message itself as the conditions of its placement (e.g. amount of funding, bans on funding from particular actors, reflection days, fair and balanced coverage, etc.) that are subject to regulation. Having said so, it is also worth noting that in response to the digitally enhanced proliferation of dis- and misinformation and the growing entanglement of the issues of dis- and misinformation and political advertising, more recent pieces of legislation have also opened the door to scrutiny of the political message itself (more about this later).[90]

D. Political advertising on social media platforms – between commercial and political speech

22 In the following we argue that from the point of view of law and freedom of expression, (paid) online political advertising on social media platforms is a special case because of the way commercial and political elements and interests are entangled (see above). Accordingly, the regulation of paid online political advertising cannot easily be dealt with under either the commercial or the political speech paradigm. To discuss the extent to which the regulation of political advertising law can learn lessons from the way commercial advertising is regulated, we therefore

85 *Bowman v. the UK* (n 72) para 38.

86 *CASE OF DEMUTH v SWITZERLAND* [2003] ECHR 38743/97 [45]. Interestingly, the Swiss Federal Council justified their decision to not grant a licence with the need to protect pluralism and the interest of an inclusive general debate: "The result may be the formation of public opinion, influenced by the media by way of specific content, and no longer primarily by way of broadly based, full programs. Such a development would indubitably have consequences for the culture of communication. Communicative integration via the electronic media would be impaired, and would lead to a society increasingly shaped by segmentation and atomisation.", cited in para. 12.

87 *CASE OF MURPHY v IRELAND* [2003] ECHR 44179/98 [2].

88 Note that unlike the rules on commercial advertising, the regulation of political advertising is largely unharmonised, though the Recommendations of the Council of Europe, Article 3 of Protocol No. 1 to the ECHR and Article 25 (b) of the International Covenant on Civil and Political Rights as well as the Code of Good Practices in Electoral Matters from the Venice Commission have probably had a certain harmonising influence.

89 A comparative analysis of the rules on political advertising would have gone beyond the scope of this study and would also not have contributed much to the already existing comparative studies. Instead, this paragraph is the result of a review of a number of comparative studies, including Apa et al. (n 37); IRIS, 'Media coverage of elections: the legal framework in Europe', (European Audiovisual Observatory 2017) <https://www.ivir.nl/publicaties/download/IRIS_Special_2017_1.pdf>, Raphaël Honoré, 'ERGA : Report on the Implementation of the European Code of Practice on Disinformation' (Conseil supérieur de l'audiovisuel 2019) 10:1/6 <http://merlin.obs.coe.int/iris/2019/10/article6.en.html>; Davor Glavaš, 'Political Advertising and Media Campaign during the Pre-Election Period: A Comparative Study' (OSCE Mission to Montenegro 2017); 'Regulation of Paid Political Advertising: A Survey' (Centre for Law and Democracy 2012).

90 One example is France with its Loi relative à la lutte contre la manipulation de l'information. 2018.

need more clarity about the possible margin of appreciation that states have in regulating *online* political advertising.

23 The fusion of commercial and political elements in advertising is in itself not new. On a number of occasions, the ECHR has had to decide on the margin of appreciation of states to regulate speech that included both commercial and political elements. On these occasions, the court highlighted that the mere fact that the speech originates from a commercial for-profit company does not in itself exclude its protection as political speech.[91] An important factor in the considerations of the court is whether the commercial interests of the individual advertiser outweigh the advertiser's interest in "participation in a debate affecting the general interest"[92] and the rights of the public to receive such information.[93] In other words, speech, even if it is uttered by a commercial player and to commercial ends, can enjoy Art. 10 ECHR protection, but states may have a larger margin of appreciation in regulating it, particularly if commercial ends are overweighted. The Court has also had to decide on cases in which political and commercial interests conflicted, and where regulatory interference was necessary to "protect public opinion from the pressures of powerful financial groups and from undue commercial influence; to provide for a certain equality of opportunity among the different forces of society; to ensure the independence of broadcasters in editorial matters from powerful sponsors; and to support the press."[94] In VgT, the Court explicitly acknowledged that a competitive advantage of 'powerful financial groups' in the realm of commercial advertising can ultimately impact the realisation of freedom of expression and media pluralism (albeit for the case of TV advertising).[95]

24 What are the possible implications of this case law for the regulation of online political targeting? Where the goal of online political advertising is to contribute to matters of public interest and debate, online political targeting will fall under the qualification of political speech, with the consequence that states are limited in their ability to regulate it, similar to political advertising in the mass media. However, a number of distinguishing features of online political advertising, as opposed to political advertising in the mass media, that we identified earlier can be expected to also affect its evaluation from the perspective of Art. 10 ECHR. One is the *ability to target advertising messages* at smaller segments of the population, or even individual users, based on various forms of profiling, including psychographic profiling as a practice that, so far, we know only from the realm of commercial advertising. We explained earlier that certain forms of psychological online political advertising could have a more pervasive or even manipulative effect and therefore could impinge on the fundamental rights of citizens to freedom of expression and free elections.[96] This pervasive or manipulative effect of online political advertising could justify a larger margin of appreciation for states to protect voters from unfair manipulations of their political choices,[97] particularly if that effect can be accredited to the means of dissemination of a political message, rather than its content.[98] Indeed, the 'pervasive effect' of particular forms of media (here, audio-visual media) has been cited repeatedly by the Court as an argument that can justify government intervention in Art. 10 ECHR.[99]

25 Another side effect of the more targeted nature of political ads on social media platforms is that *they are, unlike political ads in the mass media, more difficult for public watchdogs to scrutinise*,[100] putting more

91 *CASE OF CASADO COCA v. SPAIN* (n 57) para 35; *CASE OF DEMUTH v. SWITZERLAND* (n 90) para 41.

92 *CASE OF DEMUTH v. SWITZERLAND* (n 86) para 41; *CASE OF HERTEL v. SWITZERLAND* (n 75) para 47; *VEREIN GEGEN TIERFABRIKEN SCHWEIZ (VgT) v. SWITZERLAND* (n 78) para 71.

93 Ibid, 73.

94 *VEREIN GEGEN TIERFABRIKEN SCHWEIZ (VgT) v. SWITZERLAND* (n 78) para 72.

95 Ibid, 73.

96 Maja Brkan, 'Artificial Intelligence and Democracy: The Impact of Disinformation, Social Bots and Political Targeting' (2019) 2 Delphi - Interdisciplinary Review of Emerging Technologies 73 <https://cris.maastrichtuniversity.nl/en/publications/artificial-intelligence-and-democracy-the-impact-of-disinformatio> accessed 19 March 2021.

97 In this sense also Burkell and Regan (n 14).

98 Bayer (n 8).

99 This observation is especially valid in relation to audio-visual media, whose programmes are often broadcast very widely, confirmed in *Informationsverein Lentia and Others v Austria* [1993] ECtHR 13914/88; 15041/89; 15717/89; 15779/89; 17207/90 [38]; *VEREIN GEGEN TIERFABRIKEN SCHWEIZ (VgT) v. SWITZERLAND* (n 78) para 73.

100 Saikat Guha, Bin Cheng and Paul Francis, 'Challenges in Measuring Online Advertising Systems', *Proceedings of the 10th annual conference on Internet measurement - IMC '10* (ACM Press 2010) <http://portal.acm.org/citation.cfm?doid=1879141.1879152> accessed 19 March 2021; Balázs Bodó, Natali Helberger and Claes H de Vreese, 'Political Micro-Targeting: A Manchurian Candidate or Just a Dark Horse?' (2017) 6 Internet Policy Review <https://policyreview.info/articles/analysis/political-micro-targeting-manchurian-candidate-or-just-dark-horse>

responsibilities on individual users to recognise false and misleading political ad strategies.[101] To the extent that these concerns counter the goal of promoting public debate and free elections, one could argue that there is more room for regulation to strengthen the position of users (voters).[102]

26 The third aspect is the *commercialisation* and platformisation of online political advertising that we discussed above. In the grey area between commercial and political speech, the court has so far had to decide whether the commercial or public interest contribution of the speakers themselves was overweighted. The situation of online political advertising on social media platforms is different insofar as it is a commercial party that offers, as part of a commercial service, political speakers the opportunity to use its communication infrastructure and insights into the personal and political preferences of its users. Though Facebook and Google, for example, have some additional authorisation requirements for political and issue advertising,[103] both commercial and political ads are managed via the same business manager. The sale of online political advertising as a service by platforms favours the emergence of new practices, but also endangers the fairness and integrity of the democratic process by, for example, making it easier for foreign entities to buy political advertising, parties other than political parties to buy ads under false or misleading identities, etc.[104] The distinct roles and interests of, on the one hand, political advertisers and, on the other hand, online platforms suggest the need for further differentiation, including from an Art. 10 ECHR perspective, particularly in situations in which the selling of political advertising is "just another form of advertising".

accessed 19 March 2021; Facebook said in October that all content posted by politicians and political candidates, including paid advertising, would be exempt from any of the fact checking for intentionally misleading content, exception: voter suppression: Kate Cox, 'Misleading Political Ads Are the User's Problem to Avoid, Facebook Says' (*Ars Technica*, 27 January 2021) <https://arstechnica.com/tech-policy/2020/01/misleading-political-ads-are-the-users-problem-to-avoid-facebook-says/ 2/4>.

101 Burkell and Regan (n 14); Paddy Leerssen and others, 'Platform Ad Archives: Promises and Pitfalls' (2019) 8 Internet Policy Review <https://policyreview.info/articles/analysis/platform-ad-archives-promises-and-pitfalls> accessed 19 March 2021.

102 See also *CASE OF DEMUTH v. SWITZERLAND* (n 86).

103 https://www.facebook.com/business/help/975570072950669?recommended_by=167836590566506 ; https://support.google.com/adspolicy/answer/6014595?hl=en.

104 Leerssen and others (n 101).

E. Existing initiatives to regulate online political targeting

27 The current EU approach to the regulation of online political targeting rests on three pillars, namely protecting the personal data of voters against unfair forms of processing, increasing transparency and regulating disinformation, with enhancing transparency again an important priority.[105] Regarding the last-mentioned, so far the main regulatory instrument to deal with disinformation, and in that context also with online political microtargeting on social media platforms, is the EU Code of Practice on Disinformation: a co-regulatory initiative to set some standards regarding transparency, cooperation with authorities and academics, fact-checking and automated content moderation.[106] Signatories promise to, among other things, make efforts to explain to users why they have been targeted and who is behind the targeting. As a result of the Code, and other initiatives to exert public pressure, the major platforms have also created so-called ad archives to complement their more user-facing transparency measures.[107] The importance of transparency requirements is also underlined in the EC's recommendation from 2018 and in statement 2/2019 by the EDPB.[108] First evaluations of the Code by ERGA[109] and the EC

105 Iva Nenadić, 'Unpacking the "European Approach" to Tackling Challenges of Disinformation and Political Manipulation' (2019) 8 Internet Policy Review <https://policyreview.info/articles/analysis/unpacking-european-approach-tackling-challenges-disinformation-and-political> accessed 25 February 2021; European Commission, 'European Democracy Action Plan' Text 2 <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250> accessed 19 March 2021.

106 European Commission, 'Code of Practice on Disinformation' (2018) <https://ec.europa.eu/digital-single-market/en/code-practice-disinformation> accessed 19 March 2021.

107 Leerssen and others (n 101).

108 European Commission, Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, https://ec.europa.eu/info/sites/info/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf EDPB, statement 2/2019 on the use of personal data in the course of political campaigns, adopted on 13 March 2019, article 5. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf.

109 European Regulatory Group for Audiovisual Media Services (ERGA), 'Report of the Activities Carried out to Assist the European Commission in the Intermediate Monitoring of the Code of Practice on Disinformation (ERGA Report)' (2019)

itself[110] have revealed a number of shortcomings in implementation and compliance with the Code, prompting the EC to announce additional legislation on transparency in political advertising as part of the European Democracy Action Plan and an update of the Code.[111] In addition, the proposed Digital Service Act (DSA) includes mandatory provisions on online advertising transparency[112] and ad archives for platforms.[113] It is worth noting that the proposed rules in the DSA make no distinction between online commercial and online political advertising transparency.

28 More specifically in the context of EU elections, the EC also issued a number of recommendations, again with a strong focus on awareness- and transparency-enhancing measures.[114] The issue of data protection in political campaigns has also received some regulatory attention. The EDPB has stated that significant effects can occur in the context of microtargeting when it significantly affects the circumstances, behaviour or choices of the individual.[115] Building further upon this opinion, the EC has stated that political microtargeting, given the significance of the exercise of the right to vote, has the effect of stopping people from voting or making people vote in a specific way, could be a significant effect in the sense of Art. 22 GDPR.[116] This would make Art. 22 GDPR applicable in the case of political microtargeting.

29 In Strasbourg, the Committee of Ministers of the Council of Europe (CoE) recommended also applying its recommendation on measures concerning election campaigns[117] to non-linear audio-visual media services.[118] Though it does not specifically mention online political advertising, the recommendation more generally advises extending national rules on the fair, impartial and balanced reporting of elections to on-demand and similar services.[119] More specifically geared towards online political advertising, the CoE's Declaration on the manipulative capabilities of algorithmic processes emphasises the need to assess the applicability of existing regulatory frameworks on political communication also to the online world, and declares that "it should be ensured that voters have access to comparable levels of information across the political spectrum, that voters are aware of the dangers of political redlining, which occurs when political campaigning is limited to those most likely to be influenced, and that voters are protected effectively against unfair practices and manipulation."[120]

30 At the level of member states, the few existing initiatives to regulate online political targeting can be divided into four types. First, some focus on the *application and enforcement of data protection rules*, such as the call by the Information Commissioner's Office (ICO) for a statutory code on the use of personal information in targeted political advertising (which, at the time of writing, has not yet led to concrete

<https://erga-online.eu/wp-content/uploads/2019/06/ERGA-2019-06_Report-intermediate-monitoring-Code-of-Practice-on-disinformation.pdf>.

110 European Commission, 'Assessment of the Code of Practice on Disinformation – Achievements and Areas for Further Improvement' (2020) Text SWD(2020) 180 final <https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement> accessed 19 March 2021.

111 European Democracy Action Plan: Remarks by Vice-Pres-ident Vera Jourová' (Brussels, 12 March 2020) <https:// ec.europa.eu/commission/presscorner/detail/en/ SPEECH_20_2308> accessed 19 March 2021.

112 European Democracy Action Plan: Remarks by Vice-Pres-ident Vera Jourová' (Brussels, 12 March 2020) <https:// ec.europa.eu/commission/presscorner/detail/en/ SPEECH_20_2308> accessed 19 March 2021.

113 Proposed Art. 30 DSA, applicable only to so-called Very Large Online Platforms.

114 European Commission, 'COMMISSION RECOMMENDATION of 12.9.2018 on Election Cooperation Networks, Online Transparency, Protection against Cybersecurity Incidents and Fighting Disinformation Campaigns in the Context of Elections to the European Parliament' (2018) C(2018) 5949 final <https://ec.europa.eu/info/sites/info/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf>.

115 Article 29 Working Party, 'Guidelines For Automated Decision Making and Profiling for the Application of Regulation (EU) 2016-679), finalised on 3 October 2017, last edited and adopted on 6 February 2018 WP251rev.01.

116 European Commission, Commission guidance on the application of Union data protection law in the electoral context https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018DC0638.

117 Recommendation No. R (99) 15 of the Committee of Ministers to Member States on measures concerning media coverage of election campaigns, 9 September 1999, https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e3c6b

118 Recommendation CM/Rec(2007)15 of the Committee of Ministers to Member States on measures concerning media coverage of election campaigns, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805d4a3d

119 Ibid.

120 Council of Europe, Declaration on manipulative capabilities of algorithmic processes (n 10).

legislator proposals).[121] Then there are regulations that *mandate more user- or public-facing transparency*. The French Law of 22 December 2018, for example, obliges online platforms to inform its users about the identity of the entity behind the advertisement, the amount paid for the advertisement and the use of the user's data in the advertisement campaign during election times.[122] Article 7 of the Slovenian Law on Election and Referendum Campaigns has similar transparency requirements for all types of 'media publishers.'[123] The UK has announced an open consultation on proposals for transparency requirements for online political campaigns. This includes the obligation of advertiser identification.[124] Ireland [125] and the Netherlands[126] are debating similar initiatives.

31 Some countries follow the recommendation of the Council of Europe and consider the *application of existing rules on paid political advertising in the mass media to online advertising*, such as in the UK, where the Electoral Commission has stated that spending limits imposed on political advertisements apply to advertising of any kind, including advertising on online platforms.[127] Similarly, France extended its Electoral Code with a prohibition on online political advertising during election periods.[128]

32 Then there are initiatives that address more generally the *online distribution of false or misleading information*. An example is the controversial French Law Against the Manipulation of Information, which will be discussed in more detail in a moment.[129] In addition to transparency obligations (including the operation of ad archives), the law stipulates that during the three months preceding an election, judges can, upon the request of a public prosecutor, political candidate or party, or another interested person, decide about "inaccurate or misleading allegations or imputations of a fact likely to alter the sincerity of the upcoming ballot [and that] are disseminated in a deliberate, artificial or automated and massive manner by means of an online communication service to the public."[130] In a similar fashion, the French Media Authority (Conseil Supérior de l'Audiovisuel or CSA) is entitled to act against the dissemination by foreign state actors of false information that is likely to alter the fairness of a ballot.[131] This last example of rules that target the dissemination of false or misleading information in political communication echoes a growing array of national rules to counter the spread of mis- and disinformation, also spurred by the Covid crisis.[132]

33 While most of the regulatory initiatives so far are either in the realm of data protection law or follow the tradition of regulating political advertising in the mass media, some of the new regulatory approaches can be argued to show elements that are better known from the realm of consumer law. Examples are the requirements to inform users that a message

121 ICO, 'Democracy Disrupted? Personal Information and Political Influence' (2018) <https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf>.

122 Art. 11, Titre III : DEVOIR DE COOPÉRATION DES OPÉRATEURS DE PLATEFORME EN LIGNE EN MATIÈRE DE LUTTE CONTRE LA DIFFUSION DE FAUSSES INFORMATIONS (Articles 11 à 15), LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000037847559/..

123 The Law on election and Referendum: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4749.

124 Government of UK (August 2020): Open consultation – Transparency in digital campaigning: technical consultation on digital imprints, https://www.gov.uk/government/consultations/transparency-in-digital-campaigning-technical-consultation-on-digital-imprints.

125 Government of Ireland (November 2019): Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation – Progress Report, https://assets.gov.ie/39188/8c7b6bc1d0d046be915963abfe427e90.pdf.

126 In the Netherlands, the Staatscommissie Hervorming Parlamentair Stelsel did signal the potential positive but also negative consequences of political microtargeting as well as the fact that so far online political microtargeting is unregulated. The committee hence argued in favour of a new law on political parties that would, among other things, tackle political microtargeting, Staatscommissie Parlementair Stelsel and J Remkes, *Lage drempels, hoge dijken: democratie en rechtsstaat in balans: eindrapport* (2018).

127 The Electoral Commission, 'Digital Campaigning Increasing Transparency for Voters' (2018) <https://www.electoralcommission.org.uk/sites/default/files/pdf_file/Digital-campaigning-improving-transparency-for-voters.pdf>.

128 Art. 52 Electoral Code, https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070239/.

129 *PROPOSITION DE LOI relative à la lutte contre la manipulation de l'information*. 2018.

130 Art. 1 ibid, amending L. 163-2.-I. of the Electoral Code.

131 Art. 6 ibid, amending article 33-1 of the law n ° 86-1067 of September 30, 1986 relating to the freedom of communication.

132 For a comparative overview, see European Regulatory Group for Audiovisual Media Services (ERGA), 'NOTIONS OF DISINFORMATION AND RELATED CONCEPTS (ERGA Report)' (2019) <https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf>..

is an advertising message and to provide the identity of the issuer of that message,[133] to clearly separate editorial from commercial content[134] and to protect users from unfair and misleading advertising.[135]

34 The explicit reference to possible lessons to learn from the way commercial advertising practices are regulated is more pronounced outside Europe, notably in Australia and Canada. In Australia, the Legal, Constitutional and Administrative Review Committee of the Queensland Parliament suggested truth in advertising rules that were explicitly inspired by the rules and methods developed to deal with misleading or deceptive advertising under section 52 of Australia's Trade Practices Act.[136] In the United States, where the Fair Trade Act does not apply directly to political advertising, a number of states have adopted laws against misleading political advertising, inspired by, inter alia, the way commercial advertising has been regulated.[137] Some of these laws have been struck down by courts because of First Amendment concerns, pointing again to the difficult tension between the constitutional protection granted to political speech and the use of advertising practices better known from commercial advertising.[138] And yet, as we have argued in the previous sections, in online political advertising, and political targeting on social media platforms in particular, commercial and political elements of advertising are merged in ways that seem to broaden the margin for states to draw lessons from a long tradition of protecting users against unfair marketing practices in commercial advertising law. This is not to say that commercial advertising is or should be applied to online political advertising. However, some of the approaches and instruments developed under commercial advertising law, we argue, can usefully inspire our thinking about future approaches to the regulation of political microtargeting (within the limits of Art. 10 ECHR). This is what we try to do in the next section.

F. Possible takeaways from the regulation of commercial advertising for political advertising regulation

35 The previous sections have demonstrated that although the regulation of online commercial and online political advertising and targeting have followed very different paths and were born out of different regulatory traditions, in practice both types of advertising have many elements in common. An important common element is the use of data-driven persuasion strategies that trigger new concerns about the ability of consumers, aka voters, to protect themselves from unfair forms of advertising. We have also demonstrated that regulating fairness in advertising in the advertiser–consumer relationship has a long tradition in the regulation of commercial advertising. This section explores whether there are possible takeaways from the regulation of commercial advertising and, if so, how they could inspire the future regulation of political advertising.

I. Takeaway 1: The need for a pragmatic and flexible definition of the scope of regulation

36 One of the difficulties of regulating online political advertising is that of defining what a political advertisement is, to what extent also issue-based advertising is covered and exactly what acts fall under the notion of political advertising—in other words, the scope of the regulation.[139] The EU Code of Practice on disinformation defines political advertising as "advertisements advocating for or against the election of a candidate or passage of referenda in national and European elections", while issue-based advertising is not defined. In

133 Art. L. 163-1. of the French Electoral Code, to give but one example.

134 HLEG, *A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation* (Publications Office of the European Union 2018) <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

135 France, L. 163-2.-I. of the Electoral Code.

136 George Wiliams, 'Truth in Political Advertising Legislation in Australia' (1996) Research Paper 13 1996-97 2.

137 For an overview, Campaign Fair Practices Law (Is There a Right to Lie?', 2014, <https://www.ncsl.org/research/elections-and-campaigns/campaign-fair-practice-laws-is-there-a-right-to-lie.aspx> accessed on 19 March 2021.

138 Matt Vasilogambros, Political Candidates Don't Always Tell the Truth (And You Can't Make Them), 2019 Pew Research, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/03/21/political-candidates-dont-always-tell-the-truth > accessed on 19 March 2021.

139 Leerssen and others (n 101); Tom Cardoso, 'Google to Ban Political Ads Ahead of Federal Election, Citing New Transparency Rules' *The Globe and Mail* (4 March 2019) <https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/> accessed 19 March 2021.

European member states, the definitions of online political advertising vary greatly between actor-based approaches (who is the advertiser), whether the advertising is paid/not paid for and purpose-driven approaches (to promote a political party or political end) and are typically geared towards banning or restricting certain practices from the onset.[140] Similarly, there are huge differences in the definitions that platforms handle.[141]

37 The ambiguity of any definition of 'advertising' is a problem that the regulation of political advertising shares with commercial advertising regulation. Unfair commercial practices law opted for a broad definition: 'any act, omission, course of conduct or representation, commercial communication including advertising and marketing, by a trader, directly connected with the promotion, sale or supply of a product to consumers'.[142] But, and this is important, for the rules to apply, practices must 'materially distort the economic behaviour of consumers'.[143] In other words, when regulating fairness in commercial advertising, the law acknowledges that commercial persuasion can take many forms. The proof lies in the potential *effect* that a particular act of communication has on the consumers' decision-making process and whether that effect is achieved by fair or unfair means.

38 This could be a first valuable lesson for the regulation of online political targeting. Instead of trying to define upfront in much detail what is or is not an impermissible political ad, an alternative approach would be to opt for a fairly broad and inclusive definition, and subsequently make the assessment of the lawfulness of the political ad dependent upon the potential effect on different voters and the electoral competition.[144] This is because from a citizen's perspective, political advertising comes in different shapes and fairness has a different meaning for each type of ad. One subset of ads are concerned with maximising engagement and turnout, or dampening it by suggesting that elections are foregone conclusions. A second subset focus on candidates, either an incumbent or an opposing candidate. A third subset focus on the issue and policy standpoints of parties. Each type of ad comes with a different set of considerations about what fairness entails. For the first, for example, cueing citizens against turning out to vote is potentially an infringement of electoral fairness. For the second type mentioned above, spreading dis- or misinformation about opposing candidates might be an infringement of electoral fairness.

39 A relevant political practice could be then defined as 'any act, conduct, representation or advertising of political issues and standpoints, candidates, party programmes or part of such programmes that is directly connected with the promotion of a political party, political programme or candidate to citizens, or the engagement in the act of voting.' Such a broad definition would also acknowledge that political advertising messages themselves could not only potentially constitute unfair behaviour, but so too could the sponsoring of certain political events, websites or Facebook groups, or the creation of persuasion profiles of particularly vulnerable citizens (see below)—as long as it has the potential to affect voting decisions. For the same reason, acts by non-party political actors would be covered, as long as the primary aim is to directly influence voter decision-making. It would exclude instances of mere journalistic reporting about political events to the extent that this reporting is, in conformity with journalistic ethics of objectivity and unbiased reporting, not directed at having a particular effect on voters' behaviour. The advantage of such an approach is that it would be flexible enough to include current and future forms of online political advertising and account for the fact that the process of political opinion and preference forming can be influenced in many different ways and by many actors (including non-party actors). The legislator could then qualify under which conditions such practices have an non-permittable effect on voters or elections, for example because they are misleading or dissuading voters from voting. The drawback of such an approach is that it would be very inclusive and ultimately would require an authority that, similar to the judge in unfair commercial practices law, is authorised and competent to assess practices upon their fairness. The advantage of such an approach would be that it is the judge, bound by fundamental rights law, and not a social media platform that decides about the permissibly of a political ad.

140 European Regulatory Group for Audiovisual Media Services (ERGA) (n 132) 41–42.

141 For an excellent overview, see Center for Information, Technology and Public Life, Platform Advertising, 2020, <https://citapdigitalpolitics.com/wp-content/uploads/2020/05/Platform-comparison-tables.001.jpg> accessed on 19 March 2021.

142 Art. 2 (d) UCP

143 Art. 2 (e) UCP.

144 As hinted at also in the EU Code on Disinformation, calling for the need to develop a working definition on "issue-based advertising" "which does not limit reporting on political discussion and the publishing of political opinion and *excludes commercial advertising*" European Commission, 2021 (n 106), highlight by the author.

II. Takeaway 2 – The information that users need to assess the fairness of targeted advertising depends on the situation and the concrete targeting strategy

40 One of the key principles of unfair commercial practices law is that for commercial practices to be fair, they need to provide the consumer with all the relevant information that she needs to take an informed decision in a particular situation. On the contrary, practices that omit relevant information or contain false information or truthful information that is presented in a way that can still deceive the consumer, are considered misleading and are thus banned.[145] A necessary precondition is that the provision of misleading or the omission of relevant information has caused or is likely to cause the consumer to take a decision that she otherwise would not have taken. The reason for this qualification is that unfair commercial practices law protects not truth in advertising in abstract, but the ability of consumers to make autonomous and well-informed decisions.

41 Using political targeting strategies to mislead the voter is also a key concern in the discussion around online political targeting (see section B), but what information voters need to assess the fairness of a practice depends on the practice. Earlier we distinguished between political ads that are aimed at maximising engagement and turnout, focus on candidates or focus on the issue and policy standpoints of parties. Regarding the latter category, Zuiderveen Borgesisus et al. (2018), for example, warn of a situation in which online political targeting can be used in such a way that a party presents itself falsely as a one-issue party so that each individual receives only information on the issue that she is likely to be most interested in, while omitting information on other issues.[146] Arguably, for a voter to take an informed decision in such a situation she would need to have an idea of the broader set of issues a party stands for. This information is different from the information a voter might need for ads that fall into the second category and cue citizens against turning out to vote. Here, information about the party that commissioned the ad is relevant to assess the ad upon its value. And regarding the first category, ads that are concerned with maximising turnout, information about the strategies used might be the most relevant information for voters. For example, empirical research in the United States[147] found that 86% of respondents thought it was not okay to be targeted with political ads (as compared to 61% being uncomfortable with commercial targeting). Similar research in Europe has demonstrated that many people are concerned about online political targeting.[148] Turow et al. found that "between 57% and 70% of Americans do say it would decrease the likelihood of voting for their candidate either a lot or somewhat".[149] In other words, it can actually matter for the decision of a voter what techniques are used to maximise engagement, and hence having that information is necessary to take an adequately informed decision. Similarly, one could also argue that to be able to take an informed decision, voters should learn whether they are subject to A/B testing (meaning the message has been optimised for resonance rather than political content[150]), whether a political message has been automatically generated by AI or a bot to respond to individual profiles (rather than by a human campaigner) whether an ad is based on custom audiences, or whether it is paid for or not.

42 How is that approach distinct from current calls about the need for more voter transparency? The proposed measures at the national or European level require that voters should be informed about a number of items. For instance, the EU Code of Practice calls for transparency "also with a view to enabling users to understand why they have been targeted by a given advertisement".[151] The Council of Europe recommends revealing to users the "advertising purpose, the methods by which they

145 Arts. 6 and 7 Unfair Commercial Practices Directive.

146 Borgesius and others (n 6).

147 Joseph Turow and others, 'Americans Roundly Reject Tailored Political Advertising' (2012) 30 Annenberg School for Communication, University of Pennsylvania.

148 Tom Dobber and others, 'Spiraling Downward: The Reciprocal Relation between Attitude toward Political Behavioral Targeting and Privacy Concerns' (2019) 21 New Media & Society 1212.

149 Interestingly, the researchers also found that the percentage of voters saying that being targeted would decrease their likelihood of voting for that particular candidate was the highest in the context of social media, and 85% agreed or strongly agreed that they would be angry if they found out that Facebook was sending them ads for political candidates based on profile information they had set to private (Turow et al. (n 147)) (note that the survey took place even before the Cambridge Analytics scandal).

150 Jamie Bartlett, Josh Smith, and Rose Acton, 'The Future of Political Campaigning' (ICO 2018) <https://ico.org.uk/media/2259365/the-future-of-political-campaigning.pdf> accessed on 19 March 2021.

151 European Commission, 'Code of Practice on Disinformation' (n 106).

are targeted to citizens, and their funding".[152] Draft Art. 24 DSA requires an advertisement to be labelled as such and the provision of the name of the person on whose behalf the advertisement is displayed and meaningful information about the main parameters used to determine the recipient. And the recent French Law relating to the manipulation of information requires consumers to be explicitly informed about the identity of the political advertiser as well as the way personal data is being used.[153] The approach suggested here is less deterministic from the onset. It is a flexible approach that leaves room to take into account the concrete informational needs of users by asking: *what kind of information* and *in which form* do voters *need* to take informed decisions in this particular advertising context? In other words, this is a user-centric approach that is oriented a particular situation, as opposed to the 'long list-approach' that can be found in many of the current rules (and proposals) for regulating online political advertising. Not only misrepresenting such information, but also leaving out necessary information should be considered unfair. Such a more flexible approach would also allow to interpret the concrete information needs of voters in the light of the insights of the most recent empirical findings on users' perceptions and information requirements for taking informed decisions.[154]

III. Takeaway 3 – It should be up to judges, not platforms, to assess whether claims made are false or misleading

43 A more controversial issue than transparency is the evaluation of truth in advertising in the message itself. Much has been written on the topic of disinformation and the way it could threaten the democratic process,[155] as well as the risk of regulatory intervention interfering with fundamental rights, including freedom of expression interests.[156]

44 Engaging in commercial communication that is false or deceptive can be considered an unfair commercial practice, and thus be banned provided it causes or is likely to cause the consumer to take a decision that the consumer would otherwise not have taken (e.g. not only the message as such but also the potential effect on the consumer matters).[157] Arguably, in such a situation, the public interest in trust in a fair and functioning marketplace, and the protection of the autonomy of consumers, carries more weight than potential interferences with the freedom of expression interests of commercial advertisers. Ultimately, however, it is the judge who is tasked with this decision.

45 In the case of political advertising, this balance can tip, at least because of the higher level of protection under Article 10 ECHR and the reduced margin of appreciation of public authorities (see also section C). This is arguably less true for political advertising that is clearly unlawful (e.g. because it is defamatory) or false and purposefully harmful (so-called disinformation), including false deepfakes.[158] In all the cases the real difficulty lies in the grey zone of communication that is neither clearly false nor intentionally harmful. Any regulation or standards on unfair political practices would need to avoid a situation in which the scrutiny of such practices results in prohibited censorship or interference with political speech rights.

46 Interestingly, in Google's announcement of the changes to its political advertising rules, the company bans practices that essentially echo the principles of unfair commercial practices law, including "misleading claims about the census process, and ads or destinations making demonstrably false claims that could significantly undermine participation

152 Council of Europe, Conclusions of the Council and of the Member States on securing free and fair European elections Brussels, 19 February 2019 6573/19

153 Art. L. 163-1 of Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

154 See for the case of commercial practices: Chris Willett, 'Fairness and Consumer Decision Making under the Unfair Commercial Practices Directive' (2010) 33 Journal of Consumer Policy 247.

155 Claire Wardle and Hossein Derakhshan, 'INFORMATION DISORDER: Toward an Interdisciplinary Framework for Research and Policy Making' (Council of Europe 2017) DGI(2017)09.

156 Council of Europe, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (Council of Europe 2018).

157 Art. 6 (1) Unfair Commercial Practice Directive: 'A commercial practice shall be regarded as misleading if it contains false information and is therefore untruthful or in any way, including overall presentation, deceives or is likely to deceive the average consumer, even if the information is factually correct, in relation to one or more of the following elements, and in either case causes or is likely to cause him to take a transactional decision that he would not have taken otherwise'.

158 Tarlach McGonagle, '"Fake News": False Fears or Real Concerns?' (2017) 35 Netherlands Quarterly of Human Rights 203.

or trust in an electoral or democratic process".[159] The question is: do we want Google to be the arbiter that decides whether political claims are misleading? The heavy criticism about the 'private censorship' of platforms was exactly why Facebook refused to do exactly that, namely assess the content of political messages.[160] Concerns about possible interference with free speech rights is one side of the coin, and the fact that each platform sets a different standard for what it considers fairness in advertising is the other side.

47 One possible takeaway from the approach under unfair commercial practices law is that it should ultimately be up to a judge (or another authority) to make this decision, and this authority must be bound by fundamental rights law and procedural fairness guarantees. Legislators and judges (or similar authorities), not platforms, should evaluate in which situations the fundamental right to speak is outbalanced by the fundamental rights of citizens to form their political opinion free from deceit and false propaganda. Only in this way can a shared and transparent standard of fairness in political advertising develop. Another potential lesson is that with commercial speech, false or potentially misleading claims are never prohibited without also considering their potential effect on the ability of users to take autonomous and informed decisions. This is different from the approach that some member states have taken lately by outright banning or even criminalising certain forms of alleged disinformation in online targeting.[161] Making the effect of a political advertising on the ability of voters to take autonomous decision central could add an extra level of protection against arbitrary decision making and politically motivated censorship.

IV. Takeaway 4 – Walking the fine line between regulating content and the conditions of delivery

48 Distinct from questions about the fairness or legality of a message are questions about the fairness of the way the message is delivered. So far, the predominant approach to protecting voters against unfair forms of delivery of online political advertising focuses on the lawfulness of the way users' personal data are used, or transparency approaches (see section E). A question that the existing approaches discussed in section E are less well prepared to tackle is under which conditions do data-driven targeting political messages exploit structural power imbalances, individual vulnerabilities and advantages in persuasion power. In the European Democracy Action Plan, the EC hints at the possible necessity of "further restricting micro-targeting and psychological profiling in the political context", without being more specific about how this could be done.[162] Again, the approach to the regulation of unfair commercial advertising in general and so-called aggressive practices, in particular, can provide useful inspiration.

49 Perhaps one of the key concerns regarding online political targeting is the risk of voter manipulation and distortion of the democratic process.[163] This is a concern that debates around online political targeting share with discussions on consumer law. Also in consumer law, the use of data analytics and 'persuasion profiles'[164] has raised concerns regarding the protection of the autonomy of consumers, and the potential unfairness of these practices.[165] In its last guidance on the application of the Unfair Commercial Practices Directive, the European Commission made clear that certain forms of data-driven targeting—notably targeting that exerts undue influence or constitutes an aggressive practice—can constitute an unfair commercial practice.[166] And yet, although there is

159 'An Update on Our Political Ads Policy' (n 33).

160 Associated Press, 'Facebook Refuses to Restrict Untruthful Political Ads and Micro-Targeting' (*the Guardian*, 9 January 2020) <http://www.theguardian.com/technology/2020/jan/09/facebook-political-ads-micro-targeting-us-election> accessed 19 March 2021.

161 European Regulatory Group for Audiovisual Media Services (ERGA) (n 132).

162 European Democracy Action Plan 2020 (n 112), p. 5.

163 Jean-Baptiste Jeangène Vilme and others, 'Information Manipulation: A Challenge for Our Democracies' (Policy Planning Staff (CAPS, Ministry for Europe and Foreign Affairs), Institute for Strategic Research (IRSEM, Ministry for the Armed Forces)) <Information Manipulation: A Challenge for Our Democracies> see also section B. IV.

164 William D Wells, 'Psychographics: A Critical Review' (1975) 12 Journal of Marketing Research 196; MC Kaptein, *Persuasion Profiling: How the Internet Knows What Makes You Tick* (Business Contact Publishers 2015); William A Gorton, 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy' (2016) 38 New Political Science 61; Burkell and Regan (n 14).

165 Karen Yeung, '"Hypernudge": Big Data as a Mode of Regulation by Design" (Social Science Research Network 2016) SSRN Scholarly Paper ID 2807574 <https://papers.ssrn.com/abstract=2807574> accessed 19 March 2021.

166 European Commission, 'COMMISSION STAFF WORKING DOCUMENT GUIDANCE ON THE IMPLEMENTATION/APPLICATION OF DIRECTIVE 2005/29/EC ON UNFAIR COMMERCIAL PRACTICES

a shared perception that manipulating[167] users is potentially wrong, it is difficult to actually pinpoint the conditions under which doing so is unethical or unlawful. After all, there is also agreement that each form of advertising, commercial or political, is essentially an attempt to persuade and, ultimately, to manipulate users. The challenge is to define the conditions that distinguish between lawful persuasion and unlawful manipulation.

50 Unfair commercial practice law has a long tradition of doing exactly that, namely defining the conditions of unlawful manipulation vis-à-vis lawful persuasion. While the principles of misleading advertising address the existence and abuse of information asymmetries between advertiser and user, the rules on aggressive practices focus on situations where physical or psychological influence is applied in such a way as to reduce a user's freedom of choice, where an advertiser takes advantage of the specific situation of a user,[168] or uses mental or physical force (coercion) or harassment (causing emotional distress while not serving a legitimate purpose).[169] Unfair commercial practices law thereby makes an, important distinction (for our context) between scrutiny of the commercial message itself (i.e. false information about the price or the product itself) and the conditions surrounding the way the message is delivered (i.e. by omitting critical information the consumer needs to be able to assess the message adequately, or by using force, undue influence, etc. to reduce users' actual information choice or autonomy in responding to the message). Under unfair commercial practice law, a message can be aggressive if "in its factual context, taking account of all its features and circumstances, by harassment, coercion, including the use of physical force or undue influence, it significantly impairs or is likely to impair the average consumer's freedom of choice or conduct."[170]

51 The provisions about unfair and aggressive practices in commercial advertising law can be criticised, and rightfully so, for example because of their relative vagueness.[171] And yet the way the law deals with these practices includes a deeper truth, namely that advertising that exploits knowledge of individual biases and susceptibility to persuasion, invades an individual's personal space, [172] as well as forms of economic and intellectual domination[173] or forms of advertising that exert pressure by abusing fears or emotions, [174] are examples of practices that have crossed that precarious line between acceptable persuasion and unacceptable manipulation, particularly when they do so for commercial gain.[175] Unfair commercial practices law for the case of commercial advertising touches on concerns that are also echoed in the literature around online political advertising, particularly in context of so-called psychographic profiling practices (see section B. IV.).

52 Therefore, another important lesson from unfair commercial practices law could also be that the particular messaging strategies can under circumstances have (by design or circumstance) an adverse effect on the ability of consumers to take autonomous decisions and, if they do so, deserve legal scrutiny.[176] Arguably, in the context of online political targeting that distinction is even more relevant because those who formulate the message (and thus engage in political speech) are often distinct from those that distribute it (social media platforms as part of a commercial service) (see

Accompanying the Document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Comprehensive Approach to Stimulating Cross-Border e-Commerce for Europe's Citizens and Businesses, SWD/2016/0163 Final' (n 42).

167 The authors are well aware that manipulation is a very complex notion and that it would go far beyond the scope of this article to provide a more in-depth discussion, for a possible interpretation in the sense of unfair commercial practice law, based on insights from philosophy, see Sax, Helberger and Bol (n 23). More generally: Susser, Roessler and Nissenbaum (n 17).

168 Howells (n 22).

169 Damian Clifford, 'Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making, a True Path to the Dark Side?' (Social Science Research Network 2017) SSRN Scholarly Paper ID 3037425 <https://papers.ssrn.com/abstract=3037425> accessed 19 March 2021.

170 Art. 8 Unfair Commercial Practice Directive.

171 Howells (n 22).

172 Geraint Howells, Hans-W Micklitz and Thomas Wilhelmsson, 'Towards a Better Understanding of Unfair Commercial Practices' (2009) 51 International Journal of Law and Management 69, 76.

173 ibid 77.

174 Willett (n 154) 260.

175 See Dutch Consumer Authority ACM, 'Concept Consultatie-document Leidraad Bescherming van de Online Consument. Grenzen Aan Online Beïnvloeding' (2019) <https://www.acm.nl/sites/default/files/documents/leidraad-bescherming-online-consument.pdf>.

176 UK Electoral Reform Committee 2018, 'Digital Campaigning: increasing transparency for voters' (Electoral Reform Committee, 2018), 31.

section B). This is a subtle but important difference: while political advertisers enjoy, according to the case law of the European Court of Human rights, a high level of protection under Art. 10 ECHR, for social media platforms the selling of advertising services is first and foremost a commercial service. As we have argued above, this arguably leaves states with a larger margin of appreciation to regulate targeting strategies, commercial and political, by social media platforms, and because of the potential effects of psychographic profiling on users' autonomous decision making, there is also a clear public interest in doing so. The concept of 'aggressive practices' and the long experience of national courts in identifying the conditions under which advertisers engage in strategies to exert undue influence in the sense of unfair commercial practice law could provide useful inspiration and therefore deserves further exploration.

V. Takeaway 5 – Some persuasion strategies are simply unacceptable and should be banned altogether

53 Much of the current regulatory discourse is focused on the question of how to govern online political targeting practices, beginning with the question of how to make them transparent and observable in the first place.[177] Nevertheless, as important as more transparency in this area may be, another, even more important question remains unanswered: once we are in a position to observe all instances of political advertising (e.g. in the form of ad archives), how do we decide which practices are acceptable in a democratic society, and how should judges or regulatory authorities respond? The above discussion has already pinpointed a number of possible criteria, inspired by insights from a long history in the law of identifying unfair forms of advertising. The experience with regulating unfair commercial advertising, however, also teaches us that, in addition to the more ambiguous cases, there are instances of advertising that are simply unacceptable in a just society.

54 In unfair commercial practices law, these instances of unacceptable advertising practices are listed in the Annex to the Unfair Commercial Practices Directive. The Annex includes a wide range of forms of commercial communication that are always considered unfair. As arbitrary as this list may be, the message is clear: under certain circumstances there is a role for the regulator to ban practices that conflict with the idea of a functioning and fair marketplace. Do we need a similar list for political advertising and, if so, which instances should be included in such a list? The following section offers a number of suggestions.

55 One example to consider in that context could be targeted messages that are directed at demobilising voters,[178] giving the example of messages targeted at African-American voters with advertisements that recalled Hillary Clinton's earlier remarks about calling African-American males 'super predators', thereby using microtargeting to suppress voter turnout for their opponents.[179] Arguably, such a practice is in conflict with key principles of electoral fairness, such as the principle of equality of opportunity discussed above, and also triggers concerns about manipulation of the public discourse—thereby questioning their protection under fundamental rights law. In such a situation, is transparency enough to address the potentially anti-democratic effects? Or should society take a stance and ban this form of political targeting?

56 The reverse practice—that is, targeting voters without them being aware that they are being targeted with specific political messages (so-called dark posts)—could be another example of a practice that deserves critical discussion. Political messages like these potentially bypass the broader public discourse,[180] and thus are in conflict with established criteria of fair elections.[181] Declaring dark posts unfair could build on long-standing experience in the realm of commercial advertising, namely that advertising practices that are invisible to users (because they are unmarked or camouflaged

177 Leerssen and others (n 107).

178 Borgesius and others (n 6).

179 Example described in: Joshua Green and Sasha Issenberg, 'Inside the Trump Bunker, With Days to Go' *Bloomberg* (27 October 2016) <https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go> accessed 19 March 2021.

180 D Sunshine Hillygus and Todd G Shields, *The Persuadable Voter: Wedge Issues in Presidential Campaigns* (Princeton University Press 2009).

181 As Jess Garland, director of policy at the Electoral Reforms Society asserts: "These techniques as well as playing into tribalism and polarisation in politics are also moving democratic life outside of our shared public space." "With Facebook election ad spend soaring, who is controlling our elections?', 2019, Shropshire Star, <https://www.shropshirestar.com/news/politics/2019/05/21/who-is-controlling-our-elections/> accessed on 19 March 2021.

as editorial messages) make informed autonomous decision-making essentially impossible,[182] and because of that are considered unfair.

57 Another, related potential contender for a political targeting practice that is potentially always unfair is that of redlining,[183] in the sense of focusing on 'profitable' sections of the voting population and ignoring others, either because they are unlikely to vote for a candidate or because they are seen as secure votes. Kreiss warns that political advertisers would routinely "redline the electorate, ignoring individuals they model as unlikely to vote, such as unregistered, uneducated, and poor voters".[184] Communication scientist Joseph Turow points to another concern in this context, one that he calls "rhetorical redlining", namely the practice of presenting voters with "ads from candidates based on what the campaign's statisticians believe they want to hear—shutting them off from messages that the statisticians determined might make them waver in their support".[185] On the one hand, it could be argued that targeting political messages at particular groups in society can be a way to involve those who have shown less interest in politics, and thereby increase engagement. On the other hand, however, redlining can and in practice most likely will be used in such a way as to exclude them.[186] Such a practice seems very much at odds with the key principles of a democratic society, which requires a sphere of mutual shared values and equality: "The dynamics of deliberative democracy are characterised by the norms of equality and symmetry; everyone is to have an equal chance of participation".[187] As Bayer argues, practices like these potentially also conflict with voters' right to receive information.[188] Reasons enough to at least question their desirability in a democratic 'marketplace of ideas'.

58 Potentially, there are also other ways of delivering political advertising messages that are so problematic from the perspective of voter autonomy and fundamental rights, including the right to receive information, that they should be banned. A practice that is being very critically discussed in that context is again that of psychographic profiling. The main focus of psychographic profiling is not so much the political message itself as figuring out ways to affect how users internalise and respond to the message. As Burkell and Regan explain, in such situations it is far more difficult for voters to detect and counteract a message, particularly if it speaks to unconscious biases.[189] In such situations, constitutional concerns about interfering with the political speech of political advertisers or the commercial interests of platforms are more easily outweighed by the concerns of voters to receive information and fair elections than when more 'simple' targeting strategies are concerned with matching the right content with the right people. In a similar vein, a suggestion exists to limit the types of data that may be used for targeting. For example, Jaursch suggests operating a set list of data that may be used for ad targeting, such as electoral district or age and gender, combined with a ban on using certain other kinds of data, such as inferred data or purchased consumer data.[190] Again, doing so would amount to a restriction not so much on political speech itself, as on the way it is delivered.

59 This list is far from complete and merely serves as an argument that it may be time to develop clearer guidance as to what practices are acceptable or inacceptable in a democratic society, and that for the sake of respect for fundamental rights, such guidance needs to be transparent and prescribed by law.

G. Conclusion

60 At the heart of our proposal is the argument that data-driven targeted political advertising can not

182 Compare Unfair Commercial Practices Directive, Annex, No. 11.

183 Political communication expert Prof. Phil Howard defines political redlining as "the process of restricting our future supply of political information with assumptions about our demographics and present or past opinions". Philip N Howard, *New Media Campaigns and the Managed Citizen* (Cambridge University Press 2005) <https://www.cambridge.org/core/books/new-media-campaigns-and-the-managed-citizen/6D88539C6FD25C7026A721DF9C9AC09D> accessed 19 March 2021.

184 Daniel Kreiss (n 8).

185 Turow et al. (n 147) 72.

186 Gorton (n 164); Howard (n 183) 131.

187 Peter Dahlgren, 'Doing Citizenship: The Cultural Origins of Civic Agency in the Public Sphere' (2006) 9 European Journal of Cultural Studies 267; Bernard Manin, Elly Stein and Jane Mansbridge, 'On Legitimacy and Political Deliberation' (1987) 15 Political Theory 338. These practices are potentially also at odds with the principles of inclusive and equal elections, as codified e.g. in the Venice Code of Good Practices in Electoral Matters.

188 Bayer (n 8).

189 Burkell and Regan (n 14) 8.

190 Julian Jaursch (n 14) 29. Google, for example, has already adopted this approach by limiting targeting options to age, gender and postal code.

only distort the conditions for fair competition of ideas and opinions between political parties, but also be athreat to democracy because such a practice can impact the ability of citizens to make free, autonomous and informed political decisions. Arguably, and as in the commercial market, the marketplace of ideas can only function if citizens can take free and autonomous decisions and are adequately protected against deception, manipulation and other unfair and misleading practices.[191]

61 So far, evaluating the fairness of political microtargeting practices has very much been a process driven by individual platforms with Google, Twitter and Facebook all developing their own standards of what they consider fair or unfair advertising. As we saw earlier, these standards differ considerably, also over time, with Twitter imposing a general and very broad ban on all paid political advertising, Google banning certain forms of microtargeting and Facebook essentially adopting a liberal approach. The lack of any benchmarks or commonly agreed upon procedures to assess fairness in political advertising is in the best case confusing for voters, political advertisers and regulators, a situation that is not healthy for the political debate. In the worst case, this is a situation that promotes "platform shopping" and migration to the least strict and responsible platforms, including some less trustworthy ones.[192] Interestingly, when reviewing some of the suggestions made in recent policy initiatives, reports and documents, a trend towards identifying certain elements of fair or unfair online political advertising practices is already observable. However, this is very much an ad hoc process, without any clear conceptual approach. What is needed right now is a method of identifying evaluation criteria or standard benchmarks regarding which online political advertising practices are potentially unfair, also beyond the ambit of one particular platform. We have argued that the experiences with unfair commercial practices could serve as a useful conceptual frame to build on.

62 As this article has demonstrated, there are a number of lessons to be learned from a long legal tradition of dealing with unfair commercial advertising, and of unfair commercial practices law in particular, including:

1. The need for a pragmatic and flexible definition of the scope of political advertising regulation.
2. The information that users need to assess the fairness of targeted advertising depends on the situation and the concrete targeting strategy.
3. It should be up to judges, not platforms, to assess whether claims made are false or misleading.
4. Political persuasion can exert undue forms of influence and could thus be unfair.
5. Some persuasion strategies are simply unacceptable and should be banned altogether.

63 Political advertisers are learning from the experience of commercial advertisers with online targeting strategies. It is time that those making policies and rules for political advertising learn from a long tradition of evaluating fairness in commercial advertising law.

191 See also European Commission for Democracy Through Law (n 4).

192 Lauren Feiner, 'Google Changed Its Targeting Policies to Shine a Light on Political Ads, but Campaigns Are Now Eyeing More Opaque Platforms' (*CNBC*, 8 December 2019) <https://www.cnbc.com/2019/12/08/google-policy-change-has-political-advertisers-looking-elsewhere.html> accessed 19 March 2021.

Capacity of EU competition law to promote patent pools: A comparative study

by **Maryam Pourrahim***

Abstract: Patent pools have proved to offer significant efficiency to both licensors and licensees as they provide a one-stop-shop for a patents package, reduce transaction costs, and improve access to Standard Essential Patents (SEPs). The presented study examines whether, how and to what extend the EU competition law can promote patent pooling as a recommended mechanism for licensing SEPs. To reach this purpose, a brief review of pooling history shows how antitrust policy evolved with regard to pool establishment and operation. Patent pools in the modern era are connected to standardised technologies, and display tendency to product-based technologies rather than standard-based pooling. As a research methodology, a comparative analysis between the US and the EU antitrust laws shows that, although the procedural frameworks in the US contain only soft law, pooling there has undergone a more stable and straightforward treatment thanks to the publicly available Business Review Letters (BRLs) than in the EU which lacks a thorough assessment template. The presented substantive analysis illustrates how the two systems assess pooling's potential anti-competitive effects. Despite several similarities in their evaluation, the US generally shows a slightly more lenient approach toward patent pools. Amongst the differences, the strict EU approach regarding inclusion of non-essential/substitute patents into a pool is criticised. Each paper section is concluded by a takeaway that summarises and discusses the outcomes.

Keywords: patent pools; standard essential patents; competition law; antitrust; licensing

Recommended citation: Maryam Pourrahim, Capacity of EU competition law to promote patent pools: A comparative study, 12 (2021) JIPITEC 297 para 1

A. Introduction

1 Patent pools are a recommended tool presented in policy circles to facilitate access to patented technologies in fields ranging from biotechnology, nanotechnology, clean energy technologies to telecommunication and technical standards. They are often regarded as a solution to certain market failures in patent licensing, particularly to the risk of royalty stacking and patent thickets. The economic literature consistently recommends the creation of patent pools to solve these problems.[1]

2 Patent pools are formed when two or more patent holders decide to collectively license their patents to either each other or to third parties. In close connection to standardized technologies, today patent pools are often created when a standardized product requires multiple patented technologies for production[2]. A recent attractive filed of patent pooling is linked to licensing of standard essential

* PhD Candidate. Faculty of law. Tilburg University (NL) & University of Fribourg (CH). email: m.pourrahim@uvt.nl.

1 Anatole Krattiger and Stanley P Kowalski, 'Facilitating Assembly of and Access to Intellectual Property : Focus on Patent Pools and a Review of Other Mechanisms', Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practice (2008). p. 138.

2 The US Department of Justice & Federal Trade Commission, Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition (2007). <www.usdoj.gov/atr/public/hearings/ip/222655.pdf>. (Hereinafter: Promoting Innovation and Competition).

patents (SEPs) created in the Internet of Things (IoT) and the Information and Communication Technology (ICT) which are to enable interoperability and communication between multiple devices[3].

3 Patent pools have advantages such as facilitating equal access to licenses for all potential licensees, speeding up access to technology, integrating complementary/essential technologies, reducing transaction costs, and avoiding costly infringement litigations[4]. According to the EU Commission, many challenges in SEP licensing can be treated through patent pools as they can offer better scrutiny on essentiality, more clarity on aggregate licensing fees and one-stop shop solutions. However, pooling may create antitrust issues[5].

4 In this research, patent pools are analysed under EU competition law and US antitrust law to see under which circumstances antitrust concerns may be raised including market foreclosure, price fixing and tying. The principal question that the paper tries to answer is how EU competition law can promote patent pools while avoiding anti-competitive practices. To reach this purpose, a comparative study between the EU and the US systems is carried out.

5 The paper starts with an overview on patent pools features, their pro-competitive effects and historical development that allow reader to review the purposes which led to their establishment and the changes that antitrust policies have undergone since the emergence of pools. Patent pooling will be then analysed under US antitrust law and EU competition law through procedural and substantive analyses, which identify the differences between the two systems and examine regulatory frameworks under which each system treats the antitrust concerns. Based on these analyses, approaches to improve EU competition law capacity to promote patent pools are proposed.

B. Overview of patent pools

6 Patent pools are defined as a licensing arrangement, whereby a group of parties assemble a package of patents to license to the pool contributors and/or to third parties. Patent pools are established in two structures: (a) a group of limited members exclusively cross-license their patents to use mutually, or (b) the group allows a common agent, who can be either one of the patent holders or a third-party administrator who acts as a separate entity to carry out licensing. In the latter structure, assessment is managed by the pool agent that results in a considerable time and expense economy for SEP holders. It should be noted that patent pools managed by one of the patent holders are less favourable because the agent will gain access to the confidential sales data of other licensors which may lead to the exchange of sensitive information and subsequent anti-competitive behaviours (see section C.II.1.d)).

I. Pro-competitive advantages

7 Patent pools can prevent patent disputes between the licensor and licensee while diminishing the possibility of a licensee ending up with costly litigation over unlicensed patents.

8 In addition, if standard setting activities of industries with patents of interoperable products are owned by multiple holders, pooling can be an effective solution to the tragedy of anticommons[6] and patent thickets. In the former case, a standard with many essential patents suffers from underuse or absence of diffusion because an implementer willing to incorporate the standard into a product needs to access to all essential patents and therefore obtain licenses from all patent holders[7]. In this context, patent pooling lets a standard implementer obtain a single license at a single royalty rate for all patents in the pool, that consequently reduces the transaction costs, controls the total cumulative license fee, and improves access to patents[8].

3 European Parliament, Standard Essential Patents and the Internet of Things, January 2019. <http://www.europarl.europa.eu/RegData/etudes/IDAN/2019/608854/IPOL_IDA(2019)608854_EN.pdf>.

4 R Bekkers, E Iversen and K Blind, 'Patent Pools and Non-Assertion Agreements: Coordination Mechanisms for Multi-Party IPR Holders In' [2006] EASST 2006 Conference <http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?db=pubmed&cmd=Retrieve&dopt=AbstractPlus&list_uids=12975767088164818072related:mMxECmsvE7QJ>. p. 13.

5 European Commission, Communication, Setting out the EU approach to Standard Essential Patents, COM(2017) 712 Final, Brussels, 29.11.2017.<https://ec.europa.eu/docsroom/documents/26583>.

6 The tragedy of the anticommons happens where "multiple owners are each endowed with the right to exclude others from a scarce resource, and no one has an effective privilege of use." Michael A Heller, 'The Tragedy of the Anticommons: Property in the Transition from Marx to Markets' (1998) 112 Harvard Law Review 622. p. 624.

7 Michael Mattioli, 'Power and Governance in Patent Pools' (2014) 27 Harvard Journal of Law & Technology 421. p. 439.

8 Bekkers, Iversen and Blind (n 4). p. 6.

9 Pooling can also be helpful in dealing with patent thickets which happens where multiple independent patent holders share a technology. This situation which is common in industries like telecommunication and IT with many overlapping rights, makes implementors go through time and effort consuming negotiations of licensing agreements before manufacturing a product[9]. In this context, pooling has similar positive effects as in the anticommons situation.

10 Lastly, pooling together complementary patents facilitates technology dissemination and enables widespread use of new technologies[10]. Without pooling, a patent owner could be able to block implementers in manufacturing a new product associated with the patented technology. In contrast, by licensing their pooled patents on a group basis, the owners can offer one-stop shopping to implementers that allows more rapid development of new technologies.

II. Patent pools development over time

11 In this section, the early patent pools created in the US by the sewing machine industry and the aircraft manufactures are studied to review various policies that the US adopted in facing patent pools. Since the 1990s, the modern pools have emerged to comply with new standards such as MPEG-2 and DVD, and this is when the EU began to publicly present its assessment on patent pools.

1. Early patent pools

12 In the complete absence of regulations in 1856, one of the first patent pools was established in the US by the sewing machine industry, where the firms chose to pool patents with their competitors based on mutual agreement to mitigate the risk of litigation[11]. In 1890, the Sherman Act sought to prevent monopolies but excluded pooling and licensing due to freedom of contract and the dominancy of patent law over antitrust law in 1900s[12]. Based on a Supreme Court ruling, a patent owner enjoyed absolute freedom to license patents under any conditions decided by a contract between the patentee and the licensee[13]. The court refused to consider the creation of monopolies and fixed prices which granted the patentees an unrestricted right to practice collusive dealings under the protection of patent law[14].

13 In 1912, the absolute freedom was ended by a Supreme Court ruling, when it stated that the rights of the patentees had been pushed "to evil consequences" and that the Sherman Act imposed appropriate limits on such abuses[15]. Over the following fifty years, the Supreme Court addressed several pools, having approved some while dissolving others based on the competitive effects of each pool[16].

14 Due to the increasing demand for airplanes in WWI, the National Advisory Committee for Aeronautics proposed to form a patent pool in 1917 encompassing almost all aircraft manufacturers in the US. To access all the patents, they each had to pay a royalty. The Attorney General concluded that the pro-competitive effects of these arrangements outweighed anti-competitive effects[17].

15 Collective patent licensing reached its peak in the 1930s (with 14 pools in the US) but then curved down until 1990. The relaxing of antitrust scrutiny before WWII and the subsequent tightening after the War are often presented as an explanation for this change[18]. In addition, the Department Of Justice's (DOJs) list of patent licensing practices for *per se* antitrust violations (referred to as the "Nine No-No's") was another issue that made companies

9 Carl Shapiro, 'Navigating the Patent Thicket: Cross Licenses, Patent Pools, and Standard-Setting' (2001) 1 Innovation Policy and the Economy 119. pp.122-123.

10 Promoting Innovation and Competition. pp. 65-66.

11 Robert P Merges, 'Institutions for Intellectual Property Transactions: The Case of Patent Pools' [1999] https://www.law.berkeley.edu/files/pools.pdf, p.18.

12 ED LEVY and others, 'Patent Pools and Genomic: Navigating a Course to Open Science?' (2010) 16 Boston University Journal of Science and Technology Law 76.

13 Case, 186 U.S. 70 (1902). p.70.

14 Steven C Carlson, 'Patent Pools and the Antitrust Dilemma' (1999) 1 16 Yale J. on Reg. 359 1. p. 373.

15 Case, 226 U.S. 20 (1912).

16 Carlson (n 15). p. 374.

17 Monica Armillotta, 'Comparative Analysis: US Legal Treatment of Patent Pools – Delineating the Modern Archetype', *Technology Pooling Licensing Agreements: Promoting Patent Access Through Collaborative IP Mechanisms* (Nomos Verlagsgesellschaft mbH 2010). pp. 74.-75.

18 Justus Baron and Tim Pohlmann, 'The Effect of Patent Pools on Patenting and Innovation - Evidence from Contemporary Technology Standards' [2015] Cerna - Center for Industrial Economics. p.8.

overcautious about concluding patent pooling agreements. However, the DOJ acknowledged in 1979 that many of those nine condemned practices had significant efficiency and pro-competitive virtues and thus it rescinded the list.[19]

2. Modern patent pools

16 Pool licensing practice started rising again in the 1990s when the DOJ and the Federal Trade Commission (FTC) jointly issued new guidelines[20] for a more "benevolent scrutiny of patent licensing and placed the analysis of patent pools under the rule-of-reason" (Baron & Pohlmann, 2015: 8-9). In 1997 and 1999, the DOJ cleared the MPEG2 and two DVD pools as the first modern patent pools in the ICT standards. In fact, this period is when the EU Commission also started to issue comfort letters for those pools and as a result, a new wave of pooling was triggered.

a) Standard-based pools

17 By tradition, a pool offers a licence to a standard or a family of standards in one technological field where implementers have to deal with various pools, since different generations of standards stay relevant to a specific application even after a new, more advanced standard is introduced. Each of these standards has its own SEPs and patent pools. For example, most programmes in the fields of video coding, audio coding, and audio compression are standard-based pools.

18 In 1998, MPEG LA was established to act as an independent technical expert to determine the essentiality of patents to the MPEG-2 standard, to assemble and offer a package of hardware and software licenses to the pool members, and to distribute royalty income among the contributing patent holders on a per patent basis. Both the DOJ[21] and the Commission[22] approved the MPEG pool. In 1999, 3C and 6C DVD pools were formed to provide essential patents for DVD standards where instead of an independent administrator, one of the licensors acted as the common agent on behalf of the other pool members.

19 In the 2000s, a few licensing firms including Avanci, Sisvel, and Via Licensing started specialising on the administration of patent pools. In parallel, the Standard Setting Organisations (SSOs) have gradually initiated to collaborate with the licensing administrators. In this context, an agreement concluded between Institute of Electrical and Electronics Engineer (IEEE) and Via Licensing in 2008 with the goal of fostering patent pools for IEEE standards and reducing barriers which prevented the rapid adoption of technology standards[23]. Other SSOs established explicit policies to boost the formation of patent pools for their standards[24].

b) Product-based pools

20 With the emergence of the IoT, interconnectivity and interoperability have become essential in numerous sectors. Wireless, WI-FI, Bluetooth and 4G are already implemented in billions of products ranging from remote surgery equipment to connected cars and therefore, a wide range of firms need to get licences from the providers of these technologies. To provide access to them, some SEP holders have incorporated their SEPs into licensing platforms and pools[25]. This evolution led to a new pooling form where pools (e.g. One-Blue) started to offer all the relevant standards related to a very product.

21 Product-based pools are ideal for implementers wanting to license many patents for a specific application or product in one go. Such pools offer a licence not just for the one technological filed, but for all relevant fields. For example, if a firm wants to produce a Blu-ray recorder, One-Blue pool solves most of a licensee's needs in the field of optical discs.

19 Ky P. Ewing, Jr., Deputy Assistant Attorney General, Antitrust Div., Dep't of Justice, Remarks to the San Francisco Patent Law Association (May 5, 1979), reprinted in 4 Trade Reg. Rep. (CCH) ¶ 13,128.

20 "Federal Antitrust Guidelines for the Licensing of Intellectual Property", <https://www.justice.gov/sites/default/files/atr/legacy/2006/04/27/0558.pdf>.

21 MPEG-2 Business Review Letter. <https://www.justice.gov/atr/response-trustees-columbia-university-fujitsu-limited-general-instrument-corp-lucent>.

22 European Commission, Press release, IP/98/1155, Brussels, 18th December 1998. <https://ec.europa.eu/commission/presscorner/detail/en/IP_98_1155>.

23 IEEE-SA and Via Licensing collaboration. <https://www.ieee.org/>.

24 For e.g., see DVB's IPR Policy. <http://dvb.org/wp-content/uploads/2020/02/dvb_ipr_policy_summary.pdf>.

25 Marco Lo Bue, 'Patent Pools in the ERA of the "Internet of Things": A Fine Line Between Collusion, Market Power and Efficiencies', *The Interplay Between Competition Law and Intellectual Property: An International Perspective* (2019). p. 300.

22 In this context, Avanci, the first platform for IoT manufacturers[26], has a product-based pooling approach with the aim of licensing out relevant generations of the cellular SEPs of its licensors in each product-related programme. Thus far, it appears attractive to the major SEP holders and to IoT newcomers like BMW[27]. It offers licences to different IoT products for fixed-per-unit royalties to facilitate adoption of the related technology. Users' applications of the standardised technologies vary due to the omnipresence of technologies defined by 2G, 3G and 4G standards. Avanci claims that the best solution is product-based licensing, while adapting the royalty rate in each case to the specific use made of the technologies covered by the SEPs.[28]

3. Takeaway

23 Patent pools have a long but uneven history. Some scholars divide their history into three periods: "beginning with deference, shifting to suspicion and *per se* prohibitions, and reaching a cautious endorsement"[29]. The ups and downs in their creation and operation as well as their growth and failure were significantly influenced by changes in antitrust enforcement practice and authority evaluations. The more lenient the antitrust policy is, the more patent pools emerge and develop.

24 As shown, there is no single purpose for creating a patent pool and no single way to manage it. Early pools were associated with monopolies and cartels, then later ones were created in response to US government policy objectives addressing standardization, biomedical, and agricultural technologies since the 1990s[30]. They were established for a number of reasons ranging from clearing blocking patent positions and avoiding potential litigation, to practicing anti-competitive behaviours such as market division among horizontal competitors or naked price fixing[31].

25 The modern patent pools were created mostly in connection to standardised technologies and under a more stable institutional environment which is a response to technological and commercial considerations. This evolution continues and today, product-based pools are particularly attracting players in the IoT era as they provide a package from all relevant patents for a product at once. The potential negative impact of the EU competition policy on this type of pools is discussed in D.II.3.

C. Comparative analysis of the EU and the US antitrust laws

26 This section is dedicated to a comparative analysis between the EU and the US systems that examines their competition policies in assessing patent pools to explore the similarities and differences between the two systems.

27 It should be noted that although the EU has a poor history in patent pools compared to the and despite the fact that before 2004 the EU Commission was not demonstrating its standpoint as publicly as the US antitrust agencies were, the rapid growth in standardisation and IPR arrangements motivated the Commission to take an in-depth look at the patent pools and their interaction with the standardisation agreements.

28 The methodology adopted here is a comparative analysis between the two, focusing on procedural and substantive issues.

I. Procedural analysis

29 As agreements between undertakings, patent pools may restrict competition and potentially fall in the scope of the general competition law prohibition of Article 101 (1) Treaty on the Functioning of the European Union (TFEU). In the US, the antitrust law intervenes if a pool with monopoly power in market causes anticompetitive effects violating Section 1 or Section 2 of the Sherman Act.

26 Avanci licenses most 2G, 3G and 4G patents in a single agreement. These patents cover wireless technology. <https://www.avanci.com/>.

27 R. Lloyd, Deal with BMW is the first of many with auto-makers, says Avanci boss. <https://www.iam-media.com/litigation/deal-bmw-first-many-auto-makers-says-avanci-boss>.

28 H. Rijnen, An insider's guide to patent pools. <https://www.iam-media.com/frandseps/insiders-guide-patent-pools>. pp. 7-8.

29 Mark Miller and David Almeling, 'DoJ, FTC Redefine Antitrust Rules on Patent Pools' [2009] National Law Journal.

30 David Serafino, 'Survey of Patent Pools Demonstrates Variety of Purposes and Management Structures' [2007] Knowledge Ecology International. p. 2.

31 Bekkers, Iversen and Blind (n 4). p. 10.

1. US antitrust law framework

30 Since 1968, the Antitrust Division of the DOJ has the regulatory task of reviewing different types of business practises proposed by private parties to determine how the Division may respond to proposed business conduct. The issuance of multiple patent pools-related BRLs[32] in the late 1990s shows their effectiveness[33]. Firms planning to establish a patent pool inform the DOJ who accordingly comments on the pool's potential effects and announces whether the proposed plan is safe from an antitrust law perspective.

31 A firm requesting a business review may receive one of the following responses: (a) the DOJ does not presently intend to bring an enforcement action against the proposed conduct; (b) the DOJ declines to state its enforcement intentions and it may or may not file suit if the proposed conduct happens; and (c) the DOJ will sue if the proposed conduct happens. The first response i.e., the "safe" pooling proposal, emphasises that its enforcement intention is changeable, and the Department reserves the right to bring an enforcement action in the future if the actual operation of the proposed conduct proves to be anticompetitive in purpose or effect[34].

32 The BRLs have long provided a guidepost for private conduct offering safe harbours for business activity which the DOJ, as announced, would not condemn. Over time, they served as a "template for patent pooling arrangements that should not run afoul of the antitrust laws."[35]. Firms desiring a favourable business review can attempt to eliminate or reduce the risk of anti-competitive effects through the application of certain safeguards or mechanisms incorporated in the BRLs.

33 However, some criticise the BRLs arguing that: (a) the validity of enforcement intention is limited to the date of the letter because the DOJ reserves right for future assessment, and (b) publishing all the information submitted by party may endanger its business[36]. Regarding the first criticism, one may counterargue that judiciary systems including courts and competition/antitrust authorities cannot and should not guarantee a future act as they do not make general rules like legislatures. In a limited and narrow manner, they evaluate what one has done or on occasions like business review/comfort letters, they evaluate the firms' declared plans. They do not provide absolute legal certainty; however, they make a beneficial assessment template for the involved firms and public.

34 Publishing business information is debatable. What is mostly agreed upon between agencies and the parties when publishing a BRL is striking a balance between business secrets (private interest) and the right to information (public interests). One may advocate for the latter in the digital era because information availability (in the context of the antitrust authorities' assessment) provides more certainty and a better self-assessment possibility for new players, particularly small firms who learn through other firms' BRLs. However, the aim of these non-binding documents issued by the competition/antitrust assessment bodies is mainly to identify the key factors over which they are likely to ground their judgments of pro- vs. anti-competitiveness, and then to analyse the substance and boundaries of these components[37]. For these reasons, a letter serves its purpose by disclosing the method of analysis without needing to include confidential information.

35 Apart from the BRLs, the DOJ and FTC (the Agencies) issued IP Guidelines in 1995[38] (updated in 2017[39]) through which they clarified their antitrust enforcement position. The Guidelines deal with patent pools and emphasise that every case is evaluated in the light of its own facts to assist firms in assessing the antitrust risk related to their practice. It aims to inquire whether the restraint is likely to have anticompetitive effects and if so, whether the restraint is necessary to achieve pro-competitive

32 See Business Review Letters of 1997, 1998 and 1999 for the MPEG-2 pool, the 3DVD pool and 6DVD pool respectively and more recently IEEE in 2007, RFID in 2008, IPXI in 2013 and FVLI in 2014. < https://www.justice.gov/atr/business-review-letters-and-request-letters#page-17>.

33 Jorge L Contreras, 'Taking It to the Limit: Shifting U.S. Antitrust Policy Toward Standards Development' [2018] <https://dc.law.utah.edu/scholarship/116/>.

34 Introduction to Antitrust Division Business Reviews. <https://www.justice.gov/sites/default/files/atr/legacy/2011/11/03/276833.pdf>.

35 Robert J Gilbert, 'Antitrust for Patent Pools: A Century of Policy Evolution' (2004) 3 Stanford Technology Law Review 1. p.3.

36 C. Ehlermann, I. Atanasiu (ed.), European Competition Law Annual 2000: The Modernisation of EC Antitrust Policy, pp. 138-139.

37 LEVY and others (n 13).

38 Antitrust Guidelines for the Licensing of Intellectual Property, 1995. <https://www.justice.gov/atr/archived-1995-antitrust-guidelines-licensing-intellectual-property>.

39 Antitrust Guidelines for the Licensing of Intellectual Property, 2017. <https://www.justice.gov/atr/IPguidelines/download>. (Hereinafter: IP Guidelines)

benefits that outweigh anticompetitive effects[40]. The firms should, however, seek a BRL if they wish to know about the specific enforcement intentions regarding their particular business practice.

36 As non-binding law, the guidelines reflect the Agencies' enforcement approach. That is why the IP Guidelines do not propose rigid rules and prohibitions, but instead they apply an effect-based analysis to the licensing mechanisms. They set out three core principles[41]:

1. The Agencies regard IP as any other form of property in applying the general antitrust analysis. Activities involving IP rights and their exercise are neither free from scrutiny nor suspected of antitrust.

2. There is no presumption that an IP right confers market power. Even if a fact-based analysis proves otherwise, that power is not *per se* illegal[42].

3. The Agencies acknowledge that IP licensing permits firms to combine pro-competitive complementary factors of production.

37 In addition, the Agencies guidance published in 2007 deals *inter aila* with patent pools and presents further details regarding their efficiency and competitive concerns[43]. Nevertheless, none of these documents create laws or binding regulations. However, they can be regarded as definitive as they actually express the views of the administrative bodies responsible for assessing antitrust issues[44].

2. EU competition law framework

38 Until 2004, the EU Commission procedurally allowed parties to notify agreements to secure a decision on their legality. However, this system proved burdensome and the Commission frequently issued comfort letters, which were non-binding statements indicating that the Commission found no reason to interfere while providing some legal certainty. Since 2004, the system of notification has been removed and parties are expected to self-assess[45]. To facilitate transactions and, given the uncertainty in the application of Article 101(3), the Commission established Block Exemption Regulations (BER). These provide legal certainty for undertakings entering into certain types of agreements because they render Article 101(1) TFEU automatically inapplicable as BER presume those agreements satisfy all the conditions laid down in Article 101(3) TFEU. All other agreements require an individual assessment under Article 101 TFEU. Each BER is accompanied by some guidelines that summarise and interpret the related case law to provide practical examples of how to assess the compatibility of certain conduct with competition law rules.

39 The Technology Transfer Block Exemption Regulation (TTBER) was adopted in 2004 (updated in 2014[46]) as a regulation on technology transfer agreements[47]. The TTBER applies only to bilateral contracts between a licensor and a licensee where the latter manufactures licensed goods, provides licensed services, or has them manufactured or provided for his account.

40 There are two main agreements in the context of pools. First, are the agreements for establishing patent pools which have been always excluded from the scope of the TTBER[48] for two reasons: (a) according to the council regulation, the commission is not empowered to block exempt technology transfer agreements concluded between more than two parties[49], and(b) licensing programmes involving multiple parties do not permit the production of contract products, a necessary condition for the application of the TTBER. The second agreement is licensing out which is concluded between a pool and a third party. In 2004, the only agreements excluded in the TTBER were those to establish a pool, but the

40 IP Guidelines. pp. 16-17.

41 IP Guidelines. p. 2.

42 OECD, Licensing of IP rights and competition law – Note by the United States, DAF/COMP/WD(2019)58, 6 June 2019.<https://one.oecd.org/document/DAF/COMP/WD(2019)58/en/pdf>.

43 Promoting Innovation and Competition.

44 LEVY and others (n 13).

45 Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty, OJ L 1, 4.1.2003, p. 1-25.

46 Commission Regulation (EU) No 316/2014 of 21 March 2014 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to categories of technology transfer agreements, OJ L 93, 28.3.2014, p. 17–23.

47 Commission Regulation No 772/2004 of 27 April 2004 on the application of Article 81(3) of the Treaty to categories of technology transfer agreements, OJ L 123, 27.04.2004. This Regulation was regarded as simpler and more flexible than Regulation No 240/96; it broadly adopted the same approach than the Vertical Block Exemption Regulation

48 *Ibid.* recital 7.

49 Council Regulation 19/65, OJ Special Edition Series I 1965-1966. p. 35.

licensing out agreements were covered and benefit from the exemption. In 2014, the Commission narrowed the scope of TTBER (the licensing out agreements were also excluded) and now neither agreements for setting up pools nor licensing out agreements are covered.

41 The Commission's reasoning was that licensing out from a pool is a multiparty agreement (since contributors of a pool determine the licensing terms and conditions together) which is in contrast with the TTBER as it should principally cover only bilateral agreements[50]. This reasoning seems unconvincing because the TTBER was supposed to cover bilateral agreements even in 2004[51]. One may question why those agreements, which were considered bilateral based on the TTBER 2004, are considered multilateral after the regulatory change in 2014. It is not clear whether in 2014 the Commission saw the TTBER 2004 as a mistake so the 2014 policy change was actually a correction, or it just decided to change the definition for licensing out agreements. Lundqvist found this policy change correct, suggesting that the 2004 TTBER scope was odd and the 2014 change is a return to the right direction for the Commission[52].

42 In any case, the 2014 policy change seems anti-pooling because licensing out agreements could benefit from the exemption as they were under the scope of the TTBER. This issue makes us believe that the inclusion of licensing out agreements in the TTBER and the consequent high legal certainty could have effectively attracted firms to the pools, as the agreements' parties were sure that their agreements could benefit from the exemption (subject to the TTBER conditions[53]). In this line, the issuance of many comfort letters in the 2000s clearing patent pools can be regarded as an outcome of the legal certainty created by that policy. Alas, as the comfort letters are not in access, the extent of this effect cannot be examined.

43 The Technology Transfer Guidelines (TT Guidelines)[54], however, deal with patent pools and provide a comprehensive safe harbour for both the pools' creation and the licensing out agreements. The TT Guidelines safe harbour is a promising progress in the EU, although the Commission guidelines are soft law as they are not rule of law but rule of practice[5556]. Through guidelines, the Commission limits its power and is to follow the rules laid down therein because of the creation of legitimate expectation amongst the firms[57]. In fact, the guidelines bind the Commission in its decision but not the pooling parties, and therefore if the parties disagree, the Guidelines act no more than a good practice guidance.

3. Takeaway

44 The comparison of the two systems' procedural frameworks shows that the antitrust authorities assess patent pools through some guidelines which although soft law are helpful since their providers are the assessors of patent pools.

45 The US has a higher number of guidelines and guidances with very elaborated analyses referring to the US case law. The EU has only the TT Guidelines and since there has been limited case-law they offer less certainty than their US counterparts. However, the US regulatory framework on patent pools is

50 European Commission, Memo, Brussels, 21 March 2014, Antitrust: Commission adopts revised competition regime for technology transfer agreements – frequently asked questions. <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_208>.

51 TT Guidelines, 2004, para. 38: "According to Article 2(1) of the TTBER, the Regulation covers technology transfer agreements between two undertakings. Technology transfer agreements between more than two undertakings are not covered by the TTBER. The decisive factor in terms of distinguishing between agreements between two undertakings and multiparty agreements is whether the agreement in question is concluded between more than two undertakings."

52 Björn Lundqvist, *Standardization under EU Competition Rules and US Antitrust Laws: The Rise and Limits of Self-Regulation* (Edward Elgar Publishing Limited 2014).

53 According to the TTBER, to benefit from the exemption, the combined market share of competing firms must not exceed 20% and each market share for not competing firms must not exceed 30% on the affected relevant technology and product market. In case of competing firms. Additionally, their agreements must not contain any hardcore restrictions stated at Art. 4.

54 EU Commission, Communication, Guidelines on the application of Article 101 of the Treaty on the Functioning of the European Union to technology transfer agreements, OJ C 89, 28.3.2014, p. 3–50. At: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014XC0328%2801%29 (hereinafter: TT Guidelines).

55 Jonas Tallberg, 'Paths to Compliance: Enforcement, Management, and the European Union' (2002) 56 International Organization 609. p. 615.

56 Oana Andreea Ştefan, 'European Competition Soft Law in European Courts: A Matter of Hard Principles?' (2008) 14 European Law Journal 753. p. 12.

57 Regarding the Commission Notice: Case T-31/99, para. 257-258 and regarding the Commission Guidelines: Case T-23/99 para. 245.

soft law. The EU once provided pools with legal certainty for a decade (2004 - 2014) where licensing out agreements benefit from the binding rules of the TTBER. Although this legal certainty did not last after 2014, it may have significantly impacted the Commission assessments and the issuance of comfort letters for the patent pools at the time.

46 In the US, patent pools have been treated more stably thanks to the BRLs, while the EU due to its procedural modifications (from individual exemption to self-assessment) could not provide equal stability. The public availability of the US BRLs compared to the inaccessibility of the EU comfort letter is another advantage of the US procedural framework. This issue is further discussed in section D.I.

II. Substantive analysis

47 The main potential anti-competitive risks of pooling include price fixing, market foreclosure, collusion through pooling mechanism to exchange competitively sensitive information, reduction of innovation in the form of standard setting, and foreclosure of alternative technologies and barriers to the entry of new and improved technologies. The presented analysis aims at exploring to what extent the US and the EU share mutual approaches with each subject.

1. Antitrust concerns

a) Pooled patents

48 Antitrust risks depend largely on the relationship between the pooled patents and those outside the pool. The pooled patents can be classified as follows:

1. *Complementary* patents which are patents related to the same technology that must be used together to produce a specific output. Bundling these patents in a pool makes them more valuable than being on their own.

2. *Substitute* patents which cover alternative technologies and therefore may potentially compete with each other as they can be used in parallel without infringing each other.

49 In the context of standardization, the pooled patents are divided into *essential* and *non-essential.* Patents with substitutes to the covered technology are non-essential while those required to comply with a technical standard are essential. Essential patents are by nature complementary. However, what is essential may vary and each patent pool may define essential patents differently[58].

50 Both the systems agree that pools consisting of complementary or essential patents can lower prices to consumers as they: do not eliminate competitors, can increase efficiency, and are a pro-competitive method for disseminating technology[59]. In addition, they follow similar approaches toward the inclusion of non-essential patents into the pools as they assess the potential antitrust risks of inclusion under the rule-of-reason in the US and under Article 101(3) TFEU in the EU. Nevertheless, the systems diverge in assessing the inclusion of substitute patents, where the EU treats it more strictly than the US. As this difference can have great impacts on pooling antitrust assessment and tying concern, it is studied in detail in section D.II.

b) Validity of patents

51 Firms who fear that their patents can get invalidated by litigation may establish a pool to shield the invalid patents. This may be carried out through non-challenge provisions indicated explicitly or implicitly in the pool agreement. In the sewing machine case, the patentees agreed not to bring any infringement action, opposition, nullity or invalidation proceeding[60] against each other.

52 An invalid patent is considered not to be in a complementary relationship with other patents in the pool. Therefore, pooling such patents serves as a price-fixing mechanism. In addition, it will eliminate competition between substitute technologies outside the pool if it makes licensees accept the invalid patents and pay higher royalties[61].

53 In the pooling context, both systems consider patent validity critical due to its importance for the public[62], and a licensing scheme premised on invalid patents will not withstand antitrust scrutiny.

54 In the EU, freedom of parties to challenge the

58 MPEG-2 Business Review Letter at 5 and DVD6CBusiness Review Letter at 3 - 5.

59 Promoting Innovation and Competition. p. 76 and TT Guidelines. para. 253.

60 United States v. Singer Mfg. Co., 374 U.S. 174 (1963), p. 374.

61 Richard J Gilbert, 'Ties That Bind: Policies to Promote (Good) Patent Pools' (2010) 77 Antitrust Law Journal 1. pp.14-15.

62 Pope Mfg. Co. v. Gormully, 144 U.S. 224 (1892), p. 144 U. S. 234.

validity is one of the conditions to benefit from the safe harbour provided under the TT Guidelines[63]. In addition, a non-challenge clause in technology transfer agreement between the pool and third parties is likely to fall within Article 101(1) TFEU[64]. While the Commission once ruled that the non-challenge clause is legal (as it is merely ancillary to the technology agreement which included no other clause restricting competition), the ECJ rejected this view stating that such a clause could restrict competition within the meaning of Article 101 (1) TFEU [65].

55 In the US, the FTC dissolved the Summit/VISX pool on the ground of sheltering invalid patents and ordered the firms to cross-license their patents[66]. In RFID BRL, the DOJ stipulates that patents adjudicated as invalid or unenforceable must be removed from the pool and the licensors must promptly report any such finding. In practice, licensors have an incentive to do so when the royalties are allocated based on the number of patents in the pool[67].

56 One should note that the validity assessment is only carried out by courts if there is a challenge and given that a court ruling can be appealed, it can take years to reach the final decision on a patent validity. Furthermore, although uncertainty about patent validity is a major issue which can create distortion between large portfolio owners and smaller players, reaching certainty that a pool is only constituted by valid patents is rare. As a matter of fact, Giuri showed that only about 5% of a patent portfolio reach the stage of being reviewed by experts with technical, legal, and commercial insights[68].

63 TT Guidelines. para. 261.

64 TT Guidelines. para. 272.

65 C-65/86 - Bayer v Süllhöfer, 1988.

66 In re Summit Tech., Inc. and VISX, Inc., No. 9286 (FTC filed Mar. 24, 1998). < https://www.ftc.gov/enforcement/cases-proceedings/summit-technology-inc-visx-inc-matter>.

67 RFID Business Review Letter, p. 8. <https://www.justice.gov/sites/default/files/atr/legacy/2008/10/21/238429.pdf>.

68 Paola Giuri and others, 'Report of the Expert Group on Patent Aggregation' (2015), p. 24.

c) Individual restraints in licensing agreements

57 Licensing agreements raise the following four competition issues.

(aa) Exclusivity and non-exclusivity

58 Both the systems agree that if licensors and licensees are free to grant and obtain a licence outside the pool, this will limit the risk of foreclosure of third-party technologies and ensure that the pool does not limit innovation nor precludes the creation of competing technological solutions[69]. This can also mitigate the effects of potential market power and allows outsiders to invent around the pooled patents to compete with them. By contrast, exclusive licensing can damage innovation as licensors and licensees lack freedom to combine technologies in order to improve and compete with the pooled technologies, and they will not be able to provide products at a lower price.

59 Under the EU TT Guidelines, a non-exclusive license is one of the conditions of the safe harbour[70] and if a pool has a dominant position in the market, licences should be non-exclusive, royalties non-excessive and other licensing terms non-discriminatory[71].

60 In the US, although pool licensors are free to choose between excusive and non-exclusive licensing, BRLs suggest that they often propose granting a non-exclusive license while reserving the right to license their patents outside the pool[72]. However, the Agencies assess under the rule-of-reason whether such a non-exclusive license is a concerted conduct to prevent the outsiders from offering a competitive product, particularly in a case where the pool members collectively possess market power in the relevant market[73].

(bb) Partial pool licensing

61 Partial pool licensing takes place when a pool licenses its patents not only in one package, but also partially.

69 TT Guidelines. para. 270.

70 TT Guidelines. para. 261.

71 TT Guidelines. para. 269.

72 MPEG-2 Business Review Letter at 4; DVD3CBusiness Review Letter at 5-6; DVD6CBusiness Review Letter at 3, 6.

73 Promoting Innovation and Competition. pp. 79-80.

Proponents of partial licensing argue that this option is needed because, even if a pool were originally planned to include only essential patents, over time some of patents would no longer be essential to all the pool's licensees. In addition, licensees may legitimately desire partial licenses if they already have access to some of the pooled patents[74]. Pools offering partial licensing with a proportionate royalty would provide a party with needed patents instead of the whole package including unneeded patents[75].

62 Opponents argue that partial license turns the pool into bilateral agreements, puts a burdensome task on the pool, and engages with inconveniences such as high transaction costs and time for multiple negotiations, holders' unwillingness for negotiations, and the probability that the individually negotiated royalties collectively increase above the set package license royalty. One may wonder what happens to the one-stop-shop mechanism as the chief efficiency of pooling, if pools offer a pick-and-choose mechanism requiring multiple transactions and different royalties.

63 The two systems have adopted different approaches toward partial pool licensing. The Agencies principally show reluctance toward it and do not consider its refusal problematic. Mentioning the drawbacks of this option, the Agencies state that although partial licensing can "cull non-essential patents" from the pool, a more efficient way would be to continuously review the pool to ensure all included patents are essential[76].

64 The Commission does not explicitly mention partial-pool licensing in the TT Guidelines; however, in the assessment of the pools of non-essential but complementary technologies, it examines whether the pooled technologies are available only as a single package or the licensees have the possibility to partially obtain a licence for a proportional reduction of royalties[77]. It highlights that the latter option may reduce the risk of foreclosure of third-party technologies outside the pool.

65 Lugard & Hancher advocated this encouraging approach of the EU arguing that some pooled patents may be necessary for marketing compliant products within certain Member States while not necessary for licenses which plan to market those products in Member States where the patents in question are not registered[78].

66 One should note that partial pool licensing weakens the efficiency of pooling mechanism, and it is better not to be encouraged irrespective of circumstances. Anyhow, the following issues should be taken into account:

- Exchange of sensitive information: for example, information on royalty payments can reveal the licensee's unit volumes, revenue, and pricing when licensee and licensor are rivals in a downstream market.
- Partial pooling unreasonably presumes that the licensees are fully aware of the essentiality or non-essentiality each patent. This presumption may not be always the case particularly in the IoT space which involves many unfamiliar licensees.
- Unavailability of partial pool licensing does not necessarily have anticompetitive impacts if the pool lacks market power.
- Partial licensing is a response to the fear of inclusion of substitute patents in pool. The continuous review of patents is an alternative solution as adopted by the US.

(cc) Grantbacks

67 A grantback is an arrangement under which a licensee agrees to extend to the licensor the right to use the licensee's improvements to the licensed technology[79].

68 Broad grantbacks which include inventions related to the subject of the licensed patent or even completely unrelated inventions, particularly those that deny the innovator's right to license others, can deter innovation by reducing the returns available to follow-on innovators. Broad grantbacks may cause anticompetitive effects by limiting competition and disincentivising the licensees to engage in R&D[80].

69 Under a non-exclusive grantback, the licensee should not license back exclusively to the licensor. Both systems acknowledge that a non-exclusive grantback allows the pool to feed on and to profit

74 Promoting Innovation and Competition. pp. 83,84.

75 Paul Lugard and Leigh Hancher, *On the Merits: Current Issues in Competition Law and Policy* (illustrate, Intersentia nv 2005).

76 Promoting Innovation and Competition. p. 84.

77 TT Guidelines, para. 264 (d).

78 Lugard and Hancher (n 78).

79 IP Guidelines. § 5.6.

80 *Ibid*.

from improvements to the pooled technology[81]. It can also promote competition by allowing licensors to use the licensee's improvements to the licensed technology. This limits the ability of licensees to refuse license improvements and thus allows production of patent-conforming products which promote innovation by rewarding first innovators for enabling follow-on innovation by others and encourages subsequent licensing of innovation results[82].

70 They agree that to mitigate the grantback concern: (a) the grantback clause should be limited to improvements on the fundamental/essential patent; (b) a royalty fee formula should be set so that newly developed patents receive higher royalties than older ones that make it beneficial for licensors to introduce new essential patents into the pool; and (c) licensees should have option to choose between licensing their own patents through the pool pursuant to the same royalty-allocation rules or licensing them separately on FRAND terms[83].

(dd) Royalties

71 How to set royalty for a patent pool is another consideration of antitrust authorities. Some commentators believe that all types of government price control which set licensing royalties can erode the benefits of pricing based on market conditions leading to resource misallocation. They even argue that pools would disappear without the freedom to set royalties.[84]. On the other hand, some claim that royalty reasonableness should be checked over time through caps or considering a reasonable percentage of downstream price[85]. By the same token, the two systems have different theories.

72 Although the Agencies generally do not assess pool royalty reasonableness, they consider royalties and their formula as relevant factors when investigating alleged price coordination. If royalties are a small portion of the downstream price, it is unlikely that they are used to coordinate downstream prices[86]. But even royalties that are a great proportion of the downstream price do not necessarily raise competitive concerns[87].

73 In the EU, the firms building a technological pool compatible with Article 101 TFEU are free to negotiate and fix royalties for a pool package, subject to any commitment given to license on FRAND terms. It may be more efficient in certain circumstances if the pool royalties are agreed before choosing the standard to avoid increasing royalty rates by conferring a significant degree of market power on one or more essential technologies. Nonetheless, licensees must remain free to determine the price of products produced under the licence[88].

74 While excessive or monopolistic pricing is not a standalone theory of harm under US antitrust law but considered an indication of the free market rewarding innovations by high prices[89], excessive price is principally considered abusive violating Article 102 TFEU, even in the absence of other anticompetitive practices.

75 This theoretical divergence between the two systems is not influential in pooling practice as both have reached a common approach, that is, licensing on FRAND terms which is one of the safe harbour conditions set by the Commission in TT Guidelines and by the DOJ in the BRLs.

d) Risk of Collusion, exchange of sensitive information

76 Patent pools can harm the market by bringing horizontal competitors together and permitting them to jointly set royalty fees for their own patents. This risk becomes higher when the firms possess competing patents and may lead to monopoly prices on an otherwise competitive market. Pools may facilitate collusion by their mechanism to exchange competitively sensitive information which could facilitate downstream price coordination, discourage competition in technologies and reduce R&D innovation[90]. Notably, once interested

81 TT Guidelines. para. 271.

82 *Ibid.*

83 MPEG-2 Business Review Letter at 12, 13; DVD3CBusiness Review Letter at 8, 14; DVD6CBusiness Review Letter at 8-9, 14-16. Promoting Innovation and Competition, at 81, And European Commission, Press release, IP/03/1152, Brussels, 7th August 2003. <https://ec.europa.eu/commission/press-corner/detail/en/IP_03_1152>.

84 Promoting Innovation and Competition. p. 83.

85 Promoting Innovation and Competition. p. 82.

86 MPEG-2 Business Review Letter at 11; DVD3CBusiness Review Letter at 13 and DVD6CBusiness Review Letter at 14.

87 Promoting Innovation and Competition. p. 83.

88 TT Guidelines. para. 268.

89 US Supreme Court, *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398 (2004), 13 01 2004

90 Promoting Innovation and Competition. pp. 81-82

parties participate simultaneously to form pools of competing standards, it may lead to exchange of sensitive information between competing pools[91].

77 Both systems recognise this risk and require certain safeguards to ensure that sensitive information is not exchanged, or the exchange is limited to what is necessary for the establishment and operation of the pool[92]. The concern is mitigated when the information disseminated is historical, aggregated and published in a format that precludes identifying individual entities and is limited to the quantity, type, place of manufacture and sale of products sold before providing it to the pool. As such, the pool's members are prevented from directly accessing individual licensees' sensitive business information[93]. Adding an independent expert or licensing body is proposed to ensure that output and sales data necessary for the purposes of calculating and verifying royalties, is not disclosed to competing undertakings in affected markets[94]. The transparency of the pool creation process and the extent to which independent experts are involved in its creation and operation are also considered[95].

78 It worth mentioning that in the EU, the exchange of information is becoming more relaxed in the digital field. In the last revision of Horizontal Guidelines (HG), the Commission reformed the information exchange in the digital field emphasizing that the HG should provide clear guidance on information exchange within cooperation models. It also highlights that the revised HG should explicitly foresee that the Commission will assess the *actual* effects of the information exchange on competition[96].

91 TT Guidelines. paras. 259-261.

92 TT Guidelines. para. 261.

93 IPXI Business Review Letter.

94 TT Guidelines. para. 260.

95 TT Guidelines. para. 248.

96 Evaluation of Commission Regulation (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements and of Commission Regulation (EU) No 1218/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of specialisation agreements, 07/04/2020. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=PI_COM:Ares(2020)1972062>.

2. Antitrust safe harbour

79 While the EU Commission provides a comprehensive safe harbour for technology pools, the US Agencies provides neither *per se* prohibitions nor safe harbours explicitly, as they do not measure a pool against a checklist of safeguards but evaluate the particular facts and circumstances to determine whether the actual conduct is anticompetitive[97]. However, the Agencies identify the following safeguards that patent pools can apply to reduce the risk of competitive harm[98]:

- The patents in the pool must be valid and not expired.
- No aggregation of competitive technologies and setting a single price for them.
- An independent expert should be used to determine the essentiality of patents in the pool.
- Royalties should be reasonable.
- Non-exclusive licenses should be available.
- Pool agreement must not disadvantage competitors in downstream product markets.
- Pool participants must not collude on prices outside the scope of the pool including on downstream products.

80 Notably, the absence of these safeguards does not imply that the pool necessarily harms competition in violation of the antitrust laws. The IP Guidelines, however, state that patent pooling is anti-competitive if any of the following conditions are met:

- The excluded firms cannot effectively compete in the relevant market for the product incorporating the licensed technologies.
- The pool participants collectively possess market power in the market.
- The limitations on participation are not reasonably related to the efficient development and exploitation of the pooled technologies.

81 While in the EU, the safe harbour of the TT Guidelines covers both pool creation and licensing out agreements. Regardless of the market position of the pool's parties, if the following conditions are

97 DVD3C Business Review Letter, at 11 n.53; DVD6CBusiness Review Letter, at 12 n.64; IP2 Report, at 72–73.

98 Promoting Innovation and Competition. pp. 74-82.

met[99], Article 101 (1) will be inapplicable otherwise the pools come within the application of Article 101 (3) TFEU:

- Open participation of all interested IPR owners in the pool creation.
- Insertion of only essential/complementary technologies.
- Inclusion of sufficient safeguards against exchanges of sensitive information.
- Non-exclusive licensing.
- Licensing out to all potential licensees on FRAND terms.
- Freedom of parties to challenge the validity and essentiality of the pooled technologies.
- Freedom of parties to develop competing product and technology.

3. Takeaway

82 The presented substantive analysis of antitrust law described how the two systems apply their competition policies (i.e., the Sherman Act, and Articles 101 and 102 TFEU) to the patent pools assessment through their soft-law regulatory frameworks. This comparative analysis can be summarised as follows:

1. Both systems agree that,
   a) Inclusion of complementary and essential patents into a pool is pro-competitive.
   b) Pooled patents must be valid. However, both seem to ignore that (a) the validity assessment is only carried out by courts if there is a challenge, and (b) reaching certainty that a pool is only constituted by valid patents is rare. That pooling being only made of valid patents is crucial in safeguarding public interest and in setting royalty rates.
   c) The Grantback clause should be non-exclusive and limited to the improvements of patents essential to implementing the standard.
   d) Exchange of competitively sensitive information is considered anti-competitive and engaging an independent expert is proposed to mitigate the risk of collusion between rivals.
2. Both systems diverge from each other in the following issues:
   a) Assessment of inclusion for substitute/non-essential patents into a pool. Although the US assesses it cautiously, it recognises that it may be pro-competitive and justified under the rule-of-reason. In contrast, the EU considers this inclusion a violation of Article 101(1) TFEU so that the exemption under Article 101(3) TFEU is unlikely fulfilled. This difference in evaluation seems significant and the EU's strict policy seems unnecessary. We discuss this further in section D.II.
   b) In the US, partial pool licensing is unwelcome as it turns one pooled package into individual sub-packages. However, its refusal is not regarded as problematic *per se*. In contrast, the EU encourages partial licensing when a pool is composed of non-essential but complementary patents.
   c) In the US, licensors are free to choose between exclusive and non-exclusive licensing. An exclusive licensing can be considered even pro-competitive under the rule-of-reason analysis. A non-exclusive licence is seen in the EU as a condition to benefit from the safe harbour. Although seeming stricter, the EU does not totally rule out exclusive licensing but assesses it on a case-by-case basis.
   d) There is an old divergence between the two systems in terms of royalty rate. While excessive pricing is not a standalone theory of harm under the US antitrust law, it violates the TFEU if carried out by a dominant pool. Nevertheless, the FRAND condition makes this difference less significant, as in modern patent pools which are in close connection with standardised technologies, SEP holders are typically committed to licencing their patent on FRAND terms whether through patent pools or individual licensing.

D. Main points for improvement

83 The analyses presented in the paper show that EU competition law and US antitrust law share common approaches and policies where both have a policy to facilitate the formation of pools. However, the US system seems more pro-patent pool in two ways, that if adopted by the EU could promote its capacity in regulating patent pools.

99 TT Guidelines. para 261.

I. Assessment template for patent pools

84 Since 2003, the Commission has issued no administrative (comfort) letter for patent pools. These letters serve the same purposes as the BRLs do in the US: firms could notify their cooperation agreement to the Commission to receive an individual exemption from the application of Article 101 TFEU.

85 The reason for this is that Regulation 1/2003[100] stated that the responsibility for the assessment of agreements shifted from the Commission, in the form of individual exemption, to firms which rely on soft law and precedents for self-assessing the legality and compatibility of their agreements with Article 101 TFEU[101]. The central feature of the Regulation is the direct application of Article 101(3) TFEU, meaning that agreements, decisions, or conducts fulfilling the conditions of this Article are valid and enforceable without a prior administrative decision by a competition authority. Accordingly, there is no longer formal exemption decisions nor new comfort letters[102].

86 To complete the Regulation 1/2003, the Commission through the "Modernisation Package" adopted six notices among which the Notice[103] on informal guidance related to novel questions concerning Articles 81 and 82 EC Treaty (current 101 and 102 TFEU) is to compensate the absence of a notification system. It provides a legal framework under which firms can request a guidance letter before the Commission. Through this request, firms demand interpretation for questions raised by their actual or potential agreement which could fall within the scope of Article 101 and 102 TFEU[104].

87 Guidance letters are not Commission decisions to be binding for Member States' competition authorities nor competent courts. However, they aid firms with informed assessments of their agreements, particularly because they will be publicly available where parties agree on a public version[105]. The Commission has never (at least publicly) issued guidance letters[106]. It is not clear whether any firm has asked for them or the Commission has refused to issue them[107].

88 In addition, the few comfort letters on patent pools issued before the coming into force of Regulation 1/2003 have not been made publicly available. Therefore, the EU lacks reports presenting the Commission's assessments of patent pools that can be used by firms in their self-assessment.

89 Unlike the EU, the US gives a particular weight to predictability as a promoting factor for firms in today's fast changing world. The publication of the BRLs in the US creates a good degree of legal certainty as the DOJ's analyses presented within provide guidance for both the firms and public regarding the scope, interpretation, and application of antitrust law. The US Agencies have created a template for patent pools through the BRLs which, having led to the establishment of dozens of patent pools over time, describes the structure of modern patent pools.

90 The fact that the comfort letters are inaccessible in the EU is not defendable nor helpful. This legal uncertainty and the lack of assessment template for patent pools should be eliminated. Promisingly, the EU resumed paying attention to predictability as the recent Horizontal Guidelines revision shows a particular focus on legal certainty[108] as

100 Council Regulation, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32003R0001.

101 G. Monti, Business Cooperation in Times of Emergency: The Role of Competition Law. <https://www.competitionpolicyinternational.com/business-cooperation-in-times-of-emergency-the-role-of-competition-law/#_ednref18>.

102 C. Gauer *et al.*, Regulation 1/2003 and the Modernisation Package fully applicable since 1 May 2004, Competition Policy Newsletter. <https://ec.europa.eu/competition/publications/cpn/2004_2_1.pdf>. pp.5-6.

103 European Commission, Commission Notice on informal guidance relating to novel questions concerning Articles 81 and 82 of the EC Treaty that arise in individual cases (guidance letters). <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52004XC0427(05)>.

104 *Ibid.* para. 11.

105 *Ibid.* paras. 22-25.

106 G. Monti, Business Cooperation in Times of Emergency: The Role of Competition Law.<https://www.competitionpolicyinternational.com/business-cooperation-in-times-of-emergency-the-role-of-competition-law/#_ednref18>.

107 The Commission highlights the primary objective of the Regulation 1/2003, which is to ensure effective enforcement and stipulates that the Commission may only provide informal guidance if this is compatible with its enforcement priorities. Commission Notice. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52004XC0427(05)>. para. 7.

108 Evaluation of Commission Regulation (EU) No 1217/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the Functioning of the European Union to certain categories of research and development agreements and of Commission Regulation (EU) No 1218/2010 of 14 December 2010 on the application of Article 101(3) of the Treaty on the

the contributors advise that the Guidelines should provide a higher degree of legal certainty to participants of cooperation in digital markets[109]. This expectation is truly in line with the spirit of EU law where legal certainty is considered a general principle of jurisprudence of the ECJ and a guiding idea of most legal systems of Member States[110] Legal certainty defined as "maximum predictability of officials' behaviour"[111] is safeguarded when validly made laws are publicly declared. In this way, subjects can rely on the law and foresee application of state power[112].

II. Inclusion of substitute/non-essential patents into pool

91 Both systems agree that pools with complementary patents are assessed with greater confidence than those containing substitute patents.

92 Inclusion of only essential technologies in a pool (which are complements by necessity) safeguards it from antitrust scrutiny in both systems. In the EU, such a pool falls outside Article 101(1) TFEU irrespective of the parties' market position[113]. Limiting a pool to essential patents ensures that rivalry is neither foreclosed among patents within the pool nor between patents in the pool and patents outside it[114].

93 The EU and the US also recognise that the inclusion of non-essential patents may unreasonably foreclose the non-included competing patents from use by manufacturers. In this situation, the manufacturers may be forced to pay for unneeded technology that leads to collective bundling[115]. However, both the EU and US acknowledge that these restrictive agreements may result in pro-competitive efficiencies. Hence, they must be analysed under Article 101(3) and rule-of-reason, and be balanced against the negative effects on competition. In the EU, the conditions of Article 101(3) are likely to be fulfilled if a pool including non-essential patents: (a) fulfils all the criteria of the safe harbour, (b) proves pro-competitive effects, and (c) lets licensees have the possibility of obtaining a licence for only part of the package with a corresponding reduction of royalties.[116].

94 The EU and the US also recognise that pools composed of pure substitute patents are more likely to harm social welfare and to raise antitrust concerns. This inclusion would risk turning the pool into a price-fixing mechanism and increase the total royalty rate. However, the EU Commission more strictly assesses this inclusion than the US, as it considers it a violation of Article 101(1) and states that the fulfilment of the conditions provided in Article 101 (3) is unlikely to be obtained[117]. In fact, the EU totally rules out the inclusion of substitute patents.

95 In contrast, the DOJ states that it would not challenge the inclusion of substitute patents in a pool without considering whether it produces significant efficiencies[118]. It considers it reasonable to include substitute patents in a pool if their inclusion does not enhance market power or if the pool creates significant efficiencies that outweigh the risks of competitive harm. Such inclusion, therefore, is not seen unlawful *per se* and the competitive costs and benefits of such a pool is analysed under its fact, context, and the rule-of-reason[119].

96 The following section provides a discussion on why we believe that the US approach in this regard is more reasonable and in contrast why the EU counterpart is not necessary nor pro-pooling.

Functioning of the European Union to certain categories of specialisation agreements, 07/04/2020. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=PI_COM:Ares(2020)1972062>.

109 Main Theses on Reform of Horizontal Guidelines (HGL), Specialisation Block Exemption Regulation (SBER) & Research & Development Block Exemption Regulation (R&D BER), Ref. Ares(2020)917048 - 12/02/2020. <https://ec.europa.eu/competition/consultations/2019_hbers/index_en.html>.

110 J. Raitio, The Principle of Legal Certainty in EC Law. p.125.

111 E. Claes et al., Facing the Limits of the Law. p. 92.

112 James R Maxeiner, 'Legal Certainty and Legal Methods : A European Alternative to American Legal Indeterminacy ?' (2007) 15 Tul. J. Int'l & Comp. L 541.p. 546.

113 TT Guidelines. para. 262.

114 DVD6C Business Review Letter at 12.

115 TT Guidelines. para. 262.

116 TT Guidelines. para. 265.

117 T Guidelines. para. 255.

118 DVD6C Business Review Letter at 12.

119 IPXI Business Review Letter and Promoting Innovation and Competition, p. 78.

1. Difficulty in distinction

97 Despite having effect on antitrust assessment, the distinction between complementary/substitute and essential/non-essential patents is unclear and requires an on-going assessment. As a matter of fact, certain non-essential patents may become essential as technology evolves and certain technologies can be partly complementary and substitute.

98 Additionally, the essentiality test does not work well for patent pools outside standards and even in the case of standard-related pools, this concept is inherently ambiguous[120]. Neither system defines essential patents clearly as what is essential may vary from one patent pool to another[121]. Some pools define an essential patent in a technical context as one that is essential to manufacture a product in accordance with standard specifications. While some others, once a patent is commercially necessary based on consumers' demand, regard it as essential in assessing the potential threats on competition in by the pool creation. In this context, the definition of essentiality encompasses not only patents that are necessarily essential to the standard, but also those essential to the standard as a practical matter because there are no economically viable substitutes for that patent[122]. We believe that the determination of commercially essential patents is impossible as it requires proving the absence of real alternatives known as devil's proof, i.e. impossible proof of nonexistence[123].

99 Perhaps that is why the US IP Guidelines avoid explicitly mentioning the distinction between complementary and substitute patents, nor give any reference to their essentiality. They assess the inclusion of non-essential/substitute patents under the rule-of-reason and consider it possible, reasonable, and even efficient under some circumstances. Oddly, although the Commission highlights that the distinction between substitute and complementary is unclear[124], it makes explicit distinctions between them and accordingly specifies principles to assess competitive characteristics of each type. In addition, the Commission expresses that the essentiality examination is time dependent, as a patent essential at one point may later become non-essential or substitute due to the emergence of new third-party technologies[125].

100 One may conclude that when a distinction is not clear nor absolute, the EU, instead of taking a strict position, is better to adopt the US approach through assessing patent combinations on a case-by-case basis.

2. Uncertainties related to price fixing and competition foreclosure

101 Tying prevents licensees from switching to substitute technologies[126]. Once substitute technology is bundled in the pool and licensed as a part of the package, and the royalty paid for the package covers already a substitute technology, then licensees are less likely to license a competing technology outside the pool[127]. However, this does not always lead to price fixing and competition foreclosure. As far as price fixing is concerned, the pool is unlikely to enable collusion among licensors and create price fixing if: (a) the royalty rate is charged per-unit irrespective of patents number and type (as it was the case in the 3C DVD pool[128]), and (b) the royalty is sufficiently small compared to the total costs of manufacture[129].

102 In the EU, there is no decision that addresses tying in the context of licensing agreements and as such, this article studies the US *Philip* case to see under what circumstances tying and competition foreclosure may happen.

US *Philip* case

103 The International Trade Commission (ITC) ruled that Philips' licensing arrangement comprising of essential and non-essential patents for CD products was a tying arrangement and constituted patent misuse. The ITC decided that the anti-competitive effects of this inclusion outweighed its pro-

120 Hans Ulrich, 'Patent Pools - Policy and Problems' in Josef Drexl (ed), *Research Handbook on Intellectual Property and Competition Law* (Edward Elgar Publishing Limited 2008).p. 152.

121 MPEG-2 Business Review Letter at 5 and DVD6CBusiness Review Letter at 3 - 5.

122 RFID Business Review Letter.

123 Nobuyuki Hamanaka, 'Distinction between Complementary and Substitute Patents as a Matter of Competition Law; Observations from Comparative Perspective' (Munich Intelectual Property Law Center (MIPLC) 2011) <http://www.miplc.de/research/>. p.52.

124 TT Guidelines. para. 254.

125 TT Guidelines. para. 263.

126 TT Guidelines. para. 223.

127 *Ibid*. para. 262.

128 3C DVD Business Review Letter.

129 *Ibid*.

competitive effects as it could foreclose alternative technologies and harm competitors seeking to license alternative technologies to parties who needed to obtain licenses to Philips's essential patents[130].

104 Philips then appealed and the Court of Appeal overturned the ITC's decision based on distinguishing between "patent-to-product" and "patent-to-patent" tying arrangements. According to the ruling, in patent-to-product tying, the patentee uses the market power conferred by the patent to force customers to purchase a product in a separate market that the customer might otherwise purchase from a competitor. Hence, the patentee can use its market power to foreclose competition in the market for the product[131].

105 However, patent-to-patent tying (which is what was discussed in *Philips* case) is different as the package licensing including both essential and non-essential patents does not: impose any requirement on the licensee; prevent the licensee from using any alternative technology that may be offered by a competitor of the licensor; and, foreclose the competitor from licensing their alternative technology[132].

106 The Court also stipulated that Philips gave its licensees the option of using any of the patents in the package at the licensee's option and charged a uniform licensing fee regardless of which or how many of the patents in the package the licensee chooses to use in its manufacturing process[133]. The royalty fee neither increased nor decreased regardless of number of patents chosen by the licensee, and inclusion of non-essential patents avoided increasing the royalty rate[134].

107 The Court conclusion was that bundling essential and non-essential patents in the form of patent-to-patent arrangements is unlikely to create anti-competitive effects and is not considered an unlawful practice,

- if licensees are not forced to take from a licensor anything unwanted (i.e. tied product). In this context, to create tying there should be evidence that licensee or potential licensee asked them to remove any of non-essential patents from the package and the patentee refused to do so[135];

- if licensee is not restricted from obtaining licenses from other sources to produce the relevant technology. The court stated that patents within a package can be regarded as non-essential only if there are commercially feasible alternatives to those patents. If it is not the case, packaging those non-essential together with essential patents can have no anti-competitive effect in the market because no competition for a viable alternative product is foreclosed. In fact, in such patent packaging there is no two separate products to fulfil tying condition[136];

- if the royalty is set on a per-unit basis and it does not vary depending on whether the licensee uses only the essential patents or all of the patents in the package. The court highlighted that package license agreements in which the royalty was based on the number of units produced but not the number of patents used to produce them, can resolve all potential patent disputes in advance between the licensor and the licensee. Whereas licensing patent rights on a patent-by-patent basis can result in continuing disputes over whether the licensee's technology infringes certain ancillary patents owned by the licensor that are not part of the group elected by the licensee[137].

108 A nonessential patent is valueless. The Court explained that the value of any patent package is largely (if not entirely) based on the essential patents. It found it rational for a patentee who has essential and non-essential patents to charge what the market will bear for the essential and to offer the others for free. Because if the patentee allocates royalty fees between its essential and non-essential patents, he runs the risk that licensees will take a license to only the essential ones and thereby, he will not be able to obtain the full royalty value of the essential patent[138].

109 The court also referred to the fact that the line between competitive and complementary patents is very difficult to draw. It also added that an agreement that was perfectly lawful when executed could be challenged as *per se* patent misuse due to developments in the technology of which the

130 *U.S. Philips corp. v. ITC*, 424 F.3d 1179, 1193 (Fed. Cir. 2005), p.1184.

131 *Ibid*. 1189.

132 *Ibid*. 1180.

133 *Ibid*. 1188.

134 *Ibid*.

135 *Ibid*. 1195.

136 *Ibid*. 1194.

137 *Ibid*. 1190-1191.

138 *Ibid*.

patentees are unaware or which have just become commercially viable. Such a rule would make patents subject to being declared unenforceable due to developments that occurred after execution of the license or were unknown to the parties at the time of licensing. Not only would such a rule render a licence subject to invalidation on unknown grounds at the time of licensing but it would also provide a strong incentive to litigation by any licensee since the reward for showing that even a single license in a package was non-essential would render all the entire package unenforceable[139].

110 The case analysis shows that the anti-competitive effects of tying practice which result from the inclusion of non-essential patents into the pool is much doubtful. Therefore, the tying practice should be examined on a case-by-case basis given the fact that the inclusion may lead to pro-competitive effects, since:

- it could reduce transaction costs including costs associated with determining individual patent-by-patent royalty and monitoring of non-essential patents;
- pooling non-essential patents can create efficiency because the combination of essential and non-essential technical elements allows the technology as a whole to be exploited more efficiently than otherwise, particularly in the case of implementation patents;
- this inclusion may ensure that the production under the license conforms to quality standards; and
- it may encourage third parties to develop technology which is not essential but necessary or useful for putting the essential technology into practice.

3. Negative effects of EU approach on product-based pooling

111 The EU's strict approach toward inclusion of non-essential/substitute patents into a pool may also affect the product-based pools as a recent form of pooling discussed in section B.II.2.b). This type of pooling offers all patents necessary for a product which may consist of essential and non-essential/substitute patents. Such pooling has attracted several licensing providers including One-Blue and Avanci where they can provide their licensees with as many patents as possible for a specific application or product all at once. This also can attract newcomers in the IoT era.

112 This approach can, therefore, prevent the promotion of such pools and their significant role in the EU's economy. The 23 million European SMEs, as the lifeblood of Europe's economy, accounting for 98 percent of businesses[140] are often behind large firms in standardisation due to the technological complexity and/or the huge investment required to develop a competitive technological platform. They, however, can enhance their competitiveness and reputation by implementing standards in their products [141]. Nevertheless, as pure implementers, SMEs mostly lack the skills necessary to identify the key players in the field. Or if they identify them, they lack the means to contact them or to identify the essential patents because large licensors mainly conclude their deals within each other. Thus, providing them with one package of necessary technologies tested by an independent agent along with the cost benefit and other advantages of patent pools can be very beneficial for such a large chunk of the European economy. [142].

113 The discussion presented in this section shows that the EU's approach toward inclusion of substitute/essential patents into pools is not reasonable. Hence, we propose to analyse patent combinations on a case-by-case basis for three reasons. First, the characterisation of pooled patents is very difficult in practice and founding the legality of a practice on a varying characterisation makes no sense and undermines legal certainty. Second, this inclusion does not necessarily create price fixing nor competition foreclosure as shown. Third, this approach can negatively affect product-based pools as effective mechanisms which satisfy the IoT newcomers' needs in getting required licences for their products.

139 Ibid. 1196-1197.

140 European Commission, Thinking Big for SMEs. <https://ec.europa.eu/docsroom/documents/874/attachments/1/translations/en/renditions/pdf>.

141 Henk J De Vries and others, *SME Access to European Standardization Enabling Small and Medium-Sized Enterprises to Achieve Greater Benefit from Standards and from Involvement in Standardization* (Rotterdam School of Management, Erasmus University, Rotterdam, the Netherlands 2009) <https://www.researchgate.net/publication/259005422_SME_access_to_European_standardization_Enabling_small_and_medium-sized_enterprises_to_achieve_greater_benefit_from_standards_and_from_involvement_in_standardization>.

142 Harris Tsilikas and Claudia Tapia, 'SMEs And Standard Essential Patents: Licensing Efficiently In The Internet Of Things' (2017) LII Les Nouvelles - Journal of the Licensing Executives Society 170 <ssrn: https://ssrn.com/abstract=3009039>.

E. Conclusion

114 This study showed how competition law impacted the creation and the operation of patent pools: the more relaxed antitrust policy, the further the growth of patent pools. In the pooling promotion context, the goal should be to help patent pools develop in compliance with competition law. This will yield to innovation, FRAND access to SEPs, and consumer welfare. The pro-competitive effects of patent pools are so significant that it is worth paying great attention to the policies which apply to them. However, some EU policies have anti-pooling effects and decelerate its regulatory framework development with respect to pooling and the progress of the cutting-edge technologies.

115 Notably, there are factors beyond competition law which can have influence on patent pools. For example, firms' business models can shape their tendency or reluctance to establish or join pools. Some empirical analyses have shown that vertically integrated firms have higher pool participation rates, while pure innovators are often unwilling to join pools[143]. These factors are beyond the scope of the present paper.

143 Reiko Aoki and Sadao Nagaoka, 'Coalition Formation for a Consortium Standard through a Standard Body and a Patent Pool: Theory and Evidence from MPEG2, DVD and 3G' (2005). pp. 7-9.

The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act

by **Folkert Wilman***

Abstract: Over the past two decades the principle of knowledge-based liability has been the backbone of the EU's regime regulating the liability of social media companies, online marketplaces, cloud storage providers and many other online service providers that store and disseminate user-generated content. This article traces the origins, identifies the rationale, assesses the continued relevance and discusses the main strengths and shortcomings of this approach. It is argued that, counter-intuitive as it may seem to some, there are good grounds for retaining the key features of the current liability system, which conditionally shields such service providers from liability for their users' content. Most important is the system's ability to strike a fair balance between the conflicting rights and interests of the parties involved – not only the service providers and the users, but also the parties aggrieved by the content. That is not to say, however, that the system has no shortcomings. In particular, it is shown that the system's effectiveness in terms of tackling illegal user content causing serious 'public' harm could be improved, whilst the system also involves significant risks of unjustified removal of user content. These shortcomings do not mean that the current knowledge-based liability system should be disgcarded, however. Instead, it should be improved. Not by excluding certain service providers from the scope of the liability exemption or adding conditions, but rather by enacting complementary requirements. Against this background the article assesses to which what extent the recently proposed Digital Services Act addresses the identified shortcomings.

Keywords: intermediary liability; hosting service providers; notice and action; e-Commerce Directive; Digital Services Act (DSA)

Recommended citation: Folkert Wilman, The EU's system of knowledge-based liability, 12 (2021) JIPITEC 317 para 1

A. Introduction

1 If somebody came up today with the idea of laying down in law a provision exempting online service providers such as Facebook, YouTube and Twitter from liability for the user content that they store and disseminate, the idea would likely not be well received. These online giants are subject to increasingly critical public and political scrutiny, both in the European Union (EU) and the United States (US). The controversy surrounding the decisions by Twitter and Facebook to suspend (then) US President Trump's account for inciting violence in early 2021[1]

* Member of the Legal Service of the European Commission. The views expressed in this article are personal and cannot be attributed to the author's employer. The article is in part based on research carried out for the author's recent book: F Wilman, *The responsibility of online intermediaries for illegal user content in the EU and the US* (Edward Elgar 2020). All online sources cited were last visited on 13 June 2020. The author thanks Irene Roche Laguna and Miquel Peguera Poch for their

is only the latest example of a long-standing and broader debate about the responsibilities of such service providers. The criticism mostly turns around the perception that users, competitors and society at large are not sufficiently protected against the downsides of their ways of doing business and the power they exercise – not that the service providers themselves need protection. Yet, in both the EU and the US, there are rules in place that do precisely that: protecting the service providers concerned. For over two decades now, in both jurisdictions laws ensure that they are exempted from liability relating to the content that they store for their users, provided they do not have knowledge of the content's illegality and act expeditiously to remove the content once they obtain such knowledge. In the EU, the rule applies to all kinds of illegal content and has been laid down in Article 14 of the e-Commerce Directive (ECD), adopted in 2000.[2] The rule was inspired by a comparable rule of US law applicable specifically in relation to copyright-infringing user content, laid down in Section 512(c) of the 1998 Digital Millennium Copyright Act (DMCA).[3]

2 What is more, in its proposal for a new Digital Services Act[4] (DSA), tabled in December 2020, the European Commission ('the Commission') suggests leaving the aforementioned rule essentially unaltered. It stated that the current liability regime is "*by now established as a foundation of the digital economy*".[5] As will be seen below, whilst the DSA proposal provides for a range of new measures, it largely reproduces Article 14 ECD.[6] That implies that the basic principle would remain that of knowledge-based liability. Indeed, it appears that the Commission never even seriously questioned the continued validity of the principle; an in-depth analysis of its pros and cons is not provided for.[7] In the US, the laws in question are under review, too. A study of Section 512 DMCA by the US Copyright Office was critical on several points, but recommended some fine-tuning rather than any wholesale change.[8] But it is the second cornerstone of US liability law applicable to online service providers – Section 230 of the Communication Decency Act (CDA),[9] adopted in 1996 – that tends to be criticised most broadly and strongly.[10] This law unconditionally exempts such providers from most

comments on earlier drafts of the article.

1 See <https://blog.twitter.com/en_us/topics/company/2020/suspension.html>; <https://www.facebook.com/zuck/posts/10112681480907401> (announcing and explaining the decisions of Twitter and Facebook, respectively). More recently, see also <https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/>.

2 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market, [2000] OJ L 178/1 ('ECD').

3 17 USC Section 512. Although Section 512(c) DMCA was not the sole source of inspiration for Article 14 ECD, it is widely believed to have played an important role, as is also evident from the similar wording. See eg M Husovec, 'How Europe wants to redefine global online copyright enforcement', in T Synodinou (ed), *Pluralism or universalism in international copyright law* (Kluwer Law International 2019), 514; P Przemyslaw Polanski, 'Rethinking the notion of hosting in the aftermath of Delfi: shifting from liability to responsibility?', (2018) *Computer Law and Security Review* 34, 871; J Urban, J Karaganis and B Schofield, 'Notice and takedown in everyday practice', UC Berkeley Public Law Research Paper No 2755628 2017, 22; P Van Eecke, 'Online service providers and liability: a plea for a balanced approach', (2011) *Common Market Law Review* 48, 1456.

4 Commission, Proposal for a Regulation on a single market for digital services (Digital Services Act), COM(2020) 825 ('DSA proposal').

5 Commission, Explanatory memorandum DSA proposal, COM(2020) 825, 3.

6 See further section H below.

7 See eg the inception impact assessment relating to the DSA proposal, available via <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services> (indicating that, whilst certain adjustments might be necessary, "*the underpinning basis is as valid today as it has been 20 years ago*"). See also Commission, Impact assessment DSA proposal, SWD(2020) 348, 150 ("*the logic behind the liability regime remains valid today. [...] Hence, any update of the existing rules needs to bear in mind that the main principle of non-liability for third party content remains*").

8 US Copyright Office, 'Section 512 of Title 17: a report of the register of copyrights', 2020, 7. See also the draft bill for the Digital Copyright Act 2021, available via <https://www.tillis.senate.gov/services/files/97A73ED6-EBDF-4206-ADEB-6A745015C14B> (suggesting more substantial changes, in particular a partial staydown obligation to complement the knowledge-based liability system).

9 47 USC Section 230.

10 Critics include both former President Trump and current President Biden. President Biden (when not yet elected) called for the repeal of Section 230 CDA; see *New York Times*, 'Joe Biden, former vice president of the United States', 17 January 2020. Former President Trump and his administration (when still in office) criticised the law on several occasions. See in particular Executive Order 13925, 'Preventing Online Censorship', 85 FR 34079, 2020 (attempting to limit the law's scope of application; since revoked).

forms of liability for user content.[11] That means that – unlike under Article 14 ECD and Section 512(c) DMCA – the liability exemption is available also where the providers had been notified and nonetheless decided not to act against illegal content.[12] For now, it is uncertain whether, when and how Section 230 CDA will be reformed. It may be widely criticised, but this is done on different grounds.[13] Still, a common suggestion is to align the law with Section 512(c) DMCA and thus to make knowledge-based liability the basic principle.[14]

3 It thus appears that the principle of knowledge-based liability for online service providers in respect of the content that they store for their users is – and in all likelihood will continue to be – a key component of the liability regimes of both the EU and the US. Already for this reason it is important to properly understand this approach and especially its main strengths and shortcomings. That holds true all the more so precisely because in both jurisdictions the relevant regimes are now under review and additional measures are being considered. Given that such possible additional measures are generally not meant to *replace*, but rather to come *on top of* the current rules, the former should be designed to build on the latter's strengths and address their shortcomings. In other words, when new proposals are tabled it may be tempting to jump straight to the novel parts, such as the diligence obligations or reinforced enforcement powers set out in the DSA proposal. Yet in many respects those parts cannot properly function – and cannot be properly understood – without having regard to the foundation that the principle of knowledge-based liability provides. Developments in this field are often said to entail an evolution 'from liability to responsibility'.[15] Noteworthy as that evolution may be, a more accurate description might be 'liability *and* responsibility'.[16] The latter complements but does not replace the former.

4 That being so, this article aims to assess the continued relevance and identify the main strengths and shortcomings of the principle of knowledge-based liability as applied in the context of efforts aimed at tackling illegal content that online service providers store and often disseminate for their users. That also requires tracing the principle's origins and identifying its rationale. In doing so, the article seeks to contribute to the understanding, and allowing for the assessment, of EU law developments in this regard – most notably, the transition from the system currently laid down in Article 14 ECD to the one to be contained in the DSA. While this article accordingly mainly focuses on EU law, an account is also taken of developments in the US. That is done for several reasons. First, the US is the country where the knowledge-based liability model, as codified in law and applied in this particular context, originates. Second, many large online service providers active in the EU originate and continue to be based in the US. Their behaviour is therefore shaped by the country's legal set-up.[17] Third, in the US much experience has been gained in applying the model in practice, which offers valuable insights also for the EU's efforts to update it legal framework.

11 Section 230 CDA does not cover liability under intellectual property law. It also contains certain other exclusions, most notably in respect of liability under Federal criminal law. See Section 230(e) CDA.

12 See eg US Court of Appeals DC Circuit, *Marshall's Locksmith Service v Google*, 925 F3d 1263 (2019); US Court of Appeals 1st Circuit, *Universal Communications Systems v Lycos*, 478 F3d 413 (2007); US Court of Appeals 4th Circuit, *Zeran v America Online*, 129 F3d 327 (1997).

13 In as far as criticism by politicians is concerned, Democrats tend to criticise Section 230 CDA for being overly protective of large online service providers, whereas Republicans tend to criticise it for disadvantaging conservative viewpoints. See further F Wilman, *The responsibility of online intermediaries for illegal user content in the EU and the US* (Edward Elgar 2020), 119-130 (giving an overview of opinions of stakeholders, academics and courts on Section 230 CDA).

14 See eg J Balkin, 'Free speech is a triangle', (2018) *Columbia Law Review 118*, 2046; M Roter, 'With great power comes great responsibility: imposing a "duty to take down" terrorist incitement on social media, (2017) *Hofstra Law Review* 45, 1404; O Medenica and K Wahab, 'Does liability enhance credibility: lessons from the DMCA applies to online defamation', (2007) *Cardozo Arts and Entertainment Law Journal* 25, 265-267. Similar suggestions have occasionally been made in the case law; see eg US Court of Appeals 9th Circuit, *Batzel v Smith*, 33 F3d 1018 (2003). See also the US Senate bill with a proposal to reform Section 230 CDA that was put forward in June 2020: 'Platform Accountability and Consumer Transparency Act' (PACT Act), available via <https://www.schatz.senate.gov/imo/media/doc/OLL20612.pdf>.

15 Eg A Kuczerawy, 'General monitoring obligations: a new cornerstone of Internet regulation in the EU?', 2019, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3449170>, 1; Przemyslaw Polanski (n 3); G Frosio, 'Why keep a dog and bark yourself? From intermediary liability to responsibility', (2018) *Oxford International Journal of Law and Information Technology* 26, 1–33.

16 Cf A Savin, 'The EU Digital Services Act: towards a more responsible internet', Copenhagen Business School Law Research Paper Series No. 21-04, 2021, 5 (speaking of "*a double-edged regime of liability*").

17 Cf L Klonick, 'The New Governors: the people, rules, and process governing online speech', (2018) *Harvard Law Review* 131, 1598–1670.

5 The remainder of this article is structured as follows. First a brief overview is given of the EU's legal framework, in particular the liability exemption for hosting service providers as currently laid down in Article 14 ECD (section B). Next, the rationale of the knowledge-based liability model is explained (section C). Attention then turns to the developments – both in practice and in law – that have taken place since the principle of knowledge-based liability was enshrined in EU law about two decades ago (sections D and E). The following two sections focus on the shortcomings associated with this regime. A distinction is made between shortcomings relating to the aim of tackling illegal user content on the one hand and those relating to the protection of users on the other hand (sections F and G). Lastly, against the background of the foregoing the relevant parts of the DSA proposal are assessed (section H), before terminating with a brief conclusion (section I).

B. Current EU legal framework

6 As mentioned, in the EU, the principle of knowledge-based liability is currently enshrined in Article 14 ECD. In essence, the article states that providers of so-called 'hosting' services cannot be held liable for the content that they store for their users, unless they obtain knowledge of the illegality of the content and fail to act expeditiously by removing the content.[18] It is disputed precisely which sorts of services qualify as 'hosting' within the meaning of this provision. In itself, it is clear that the concept of 'hosting' refers to the storage by a service provider of content provided by and stored at the request of users of the service in question.[19] A broad range of services could therefore, in principle, qualify. The case law captures the activities undertaken by social media companies such as Facebook, by online marketplaces such as eBay and by video-sharing platforms such as YouTube.[20] Yet a broad range of other activities, such as those performed by cloud storage providers and consumer review sites, should normally be able to qualify as well. The concept is therefore considerably broader than traditional website hosting.[21]

7 The Court of Justice of the EU ('Court of Justice' or 'Court') has specified that, for the hosting activities to be covered by Article 14 ECD, the service providers concerned must not "*play an active role of such as kind as to give them knowledge of, or control over*" the user content in question.[22] This serves as a reminder that the liability exemption at issue here is not available where the content potentially giving rise to liability is the provider's 'own' content.[23] Yet the Court's criterion is broader. It also relates to content in respect of which the provider departed from the neutral position that it is expected to retain as an intermediary.[24] In the context of the activities of an online marketplace the Court has clarified that the service provider retains a neutral position where it "*stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers*". By contrast, the service provider is considered not to have retained such a neutral position where it "*provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers*".[25]

8 A degree of uncertainty exists as to where the line should be drawn precisely, however.[26] That is so especially because many service providers do not merely store user content, but also conduct certain additional activities in relation thereto. For instance, organising the user content by indexing it, making it searchable or recommending it to other users.

18 For reasons of ease of reference and readability, some matters are simplified in this article. First, Art 14(1) ECD covers not only the situations where the service providers *obtain* knowledge, but also where they already *have* it. Second, the reference to 'knowledge' is meant to cover both types of knowledge that Art 14(1) distinguishes, namely, 'actual knowledge' and 'awareness' (the latter being applicable specifically in relation to actions for damages and entailing construed knowledge). Third, Art 14(1) provides, as an alternative to the *removal* of illegal content, also for the possibility of *disabling access* thereto.

19 The term 'storage' refers to the holding of data in the memory of a server. See CJEU, *L'Oréal v eBay*, C-324/09, ECLI:EU:C:2011:474, 110.

20 See, respectively, CJEU, *Glawischnig-Piesczek v Facebook Ireland*, C-18/18, ECLI:EU:C:2019:821; CJEU, *L'Oréal v eBay* (n 19); CJEU, *YouTube*, C-682/18 and C-683/18, ECLI:EU:C:2021:503.

21 Cf Przemyslaw Polanski (n 3), 875-877 (making a similar point). See also J Van Hoboken, J Quintas, J Poort and N Van Eijck, 'Hosting intermediary services and illegal content online: an analysis of the scope of Article 14 ECD in light of developments in the online service landscape', Study for the Commission, 2018, 9-16 (containing a typology of hosting services).

22 CJEU, *L'Oréal v eBay* (n 19), 113. See also CJEU, *YouTube* (n 20), 106.

23 This includes content that has been provided by a user that is under service provider's control or authority (Art 14(2) ECD). See also CJEU, *Papasavvas*, C-291/13, ECLI:EU:C:2014:209.

24 Cf CJEU, *YouTube* (n. 20), 105-105; CJEU, *L'Oréal v eBay* (n 19), 112.

25 Ibid, 115-116.

26 See eg Commission, Impact assessment DSA proposal, SWD(2020) 348, 31-32. See also para 46 below.

Arguably, many of such activities are needed to enable users to have meaningful access to the large quantities of user content that many service providers store.[27] Importantly, the aforementioned criterion articulated by the Court of Justice does not require absolute passivity[28] – it implies that the service provider *can* be active to some extent, provided its involvement is not such as to give it knowledge of or control over the user content concerned. The recent judgment by the Court of Justice in the *YouTube* case provided some further guidance in this respect, at least in situations involving allegedly copyright-infringing user content stored on video-sharing and file-sharing platforms.[29] The judgment implies that the mere fact that the service providers concerned conduct the aforementioned kinds of activities does not mean that they are, necessarily and a priori, excluded from the scope of Article 14 ECD for being 'too active'. The Court appeared to assess the matter rather under the conditions on the providers acting expeditiously upon obtaining knowledge. At the same time, the judgment still leaves uncertainty. That is so especially in relation to the question identified therein whether the service providers contribute, 'beyond merely making the platform available', to giving the public access to the stored user content in breach of copyright. The main conclusion therefore appears to be that there are few bright-line rules. Rather, a case-by-case assessment is required to determine whether the provider's role is a neutral one.

9 When it comes to the types of liability stemming from illegal user content covered by the liability exemption, the scope of the protection offered by Article 14 ECD is wide. Although the Court of Justice has to date not expressly confirmed this, it is generally believed that the term 'liability' refers to liability regardless of whether it is civil, administrative or criminal in nature.[30] The liability exemption is 'horizontal' also in another sense: it applies irrespective of the field of law at issue. Consequently, covered is possible liability under laws on, inter alia, intellectual property, defamation, privacy, anti-terrorism, child pornography and hate speech.[31]

10 It is important to underline that we are dealing here with an *exemption* from liability. The rules potentially *establishing* the liability of the service providers are in principle to be found in the laws of the Member States (and, occasionally, EU law).[32] Therefore, where a hosting service provider fails to meet the conditions of the liability exemption of Article 14 ECD – in particular, expeditiously removing the item of illegal content upon obtaining knowledge thereof – this does not necessarily mean it is liable for the user content in question. Rather, it means that the hosting service provider is not a priori *shielded* from such liability. One 'type' of liability is carved out from the liability exemption, however. National courts or administrative authorities can, in accordance with the applicable rules of national law, require a hosting service provider to "*terminate or prevent an infringement*", irrespective of whether or not the conditions of the liability exemption are met.[33] In other words, injunctive relief is excluded from the scope of the liability exemption.

11 Under Article 14 ECD, the knowledge of the illegality of items of stored user content, which in turn triggers the expectation for hosting service providers to expeditiously remove such content (if they want to benefit from the liability exemption, that is), can be obtained in several manners.[34] The

27 See also para 14 and 20 below (expanding on the quantities of user content stored).

28 The discussion is therefore sometimes wrongly simplified as being about the active or passive role of the service provider. In this regard, it is noticeable that, in CJEU, *L'Oréal v eBay* (n 19), the word 'passive' is not mentioned at all, although that is different in other rulings, most notably CJEU, *YouTube* (n. 20), 105 and CJEU, *Google France*, C-236/08 to C-238/08, ECLI:EU:C:2010:159, 113-114. See also Opinion Advocate General (AG) Jääskinen, *L'Oréal v eBay*, C-324/09, ECLI:EU:C:2010:757, 138-146 (strongly criticising the approach seemingly requiring strict neutrality taken in *Google France*). Cf Van Hoboken et al (n 21), 31 and 33 (arguing that in this connection the terms 'neutral', 'active' and 'passive' should be understood as terms of art and as non-binary, encompassing a range of meanings along a spectrum of potential activities).

29 CJEU, *YouTube* (n. 20), in particular 108 and 114. See also the opinion of AG Saugmandsgaard Øe in that case, ECLI:EU:C:2020:586, 143-168.

30 See eg AG Saugmandsgaard Øe, *YouTube* (n 29), 138; Opinion AG Szpunar, Case C-484/14, *McFadden*, ECLI:EU:C:2016:170, 64; Commission, Proposal for a Directive on certain legal aspects of electronic commerce in the internal market, COM (1998) 586 ('Proposal ECD'), 27 and 29.

31 Cf Recital 16 Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, [2001] OJ L 167/10 ("*Liability for activities in the network environment [...] is addressed horizontally in [the ECD]*"). Cf also Commission, Proposal ECD, COM(1998) 586, 27. See however also para 50 below (regarding the specific regime applicable to certain service providers in relation to copyright-infringing content contained in Art 17 CDSM Directive, which deviates from Art 14 ECD).

32 Cf eg CJEU, *Google France* (n 28), 107; Commission, Proposal ECD, COM(1998) 586, 27.

33 Art 14(3) ECD. Cf CJEU, *Facebook Ireland* (n 20), 25.

34 CJEU, *L'Oréal v eBay* (n 19), 122.

knowledge will frequently be obtained through the reception of a notice – that is, a message sent by a third party informing the service provider of the presence of allegedly illegal content on its service and typically requesting its removal. As such, the liability exemption provides the basis for a system of 'notice and takedown', also known as 'notice and action'.[35] The resulting notice-and-action system is and remains in many respects the "*most popular internet enforcement mechanism*".[36] However, this does not mean that the service providers concerned cannot obtain knowledge of illegal user content on their services in other manners. That can occur, most notably, through investigations carried out on their own initiative. Large service providers, in particular, are increasingly proactive in scanning and moderating the content that they store for their users.[37]

C. Knowledge-based liability: rationale

12 Why is that providers of hosting services should be allowed to benefit from a conditional liability exemption of the type outlined above? Why not make them subject, for instance, to specific rules imposing strict liability for the content that they store and often disseminate for their users? These questions can be approached from two viewpoints: that of the hosting service providers themselves, and that of the other parties involved.

13 Starting with the former, there are two main elements that together argue against holding hosting service providers strictly liable. The first element is that, as was touched upon above, the content in question is by definition not their 'own'. The service providers do not create or submit the content themselves and they normally do not have knowledge of or control over the content either, at least initially. It seems natural to apply stricter liability standards only to parties that know of or exercise control over certain illegal material or conduct – or that are at least reasonably *capable* of obtaining such knowledge or exercising such control. For example, as a general rule, producers are strictly liable for their products and employers are strictly liable for the acts of their employees.[38]

14 The second main element that argues against holding hosting service providers strictly liable for user content relates to the large quantities of such user content that they tend to intermediate. This point is probably best exemplified by the ruling by an US court in *Netcom*, the case that lay the groundwork for Section 512(c) DMCA's notice-and-action mechanism, which in turn was a source of inspiration for the EU regime.[39] The case arose in 1995, in the early days of the popular internet. The court held that "*billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network*" and that it is "*practically impossible to screen out infringing bits from non-infringing bits*".[40] It therefore refused to hold the online services providers concerned primarily liable for the infringements in question, but did not rule out secondary liability. Likewise, the "*staggering*" amounts of user content at issue also played an important role in *Zeran*, the case that decisively shaped the broad manner in which Section 230 CDA's liability exemption is construed in the US.[41] This does not appear to be fundamentally different when it comes to Article 14 ECD.[42] In fairness, the quantities of user content involved do not, in themselves, necessarily *rule out* the service providers having knowledge of or control over the content. It rather means that they would have to take quite far-going measures to obtain such knowledge or control. In this regard, a comparison can be drawn with distributors of third-party materials in the offline world, such as postal service providers or bookshops. These parties could theoretically be required to examine all such materials that they transmit or sell, with a view to screening out illegal materials. Yet it would be, as the

35 Cf Recital 40 ECD.

36 J Riordan, *The liability of internet intermediaries* (Oxford University Press 2016), 63. See eg also Urban et al (n 3), 114 (concluding, based on an extensive study carried out in the US, that the notice-and-action system "*continues to provide an efficient method of enforcement in many circumstances*").

37 See eg J Kosseff, *The twenty-six words that created the internet* (Cornwell University Press 2019), 241-242; Klonick (n 17), 1619-1621. More generally, see T Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media* (Yale University Press 2018).

38 Cf A Yen, 'Internet service provider liability for subscriber copyright infringement, enterprise liability, and the First Amendment', Boston College Law School Research Paper No 2000-03, 2000, 25-28.

39 US District Court Northern District of California, *Religious Technology Center v Netcom*, 907 F.Supp. 1361 (1995). See also HR Rep No 105-551, pt 1 (1998), 11 (noting that the bill that was to become Section 512 DMCA essentially codifies the ruling in *Netcom*).

40 Ibid, 1372-1373.

41 US Court of Appeals, *Zeran* (n 12), 331.

42 Cf AG Saugmandsgaard Øe, *YouTube* (n 29), 175 and 183.

US Supreme Court put it, "*altogether unreasonable to demand so near an approach to omniscience*" from these intermediaries.[43]

15 That leads us to the second perspective: that of the other parties involved. Apart from the service providers, there are two such other parties in a typical situation: the *users* of the services and the *parties aggrieved* by the illegal content stored. Starting with the users, the key point is that the service provider's burden resulting from the imposition of strict liability may well become the public's burden, to again echo the US Supreme Court.[44] The measures that the service providers may feel obliged to take in order to avoid being held strictly liable will have adverse consequences for the users, too. The consequences could be economic in nature, such as higher costs for the use of the services. They could also consist of invasion of the users' privacy resulting from extensive and intrusive monitoring. What is more, the consequences could consist of reduced possibilities for users to express themselves and to receive information. That could occur for several reasons, including for example: because the measures taken by the service providers are inaccurate and block or remove user content wrongly thought to be illegal; because the service providers decide to no longer provide certain services in view of the liability risks; or because such measures deter users from uploading content in the first place. All this underlines the *instrumental* nature of the knowledge-based liability exemption. It serves not only to protect the service providers, but also – and arguably even primarily – the users.

16 In addition, one should take account of the interests of the aggrieved parties, such as the persons who hold the intellectual property right that is infringed or who are defamed by the user content. These parties would generally benefit from the imposition of strict liability, because that would strongly incentivise the service providers to take the aforementioned measures aimed at tackling the user content that infringes their rights. However, as noted, that approach would have significant downsides not only for the service providers, but also for their users. If, conversely, the service providers were to be broadly or even completely exempted from any form of liability, the aggrieved parties would likely encounter serious difficulties in enforcing their rights. This is one of the main reasons why the broad and unconditional liability exemption of Section 230 CDA is criticised.[45] True, aggrieved parties could then still have redress against the users who provided the content. However, this possibility may well be remote or even largely meaningless in practice, considering how difficult it tends to be to identify those users and hold them accountable.[46] Put differently, by excluding aggrieved parties' redress against the service provider involved, one thwarts their possibilities to obtain effective redress. That would occur despite the fact that the service providers are typically in a good position to terminate the violation of the aggrieved parties' rights and limit the negative consequences thereof. Indeed, their position as "*single point of control*" and their "*superior ability to avoid harm*"[47] is the main reason to involve them in efforts aimed at tackling illegal online content in the first place.[48]

17 The knowledge-based liability model thus aims to strike a middle-way. It avoids the negative consequences of stricter forms of liability that would impact not only the service providers themselves, but also their users. At the same time, it does not completely preclude the possibility for aggrieved parties to have recourse to the service provider concerned where their rights are at stake. Indeed, given that submitting a takedown notice typically requires relatively little effort and expense from aggrieved parties and may lead to swift results,[49]

43 US Supreme Court, *Smith v California*, 361 US 147 (1959), 153–154.

44 Ibid.

45 See Wilman (n 13), 121 (with further references).

46 See eg Kosseff (n 37), 221-222 ("*Given the uncertainty of the unmasking process, it is disingenuous to simply dismiss the harms suffered by plaintiffs [...] because they did not sue the [user providing the illegal online content concerned]*"); European Court of Human Rights (ECtHR), *Høiness v Norway*, Appl no 43624/14 (2019), 70 ("*Turning to the possibilities for the applicant to pursue claims against the anonymous individual or individuals who had written the comments, the Court sees no reason to contest the applicant's allegation that she would have faced considerable obstacles in attempting to do so*").

47 See, respectively, F Wu, 'Collateral censorship and the limits of intermediary immunity', (2011) *Notre Dame Law Review* 87, 314; J Balkin, 'Free speech and hostile environments', (1999) *Columbia Law Review* 99, 2302. See eg also M Rustad, and T Koening, 'Rebooting cybertort law', (2005) *Washington Law Review* 80, 390 (referring to online service providers as 'least-cost avoiders' of harm).

48 See eg Recital 2 Recommendation (EU) 2018/344 on measures to effectively tackle illegal online content, [2018] OJ L 63/50 ('Illegal Content Recommendation') ("*In the light of their central role and the technical means and capabilities associated with the services that they provide, online service providers have particular societal responsibilities to help tackle illegal content disseminated through the use of their services*"); Recital 59 Infosoc Directive (explaining the creation of the possibility to issue injunctions against online intermediaries by noting that they tend to be "*best placed to bring [...] infringing activities [by the users of their services] to an end*").

49 Cf K Wallberg, 'Notice and takedown of counterfeit goods in

the principle normally provides these parties with a realistic prospect of redress.

D. Developments in practice

18 There are obvious changes – especially in the online world – since laws such as the ECD in the EU and Sections 230 CDA and 512 DMCA in the US were adopted over two decades ago. That was a time when judges still felt the need to explain in judgments relating to online matters what the internet actually was.[50] Back then, internet users worldwide numbered in the tens of millions, not the billions of today.[51] It is true that some of the services involved already existed in embryonic form. Social networks can trace their origins to bulletin boards, for example. Nonetheless, such services are hardly comparable, both in terms of their key features and the manner in and extent to which they are used. Most of today's well-known service providers such as YouTube, Facebook, Twitter, Instagram and TikTok did not yet exist at the time. Bandwidth has also grown exponentially. That has greatly facilitated the possibilities to transmit user content, both of the legal and the illegal kind. The introduction of smart phones means that many people are almost continuously online.

19 While highly significant in many ways, in and of themselves, those changes tell us little about the continued relevance and suitability of the legal framework sketched above, however. In order to establish that, the following three points should be considered in particular.

20 To begin with, the quantities of content that some hosting service providers store for their users are nowadays larger than ever before. To illustrate the point: reportedly YouTube's over two billion monthly active users upload around 500 hours of video per minute and Twitter's 330 million monthly active users send around 500 million tweets a day.[52] In line with what was said above, these staggering numbers arguably reinforce the need for limiting the liability of the service providers to only user content that they know (or should know) to be illegal. However, there is also another noteworthy development: the typically increased ability of service providers to *obtain* knowledge of or control over the content that they store. The best-known example is probably YouTube's Content ID tool, which automatically checks uploaded user content and allows for the blocking of content that matches with copyright-protected works. YouTube is by no means alone in using such tools. Many large hosting service providers do so, not only in respect of copyright-infringing content but also of content depicting nudity, self-harm, terrorist content and hate speech, among other things.[53] As already touched upon above, they also tend to be increasingly active in relation to the user content stored, especially by improving accessibility and moderating the content. In addition, they apply increasingly sophisticated means that allow them to specifically target advertising as well as gather and process large amounts of data relating to their users. In this light, the commercial internet has said to have developed into "*the most surveilled zone of human activity in history*".[54] Although the proactive tackling of illegal user content certainly

the Digital Single Market: a balancing of fundamental rights', (2017) *Journal of Intellectual Property Law & Practice* 12, 933 (noting that the formal requirements imposed by hosting service providers are "*few and easy to satisfy*"). As to the speed of removals, as mentioned, Art 14(1) ECD is conditional upon hosting service providers removing notified illegal content "*expeditiously*". In practice, that often means removal within at most a few days. Cf Commission, Code of conduct on countering illegal hate speech online – fourth evaluation confirms that self-regulation works, 2019, 2 (indicating that service providers meet their commitment to remove illegal hate speech within 24 hours pursuant to the 2016 Code of Conduct on Countering Illegal Hate Speech Online in 89% of the cases); Commission, Report assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872, 9–10 (indicating that 93% of child sexual abuse material notified by hotlines in Europe is removed within 72 hours).

50 Eg US Supreme Court, *Reno v ACLU*, 521 US 844 (1997), 849-850.

51 Ibid, 850. In January 2021, the number of active internet users worldwide reportedly stood at over 4,66 billion. See <https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Almost%204.66%20billion%20people%20were,percent%20of%20total%20internet%20users>.

52 See <https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/#:~:text=As%20of%20May%202019%2C%20more,for%20online%20video%20has%20grown>; <https://www.brandwatch.com/blog/twitter-stats-and-statistics/>.

53 See Wilman (n 13), 255-256 (with further references).

54 D Keats Citron and N Richards, 'Four principles for digital expression (you won't believe #3!)', (2018) *Washington University Law Review* 95, 1375. See also D Keller, 'Who do you sue? State and platform hybrid power over online speech', Hoover Institution Essay Aegis Series Paper No. 1902, 2019, 1 ("*Facebook and other large internet companies can monitor every word users share and instantly delete everything they don't like. No communications medium in human history has ever worked this way*").

involves challenges,[55] the argument that services providers cannot reasonably be required to do more in this respect than 'just' reacting to notices (and, occasionally, injunctions) thus no longer seems entirely convincing.

21 What was said in the previous paragraph comes with an important qualifier, however, which is the second point to be noted. The foregoing may hold true for a comparatively limited number of large hosting services providers, which have very considerable technological, human and financial means at their disposal. However, it does not – or at least not to the same extent – hold true for many other, smaller hosting service providers. In the EU, there are estimated to be over 10,000 hosting service providers, 85% of which are either micro or small enterprises.[56] The rise of 'mega-platforms' such as Facebook and YouTube raises all kinds of concerns, including competition-related ones, which largely fall outside the scope of this article.[57] Nonetheless, it is a widely shared concern that imposing on hosting service providers increased obligations to tackle illegal user content would reinforce the position of the incumbents.[58] The latter generally have the means to take the necessary measures to meet such obligations, even if they involve considerable investments. YouTube's Content ID tool, for instance, costs an estimated total of 100 million USD to develop and operate,[59] whilst Facebook employs tens of thousands human content moderators.[60] Their smaller competitors, including new entrants and start-ups, may not have the means to meet such obligations. The pockets of the 'mega-platforms' may also be deep enough for them not to be overly fearful of damages claims for any illegal content that their users may upload. For many others, however, the decision not to remove potentially illegal content can boil down to 'betting the company'[61] – something that they are understandably not very inclined to do. Therefore, whilst the knowledge-based liability exemption may not solely be about protecting hosting service providers, many of them still need the protection afforded to them. The protection is arguably needed now even more than before if smaller providers are to stand a chance to compete with the large incumbents.

22 As a third point, the generally large – and sometimes enormous – quantities of user content stored illustrate how broadly hosting services are used for all kinds of economic, social, recreational, cultural and political purposes. Whether you want to buy or sell a second-hand product, listen to music, stay in touch with friends, rent a holiday home or check out consumer reviews before booking a restaurant – all of these activities will in many cases involve the use of hosting service providers. It has been said that, fundamentally, "*there is not a single online service or activity that does not involve the activity of one or more hosting service providers*".[62] The online sphere is also an important battlefield in any modern political campaign, just as the services at issue here are widely used for people to organise themselves for all kinds of other purposes, stay informed and exchange information. Many of these activities are of course perfectly legitimate and even socially beneficial. Yet, there is no denying that the services are also widely used for all kinds of illegal purposes. This is not new; the liability exemptions of the ECD and its US counterparts were drafted in part with the aim of combatting illegal activities conducted online.[63] Nonetheless, difficult as this may be to quantify, it seems safe to say that the scale of the problem has increased. In relation to child sexual abuse material it has been observed, for instance, that "*[t]echnology has generated a paradigm shift in both the victims' online exposure and the offenders' ability to*

55 For instance, relating to the accuracy of automated means used (particularly in context-sensitive situations) and the psychological toll for human content moderators.

56 Commission, Impact assessment DSA proposal, SWD(2020) 348, 24.

57 See in this regard in particular the DSA's 'sister act': Commission, Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Acts), COM(2020) 842.

58 See eg G Frosio and C Geiger, Taking fundamental rights seriously in the Digital Services Act's platform liability regime', 2020, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756>, 31 ("*Imposing new burdensome obligations on [online service providers] would decrease innovation by making it more expensive for new players to enter the market*"); A Bridy, 'Three notice failures in copyright law', (2016) *Boston University Law Review* 96, 791 ("*For large, well-capitalized providers like the Googles and Facebooks of the world, taking on extra enforcement burdens may not be onerous. For new entrants and smaller providers, however, those extra costs may be unbearable*"). See also AG Saugmandsgaard Øe, *YouTube* (n 29), 194.

59 A Bridy, 'The price of closing the "value gap": how the music industry hacked EU copyright reform', (2020) *Vanderbilt Journal of Entertainment and Technology Law* 22, 350.

60 M Zuckerberg, 'Blueprint for content governance and enforcement', 15 November 2018.

61 Urban et al (n 3), 43.

62 Van Hoboken et al (n 21), 11-12.

63 Cf Commission, Proposal ECD, COM(1998) 586, 4 (explaining that the aim is to establish a balanced regime "*in order to stimulate cooperation between different parties thereby reducing the risk of illegal activity online*").

share [such material] securely and interact anonymously with children and other offenders online".[64] The head of the EU Fundamental Rights Agency has called online hate speech "*a plague of our times*", adding that "*things are getting worse*".[65] A US judge observed that "*[r]ecent news reports suggest that many social media sites have been slow to remove the plethora of terrorist and extremist accounts populating their platforms, and that such efforts, when they occur, are often underinclusive*".[66]

23 In conclusion, whilst not unidirectional, the developments outlined above confirm and broadly reinforce the need for a 'middle way' approach like the one embodied in the knowledge-based liability model. In essence, that is because for all parties involved – and, by extension, for society as a whole – the stakes have increased. That goes for persons negatively affected by, for example, copyright infringement, defamation or privacy violations occurring online, in view of the broad reach of many of services in question and the internet's inability to 'forget'.[67] At the same time, the stakes for users who may be wrongly targeted by, or who may otherwise suffer adverse consequences of, service providers' measures to tackle illegal online content appear to have increased as well. For instance, having your account or the entire service provision suspended can significantly limit your ability to express yourself, obtain information or engage in social interactions and legitimate commercial activities online. Furthermore, if even some of your most intimate and sensitive communications take place online, it becomes all the more important that they remain private. As to the service providers themselves, whilst the relatively few large ones could reasonably be made subject to further-going requirements, it appears that for many others the current liability exemptions are as important today as they were two decades ago.

64 WeProtect Global Alliance, Threat Assessment Report 2018, 2018, 7.

65 M O'Flaherty, Director EU Agency for Fundamental Rights, 'Opening address at the roundtable on artificial intelligence and online hate speech', 31 January 2019.

66 Partially concurring and partially dissenting opinion Judge Katzmann, US Court of Appeals 2nd Circuit, *Force v Facebook*, 934 F3d 53 (2019), 84–85 (with further references).

67 See eg ECtHR, *Delfi v Estonia*, Appl no 64569/09 (2015), 110 ("*Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online*").

E. Developments in EU fundamental rights law

24 The continued and reinforced need for a 'middle way' approach in relation to the liability of online service providers for the user content that they store and often disseminate comes to the fore even more when another evolution, which is not factual but legal in nature, is taken into account. Namely, the rise of the fundamental rights dichotomy in the EU legal order. To be sure, fundamental rights-related concerns emerging in the present context are not new, either. The ECD highlights in its recitals the importance of the fundamental right to freedom of expression, for instance.[68] Yet it seems clear that, especially in the EU, the issue at stake is increasingly framed in terms of fundamental rights. A few examples include: rightsholders confronted with online copyright infringement are not merely suffering economic damage, but may have their fundamental right to protection of intellectual property violated;[69] persons affected by online defamation may act to protect not only their reputation, but also their fundamental right to a private and family life;[70] the dissemination of child sexual abuse material is not only problematic in and of itself, but can involve violations of several fundamental rights, notably the prohibition of inhumane and degrading treatment, the right to respect for private and family life, and the rights of the child;[71] requirements imposed on online service providers to tackle illegal user content are not merely burdensome, but can call into question their fundamental right to freedom to conduct a business;[72] and filtering and blocking measures taken by service providers can be not only

68 See in particular Recitals 9 and 46 ECD.

69 See eg CJEU, *McFadden*, C-484/14, ECLI:EU:C:2016:689, 81; CJEU, *UPC Telekabel*, C-314/12, ECLI:EU:C:2014:192, 47 (both referring to Art 17(2) Charter).

70 See eg ECtHR, *Delfi v Estonia* (n 67), 137 (referring to Art 8 of the European Convention of Human Rights (ECHR), which corresponds to Art 7 Charter).

71 See eg CJEU, *La Quadrature du Net*, C511/18, C512/18 and C520/18, ECLI:EU:C:2020:791, 128 (referring to Art 4 and 7 Charter); Commission, Proposal for a Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, COM(2020) 568, 4 (referring to Art 24 Charter).

72 See eg CJEU, *McFadden* (n 69), 88; CJEU, *Scarlet Extended v SABAM*, C-70/10, ECLI:EU:C:2011:771, 48 (both referring to Art 16 Charter).

annoying for their users, but may negatively affect their fundamental rights to privacy, protection of personal data and freedom of information.[73]

25 All this reflects in part the increased use and importance of the services in question, described earlier. However, it also reflects the fact that EU fundamental rights law itself has evolved significantly over the past two decades. To start, it was not until 2009 that the Charter of Fundamental Rights of the EU ('the Charter') became legally binding.[74] Although fundamental rights were already protected beforehand (as general principles of EU law), this development has undoubtedly increased the visibility and importance of fundamental rights protection in the EU. This results not only from their codification as such, but also from the fact that the Charter expressly recognises several relatively novel rights, such as protection of personal data, the freedom to conduct a business, protection of intellectual property and the rights of the child.[75] As indicated in the previous paragraph, these rights may well be at issue in cases arising in the present context.

26 Furthermore, the requirement to strike a 'fair balance' in situations where several conflicting fundamental rights are at stake is by now well established under the case law of the Court of Justice. As such, it constitutes a cornerstone of the EU fundamental rights regime. Yet the requirement was only first clearly articulated in 2008.[76] That is well after the adoption of the ECD. Tellingly, the ECD frames the issue in terms of balancing the conflicting *interests*.[77] It appears that, at the time, the EU legislator primarily had economic interests in mind, such as ensuring the affordability of access to online services and stimulating the development of electronic commerce.[78] Under said case law, these interests have since been 'upgraded' to conflicting *fundamental rights* that are to be balanced.

27 To this should be added the emerging – and still very much developing – case law of the Court of Justice on three other fundamental rights doctrines.[79] First, a main driver behind the developments in the US in this area is the risk that imposing liability for user content that online service providers intermediate may have a 'chilling effect' on freedom of expression.[80] This term refers to the indirect negative effect that such liability may have on the dissemination and reception of legitimate expressions online.[81] Without having expressly used the term thus far, the Court has acknowledged that such a chilling effect must be avoided also as a matter of EU fundamental rights law.[82] This reinforces the argument against imposing overly strict forms of liability on hosting service providers.

28 In addition, there is the doctrine on the 'horizontal direct effect' of the Charter.[83] This refers to the obligations on private parties to respect the rights enshrined in the Charter in their relationship with other private parties. To date, the Court of Justice has recognised such a horizontal direct effect only in respect to some of those rights,[84] whilst it is for now

73 CJEU, *GS Media*, C-160/15, ECLI:EU:C:2016:644, 31 and 45 (referring to Art 11 Charter); CJEU, *Scarlet Extended* (n 72), 51-52 (referring to Art 8 and 11 Charter).

74 The Charter became legally binding through the Treaty of Lisbon, which entered into force in December 2009. The Charter has the same legal value as the EU Treaties (Art 6(1) Treaty on European Union.

75 Art 8, 16, 17 and 24 Charter, respectively.

76 CJEU, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, 68.

77 Recital 41 ECD.

78 See AG Saugmandsgaard Øe, *YouTube* (n 29), 194; Commission, First report on the ECD, COM(2003) 702, 14 and 20.

79 Note that the doctrines referred to above are novel in as far as the Charter and the case law of the CJEU is concerned. The former ('chilling effects') and the latter doctrine (positive obligations) have both been extensively articulated in case law of the ECtHR. As regards the former, see eg T Baumbach, 'Chilling effect as a European Court of Human Rights' concept in media law cases', (2018) *Bergen Journal of Criminal Law and Criminal Justice* 6, 92–114. As regards the latter, see eg the case law cited in para 29 below.

80 See eg US Court of Appeals, *Zeran* (n 12), 331 ("*The specter of tort liability in an area of such prolific speech would have an obvious chilling effect*").

81 See further L Kendrick, 'Speech, intent and the chilling effect', (2013) *William & Mary Law Review* 54, 1633–1691; F Schauer, 'Fear, risk and the First Amendment: unravelling the chilling effect', (1978) *Boston University Law Review* 58, 685–732. See also para 15 above.

82 CJEU, *La Quadrature du Net* (n 71), 128; CJEU, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, 28 (both in the context of the retention of personal data). Cf A Kuczerawy, *Intermediary liability and freedom of expression in the EU: from concepts to safeguards* (Intersentia 2018), 160 (making a similar point). Some AGs have been more explicit: see in particular Opinion AG Cruz Villalón, *eDate Advertising*, C-509/09 and C-161/10, ECLI:EU:C:2011:192, 46.

83 See in particular CJEU, *Cresco Investigation*, C-193/17, ECLI:EU:C:2019:43; CJEU, *Bauer*, C-569/16 and C-570/16, ECLI:EU:C:2018:871; CJEU, *Egenberger*, C-414/16, ECLI:EU:C:2018:257.

84 See eg CJEU, *Association de médication sociale*, C-176/12,

uncertain what this entails concretely.[85] Those rights include, however, the prohibition of discrimination and the right to an effective remedy[86] – fundamental rights that may well be of relevance in the present context. The Court has also indicated that providers of certain online services themselves (as imposed to the public authorities concerned) are under certain circumstances to ensure the aforementioned fair balance between conflicting fundamental rights.[87] It is not inconceivable, therefore, that hosting service providers have certain obligations directly under EU fundamental rights law. Possible obligations could include being particularly attentive when it comes to racist and xenophobic expressions or ensuring that aggrieved parties can effectively address stored illegal content. Rather than making secondary law redundant, this development may well create uncertainty that is best addressed through adopting acts of secondary EU law that give concrete expression to any such obligations.

29 Lastly, the Court of Justice has acknowledged even more recently the existence of 'positive obligations' resulting from the Charter.[88] That means that relevant public authorities should not only ensure that they do not violate fundamental rights, but also take active steps to safeguard those rights. Again, this probably does not hold true for all Charter rights and it remains to be seen what this means in operational terms.[89] The implications for the present purposes could nonetheless be considerable. For instance, it has long been argued that to adequately protect the rights of all parties involved, the EU legislator should lay down binding rules on notice-and-action procedures.[90] Such arguments are (even) more convincing now that they can potentially rely on this recent line of case law. The case law of the European Court of Human Rights[91] suggests that one could, depending on the circumstances, also think of positive obligations to establish a legal framework through which: anonymous perpetrators can be identified and prosecuted;[92] infringements of intellectual property rights do not go unsanctioned;[93] and safeguards against abuse are provided for and access to a remedy before a court is ensured.[94]

30 In summary, the fundamental rights landscape has evolved quite drastically. The above jurisprudential developments are not specific to matters relating to the liability of hosting service providers. Nonetheless, they have important implications for the present purposes, especially since the issues emerging in this context so often involve the exercise of (conflicting) fundamental rights. More specifically, the increased emphasis on fundamental rights suggests that the EU legislator's discretion may be limited in several respects.[95] For one thing, its discretion *not*

EU:C:2014:2, 48 (indicating that Art 27 Charter does not have horizontal direct effect).

85 There is, for instance, the question as to precise consequences of any such horizontal direct effect, beyond the disapplication of incompatible rules of national law. In addition, see K. Lenaerts, President CJEU, speech at the conference 'Making the EU Charter of Fundamental Rights a reality for all: 10th anniversary of the Charter becoming legally binding', 12 November 2019 (suggesting that 'only' the essence of the relevant fundamental rights could work directly in relationships between private parties). In any event, the effects are limited to fields covered by EU law (see Art 51(1) Charter).

86 CJEU, *Egenberger* (n 83), 76 and 78 (relating to Art 21 and 47 Charter). See also CJEU, *Veselības ministrija*, C243/19, ECLI:EU:C:2020:872, 36 (regarding Art 21 Charter).

87 CJEU, *GC v CNIL*, C-136/17, ECLI:EU:C:2019:773, 75-76 (relating to the 'right to be forgotten' as established in EU law on the protection of personal data).

88 See in particular CJEU, *La Quadrature du Net* (n 71), 126 (referring to Art 3, 4 and 7 Charter).

89 Cf L Woods, 'Article 11', in S Peers, T Hervey, J Kenner and A Ward (eds), *The EU Charter of Fundamental Rights: a commentary*, Hart 2014, 311–339, 332 (referring to the "*uncertain realm of states' positive obligations*"). Cf also ECtHR, *Osman v UK*, Appl no 23452/94 (1998), 116 (pointing out that a positive obligation "*must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities*").

90 See (among many others) eg A Savin, *EU internet law* (Edward Elgar 2017), 153; A Kuczerawy, 'The power of positive thinking: intermediary liability and the effective enjoyment of the right to freedom of expression', (2017) *Journal of Intellectual Property, Information Technology Law and Electronic Commerce Law* 3, 237; Riordan (n 36), 384; Van Eecke (n 3), 1463; R Julià-Barceló, and K Koelman, 'Intermediary liability in the e-Commerce Directive: so far so good, but it is not enough', (2000) *Computer Law & Security Report* 16, 231.

91 The case law of the ECtHR on the ECHR can be of indirect yet significant importance in the EU legal order. See in particular Art 52(3) Charter (indicating that, in as far as Charter rights correspond to rights guaranteed under the ECHR, the meaning and scope of the former are the same as the latter).

92 ECtHR, *K.U. v Finland*, Appl no 2872/02 (2008), 48–49 (in the context of the protection of minors).

93 ECtHR, *Sunde v Sweden*, Appl no 40397/12 (2013), D (regarding the protection of copyright).

94 ECtHR, *Barbulescu v Romania*, Appl no 61496/08 (2017), 115, 120 and 122 (relating to a situation involving employers monitoring their employers' communications).

95 Cf also, more generally, CJEU, *Digital Rights Ireland* (n 82), 47–48 (indicating that in situations where fundamental rights play

to regulate relevant issues in any detail may have been reduced.[96] For another thing, especially in view of the requirement of fair balance, its discretion to opt for stricter forms of liability than knowledge-based liability might be limited too. That holds even more true when the case law of the European Court of Human Rights is taken into account. That case law suggests that a 'rigid', strict liability approach might not be feasible from a fundamental rights viewpoint, since it "*effectively precludes the balancing between the competing rights*".[97] In contrast, a knowledge-based (and, more specifically, a notice-based) liability model can "*function in many cases as an appropriate tool for balancing the rights and interests of all those involved*",[98] although the imposition of stricter requirements can be acceptable in certain cases.[99] It thus appears that the 'middle way' approach embodied in the knowledge-based liability model is generally well suited to achieve the fair balance that EU fundamental rights law requires.[100]

F. Effectively tackling illegal user content

31 None of the aforementioned arguments should be taken to mean that the knowledge-based liability model does not having certain shortcomings. The shortcomings fall into two broad categories. The first one relates to the objective of effectively tackling illegal user content. It has already been seen that this objective continues to be highly relevant, considering the broad use made of the services in question to store and spread illegal content of all kinds.

32 The current EU system of knowledge-based liability leaves room for improvement in this regard because, first of all, it is ultimately voluntary. Any hosting service provider is free, legally speaking, to ignore a notice received, no matter how manifest the notified illegality and how precise and well-substantiated the notice may be. To be sure, national notice-and-action schemes may impose certain procedural requirements and most service providers will generally not ignore such notices because it would deny them the benefit of the liability exemption of Article 14 ECD. However, rogue operators – which do not even feel the need to give the *appearance* of being bona fide economic actors – may have little incentive to act upon such notices, especially if they are established outside the EU. In fact, the ECD, and therefore also its Article 14, only applies to online service providers established in the EU.[101] Providers based in third countries therefore cannot benefit from the liability exemption, no matter how expeditiously they act upon the notices that they may receive. The fact that such providers are established outside the EU can also make it difficult in practice to apply and enforce national liability rules. Thus, the paradoxical effect is that under the current system hosting service providers that facilitate the most damaging and blatantly illegal conduct of their users may be the least incentivised to act against such conduct.[102]

33 Second, the EU system, like any system that mostly relies on notices for service providers to obtain knowledge of and act against illegal content, is inherently dependent on notifying parties. The system will therefore only function well if there are parties that are willing and able to first detect and then notify (alleged) illegal content to the hosting service providers that store it (and take judicial action if need be). For most content causing 'private' harm that will generally not be an insurmountable problem. The monetary, reputational or emotional harm inflicted by intellectual property right infringements, defamation or invasions of privacy, as examples, means that the persons concerned gen-

an important role and the interference with those rights is serious, the EU legislature's discretion is reduced and the judicial review of the exercise of the discretion by EU courts is strict).

96 This may result not only from uncertainty relating to horizontal direct effects and the positive obligations mentioned above, but also from the 'quality' of the law requirement applicable under Art 52(1) Charter, which means inter alia that laws limiting the exercise of fundamental rights must be formulated with sufficient precision. See eg CJEU, *Chodor*, C-528/15, ECLI:EU:C:2017:213, 38.

97 ECtHR, *Magyar Tartalomszolgáltatók Egyesülete (MTE) v Hungary*, Appl no 22947/13 (2016), 89. See also ECtHR, *Magyar Jeti v Hungary*, Appl no 11257/16 (2018), 83 ("*objective liability may have foreseeable negative consequences on the flow of information on the Internet, impelling article authors and publishers to refrain altogether from hyperlinking to material over whose changeable content they have no control. This may have, directly or indirectly, a chilling effect on freedom of expression on the Internet*").

98 Ibid, 91.

99 ECtHR, *Delfi v Estonia* (n 67) (relating to a situation involving manifestly illegal hate speech).

100 See further Frosio and Geiger (n 58).

101 Recital 58 ECD.

102 Cf Commission, Impact assessment proposal TCO Regulation, SWD(2018) 408, 6 (noting that a large part of the service providers storing terrorist content are established outside the EU). On the other hand, see Commission, EU strategy for a more effective fight against child sexual abuse, COM(2020) 607, 2 (referring to reports indicating that, globally, most child sexual abuse material is hosted in the EU).

erally have every interest in actively trying to have the content taken down. That is often different, however, for content causing 'public' harm – that is, illegal content that primarily affects certain groups or society as a whole, rather than specific individuals. Think of terrorist content, child sexual abuse material or certain forms of racist or xenophobic speech. Of course, under the EU system any user remains free to notify such content when he or she encounters it, and some users certainly do so. However, ordinary users will generally not make an elaborate effort to this effect and their notifications are not always very helpful.[103] Other parties have stepped in to try to close the resulting 'enforcement gap'. Think, for instance, of non-governmental organisations dedicated to tackling child sexual abuse material by notifying it to service providers. However, whilst the activities of such organisations are undoubtedly important, their means are often limited and not evenly distributed.[104] Europol and certain national law enforcement authorities essentially do the same thing in relation to terrorist content online. However, such activities are not uncontested and may not be sufficient.[105] All this means that some of the worst and most harmful types of illegal user content may not be tackled in a sufficiently effective manner.

34 Third, the type of redress available in the context of the notice-and-action system for which the knowledge-based liability exemption provides the basis is limited to the removal of (or the disabling of access to) illegal user content. Removal is obviously helpful in addressing the immediate problem. However, in practice, the content in question may already have been spread further, or the same or other users may simply re-upload the removed content.[106] That naturally reduces the practical effectiveness of the removal. As the ECD stands, hosting service providers are not legally incentivised – let alone obliged – to try to prevent such further spreading or re-uploading of illegal content from happening. In other words, there is no 'notice-and-*stay*down' mechanism. More generally, the system established by the ECD does not encourage or oblige hosting service providers to make any structured effort to address the problem of illegal content provided by their users.[107] At EU level no provision has been made either for measures aiming to hold users who provide illegal content accountable, such as rules requiring hosting service providers to provide, upon justified requests, information about those users, or to bar those users from using their services.[108] The current EU system is, one could say, purely focused on combatting the symptoms (illegal content) rather than addressing those at the root of the problem (users providing illegal content).

35 In many ways, the shortcomings outlined above are related to the knowledge-based liability system's origin and nature. As pointed out earlier, the EU system was inspired by the US system laid down in Section 512(c) DMCA. The First Amendment to the US Constitution leaves the US legislature relatively little scope to regulate speech-related matters. This is one of the reasons why when enacting the DMCA, the US legislature decided to *encourage* but not legally *require* the tackling of illegal content, by offering the services providers concerned that meet certain conditions a 'safe harbour' (namely, the liability exemption).[109] From a European viewpoint,

103 See eg Internet Watch Foundation, Annual Report 2018, 2019, 18 (stating that only 28% of reports about alleged child sexual abuse material were accurate); T Wischmeyer, 'Making social media an instrument of democracy', (2019) *European Law Journal* 25, 176 (noting that, in the first six months of 2018, large hosting service providers found only between 11 and 27% of users' complaints submitted under the German NetzDG (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*; Network Enforcement Act) justified).

104 See Wilman (n 13), 280-281 (with further references).

105 As regards the activities not being sufficient, see Commission, Impact assessment proposal TCO Regulation, SWD(2018) 408, 12-13. The activities are not uncontested because some consider it inappropriate for public authorities to use the notice-and-action mechanism, in particular where user content is notified for alleged violations of the providers' terms and conditions rather than alleged violations of the applicable law. Cf European Parliament, Legislative resolution on the proposal for a Regulation on preventing the dissemination of terrorist content online, P8_TA(2019)0421 (suggesting deleting the parts of the Commission proposal for the TCO Regulation intended to facilitate the submission and processing of these particular kinds of notices, known as 'referrals').

106 Cf CJEU, *Facebook Ireland* (n 20), 36 ("*Given that a social network facilitates the swift flow of information stored by the host provider between its different users, there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network*").

107 See also para 46 below (explaining that the argument is sometimes made that the current EU system does, in fact, the very opposite - that is, *dis*couraging such efforts, in view of the risk that hosting service providers undertaking such voluntary activities might be deemed 'too active' to be able to benefit from the liability exemption).

108 Cf Art 15(2) ECD (indicating that the matter is essentially left to each Member State).

109 M Sag, 'Internet safe harbors and the transformation of copyright law', (2018) *Notre Dame Law Review* 93, 513; W Seltzer, 'Free speech unmoored in copyright's safe harbor: chilling effects of the DMCA on the First Amendment, (2010) *Harvard Journal of Law & Technology* 24, 176. Something similar applies in respect of Section 230 CDA; see Kosseff (n 37), 74.

this is a somewhat unusual legislative technique. Normally, the EU legislator lays down certain legal requirements which are then enforced principally under the administrative (or criminal) law of the Member States.[110] In addition, as also noted earlier, the DMCA is focused solely on copyright-infringing content. Copyright is principally an 'individual' right. It is, moreover, a right that can represent a considerable monetary value. That means that a 'supply' of notifying parties (and, by extension, parties that may bring actions for injunctions or damages if their notices are not acted upon) is virtually ensured. As has been seen, that cannot be taken for granted in relation to other types of illegal content that the EU system – unlike the DMCA – also covers, especially not where it concerns illegal content causing 'public' harm.

36 More fundamentally, the notice-and-action model is meant as a sort of 'first aid':[111] a quick, inexpensive and uncomplicated (as compared to judicial proceedings) way of getting rid of illegal user content. In many respects the model achieves that objective fairly well.[112] As noted earlier, submitting a notice is generally easy and inexpensive, and it can lead to swift removal. However, precisely because of the emphasis on informality, affordability and speed – and most of all the absence of a truly objective and impartial arbiter – the type of redress available is limited. That holds true especially for the current EU system, which is purely focused on removal. The DMCA, in contrast, provides for complementary requirements, including for the service providers concerned to disclose information on users allegedly involved in unlawful activities upon request and to operate a repeat infringer policy.[113] Experience in the US shows that the imposition of such requirements in the context of a system of simplified and 'privatised' enforcement tend to raise complex questions, both of principle and practical implementation.[114] This is unlikely to be different in the EU. Think of challenges in terms of ensuring compliance with the requirements resulting from the Charter and from secondary EU law, such as the General Data Protection Regulation[115] (GDPR) and the prohibition of general monitoring or active fact-finding obligations of the ECD.[116] While important to ensure that illegal content is effectively tackled, it is doubtful whether other remedies should be provided for systems such as the ones at issue here. Arguably, such complex questions cannot be properly dealt with by means of 'first aid', but rather call for the involvement of a specialist – that is, a court or an independent administrative authority.

G. Protecting users' rights and interests

37 The second category of shortcomings of the EU's current knowledge-based liability system consists of the risks it creates for the rights and interests of the users of hosting services. The risks referred to here relate not to the dissemination of illegal content, but rather to the measures that hosting service providers may take to tackle such content. The 'bias towards takedown'[117] that is inherent in any system of this kind is of particular importance in this regard. The bias results from the unequal incentives for service providers when they have to decide whether or not to remove user content when its legality has been called into question. As touched upon earlier, the decision *not* to remove such content can have serious legal consequences. Most notably, it may lead to damages claims, but potentially also liability under criminal law. The decision to *remove* the content in question, by contrast, tends to have only limited consequences for hosting service providers. The legal risks relating to such a decision are generally limited. That is because the monetary value at stake will often be modest. The users concerned are therefore unlikely to sue and, even if they do, they might struggle to prove that they suffered serious

110 That does not mean, of course, that under EU law there is no scope to claim damages for violations of that law. The point is rather that damages claims are generally not the *principal* enforcement mechanism.

111 S Bar-Ziv and N Elki-Koren, 'Behind the scenes of online copyright enforcement: empirical evidence on notice & takedown', (2017) *Connecticut Law Review* 50, 383.

112 See eg Kuczerawy, 'The power of positive thinking' (n 90), 228–229 (stating that notice-and-action systems provide relief "*far quicker than the relief typically provided by the judiciary*"); Riordan (n 36), 64 (observing that notice-and-action systems tend to be effective, cheap and rapid).

113 See Section 512(h) and (i) DMCA, respectively.

114 See Wilman (n 13), 140-141 and 150-152, respectively (explaining that the above requirements raise, among other things, critical questions as to the possibility to address the matters without the involvement of a court as well as the many uncertainties left by the relevant provisions of US law).

115 Regulation (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, [2016] OJ L 119/1 ('GDPR').

116 Art 15(1) ECD.

117 Urban et al (n 3), 126.

and quantifiable damage. In addition, hosting service providers tend to contractually limit or exclude their liability towards their users for these kinds of decisions.[118]

38 It is true that non-legal considerations should also be taken into account. Removal decisions that are unjustified (or *perceived* as unjustified) can result in angry users and negative publicity, for example. The latter seems an especially relevant consideration for many hosting service providers. This could make them hesitant to remove user content. Nonetheless, such considerations are counter-balanced by certain other non-legal factors. Think of negative publicity that may result from the decision not to remove contested content, the 'stickiness' of many of the services in question (resulting from the effort involved in migrating to another service), the network effects benefitting many of the service providers and the lack of transparency as to their content removal policies and decisions. The chances of users leaving on a significant scale over contested content removal decisions may therefore be rather limited. In view of the often large quantities of user content stored, the attractiveness and profitability of hosting services is generally unlikely to suffer too much from the removal of a few – or even quite a few – individual items of allegedly illegal user content.[119]

39 Furthermore, other than in cases of manifest illegality, hosting service providers may well struggle when seeking to determine the legality of specific items of user content that they store. To be able to do so, one generally needs to know the relevant *factual* context. For example, whether a certain allegation is true (in cases of possible defamation), or whether certain material is disseminated with the consent of the persons involved (in cases of possible violations of privacy or intellectual property rights). This can be hard for the providers to determine. Moreover, the *legal* assessment is often not straightforward either. For example, it can be challenging to determine whether a given item of user content not just reports on certain terrorist activities but glorifies them, or whether a statement is not just offensive or ironic but instead constitutes a prohibited racial slur. Extra complexity is added by the fact that the laws of the Member States still tend to differ considerably despite being harmonised in some fields and to some extent.[120] Even determining which law applies in the first place may not be straightforward in the online sphere. Working all this out tends to be complex and (therefore) costly for service providers. It is often not only legally safer, but also easier and cheaper for them simply to remove user content that could, potentially, be illegal.

40 Thus, hosting service providers may well decide to remove the user content in question, especially in 'grey area' cases – of which there are many in practice. That means that it is unavoidable that user content that is *not* actually illegal is removed as well. This naturally has a negative effect on users' possibilities to lawfully express themselves and gather information online. In this connection, it should be recalled that a system relying on the submission of notices offers aggrieved parties a low-threshold manner to enforce their rights. The threshold is so low, in fact, that risks of mistakes and abuse exist. While hard to assess and quantify (largely due to the lack of transparency), research conducted in the US indicates that these risks are real and should be taken seriously.[121] Some unjustified removals result from honest mistakes, which may be hard to avoid. Yet, it appears that grossly erroneous or outright abusive notices, for instance to supress criticism or disadvantage competitors, are not uncommon.

118 Ibid, 16. See also Sag (n 109), 535.

119 Cf E Goldman, 'Why Section 230 is better than the First Amendment', (2019) *Notre Dame Law Review* 95, 41 (noting that online service providers rarely make a lot of money from any single item of user content); Balkin, 'Free speech is a triangle' (n 12), 2017 (noting that denying access to small numbers of speakers does not damage the providers' business model).

120 That relates not only to secondary EU law, but also eg the freedom of expression. See CJEU, *Google v CNIL*, C-507/17, ECLI:EU:C:2019:772, 67.

121 See also Urban et al (n 3) (reporting on two studies finding that 31 respectively 70% of the takedown notices assessed raised substantive questions; whilst also noting that nearly every intermediary and several copyright holders interviewed expressed concern about the takedown of non-infringing content); D Seng, 'Who watches the watchmen? An empirical analysis of errors in DMCA takedown notices', 2015, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2563202> (finding error rates of up to 8,3% in relation to 'functional' requirements, such as adequately specifying a takedown request, while also finding misidentification of the copyright holder and requests to remove content which is no longer available); J Urban and L Quilter, 'Efficient process or chilling effects: takedown notices under Section 512 of the Digital Millennium Copyright Act', (2006) *Santa Clara High Technology Law Journal* 22, 621–693 (finding that at least a third of the assessed takedown notices contained major flaws, notably as regards the underlying claims). See also Bar-Ziv and Elki-Koren (n 111), 344 (regarding the use of the notice and takedown procedure in accordance with Section 512 DMCA in Israel, finding that the procedure offers "*fertile ground for misuse*").

41 There are of course certain relevant differences between the legal systems in the EU and the US. For example, unlike in the US, punitive or statutory damages are not commonly provided for in the EU. That means that the financial risks associated with a provider's decision not to remove user content – in view of the risk of damages claims – may be more limited. On the other hand, in the EU it is in principle possible for *anyone* to submit a notice that might lead to knowledge on the side of the hosting service provider.[122] In the US, this possibility is reserved for what will generally be more or less professionally operating actors (namely, copyright holders), who are legally required to state their good faith belief that the use of the content in question is not authorised.[123] Furthermore, the fact that, unlike in the US, there are at present no binding EU rules on notice-and-action procedures enlarges the uncertainty and thus the 'grey area' referred to above, in which service providers may well remove allegedly-yet-not-manifestly illegal content just to be on the safe side. As importantly, the absence of such EU rules on notice-and-action procedures means that the availability of the principal safeguard of the US system to protect users' rights and interests – the so-called counter-notice procedure[124] – is not legally guaranteed. Such counter-notice procedures allow affected users to contest the claims of infringement made in relation to the content that they provided. It is true that the US counter-notice procedure is little used in practice.[125] That is likely due in part to the design of the procedure.[126] In any event, this fact does not alter the principal point that it is important to afford users a realistic opportunity to defend their interests if not before, then at least immediately after the removal of their content.

42 In addition, it has increasingly become clear over the past years that risks to the rights and interests of users also result from the content moderation measures that hosting service providers take to tackle content that may not be *illegal*, but that is against their *terms of service*. Providers' terms and conditions are often stricter than the law.[127] They may preclude, for instance, the provision of content containing nudity, offensive expressions or controversial political views. The decisions by Facebook and Twitter to suspend (then) President Trump's account, referred to earlier, illustrate both how powerful some of these providers are and how controversial their decisions can be.[128] In principle, providers are free to set and enforce such contractual rules, even in respect of content that may be perfectly legal, as an exercise of their freedom of contract that is part of the freedom to conduct a business.[129] Nonetheless, this development implies that the challenge is not only to ensure that 'what is illegal offline is also illegal online', as the adage has long been.[130] The challenge is also, and increasingly, to ensure that, conversely, what is *not* illegal offline is not 'illegal' (contractually prohibited) online either. Not, at least, where the contractual prohibitions unduly restrict users' freedom of expression and information or where the manners in which those prohibitions are enforced are arbitrary, excessive or not transparent.

122 Considering the 'horizontal' nature of Art 14 ECD and the fact that neither this article nor the case law relating thereto available to date contains any restriction in this respect.

123 Section 512(c)(3)(A) DMCA.

124 Section 512(g)(2) DMCA.

125 See ICF, Grimaldi and 21c Consultancy, 'Overview of the legal framework of notice-and-action procedures in Member States', Study for the Commission, 2018, 119 (reporting on 'counter-notice rates' – that is, the percentage of removals that lead to counter-notices – of often less than 1%, although for some online service providers the rate can be over 10%). See also Sag (n 109), 504 and 535; E Asp, 'Section 512 of the Digital Millennium Copyright Act: user experience and user frustration', (2018) *Iowa Law Review* 103, 770–773; Urban et al (n 3), 44 and 118 (all pointing to the limited use made of the DMCA's counter-notice procedure).

126 Wilman (n 13), 160.

127 See J Balkin, 'Free speech in the Algorithmic Society: big data, private governance and new school speech regulation', (2018) *University of California, Davis* 51, 1194–1195 ("*Online communities enforce speech norms that protect far less expression than the corresponding obligations of government under the American First Amendment*"); D Keller, 'Internet platforms: observations on speech, danger, and money', Hoover Institution Essay Aegis Series Paper No. 1807, 2018, 4 ("*Most well-known platforms take down considerably more content than the law requires*"); Gillespie (n 37), 34 ("*In most cases [online service providers'] ceaseless and systematic policing cuts much, much deeper than the law requires*").

128 See para 1 above. Note that the question whether President Trump acted illegally seems only of secondary importance in the context of this discussion; the reason for taking the suspension decisions was that he violated the providers' (broadly drawn) terms of service.

129 Cf CJEU, *Sky Österreich*, C-283/11, ECLI:EU:C:2013:28, 42–43.

130 Eg Commission, Tackling illegal content online: towards an enhanced responsibility of online platforms, COM(2017) 555, 2.

H. DSA proposal

I. Liability regime

43 The Commission's decision to retain, in the DSA proposal, the knowledge-based liability model for hosting services providers seems understandable in view of the foregoing, even if the reasons for doing so may perhaps not have been very well explained. Indeed, as noted, from a legal viewpoint the Commission arguably had little scope to opt for a fundamentally different approach.[131] This has to do, in particular, with the suitability of this model to achieve the required fair balance between conflicting fundamental rights. More specifically, the need to avoid 'chilling effects' on users' freedom of expression appears to have also played a role in the Commission's decision-making.[132] Considering the EU legislator's seemingly reduced discretion *not* to act in situations where fundamental rights may be infringed, the DSA proposal could be seen as reflecting not only a political and policy choice to act, but to some extent also a legal imperative to do so under EU fundamental rights law. In any event, it is noticeable that whilst the ECD only makes a few mentions of fundamental rights in its recitals, the protection thereof has been 'upgraded' to the very objective of the DSA proposal.[133] In line with that objective, the relevant fundamental rights are not only concretised in numerous specific legal obligations for hosting services providers and corresponding rights for users; in certain cases the proposal also requires the providers to take fundamental rights as such into account.[134]

44 The decision to retain the knowledge-based liability model is certainly not a purely legal one, though. The broad support for the key features (although not necessarily all specific aspects) of the current model is likely to have played a role, too. Such support is evident, for instance, from the public consultation,[135] academic studies[136] and the position taken by the European Parliament shortly before the publication of the DSA proposal.[137] The fact that the existing liability exemption would be 'transplanted' from the ECD to the new DSA Regulation could help address one of the main points of criticism: the diverging ways in which the current rules are understood and applied across the EU. Unlike directives, regulations do not require transposition into national law but instead apply directly and in the same way across the entire EU.

45 When zooming in on Article 5 DSA proposal, which is to replace current Article 14 ECD, it becomes apparent that in this respect the proposal seeks to change relatively little. The former is largely a copy of the latter. Drafting changes are limited and can mostly be explained by the fact that the DSA is a regulation, not a directive. Even the corresponding recitals of the DSA proposal echo those of the ECD to some extent, although they also provide certain clarifications. While helpful, these clarifications are hardly spectacular. The relevant recitals of the DSA proposal mostly recall case law of the Court of Justice relating to the current law or address

131 See section E above (on relevant developments in EU fundamental rights law).

132 See Commission, Explanatory memorandum DSA proposal, COM(2020) 825, 12; Commission, Impact assessment DSA proposal, SWD(2020) 348, 19.

133 Art 1(2) DSA proposal.

134 See Art 12(2) (requiring hosting service providers to take due account of the fundamental rights of users when applying the restrictions contained in their terms and conditions) and Art 26(1)(b) DSA proposal (requiring certain very large hosting service providers to assess significant systematic risks relating to their service provision inter alia for the exercise of certain fundamental rights). As such, the DSA proposal can be seen as a further step in the process of 'horizontalisation' of EU fundamental rights law, be it that the horizontal effects stem not directly from the Charter but rather arise via secondary EU law.

135 Commission, Impact assessment DSA proposal, SWD(2020) 348, 26 ("*On the topic of the liability of intermediaries, a large majority of stakeholder groups broadly considered the principle of the conditional exemption from liability as a precondition for a fair balance between protecting fundamental rights online and preserving the ability of newcomers to innovate and scale*").

136 See eg Frosio and Geiger (n 58), 4 (arguing that, despite shortcomings, the ex post knowledge-and-takedown mechanism of the ECD remains fully justified and pertinent from a fundamental rights perspective); A De Streel and M Husovec, 'The e-Commerce Directive as the cornerstone of the internal market: assessment and options for reform', Study for the IMCO Committee of the European Parliament, 2020, 47 (arguing that, given its success, the liability exemption of Art 14 ECD should be preserved); J Nordemann, 'The functioning of the internal market for digital services: responsibilities and duties of care of providers of digital services', Study for the IMCO Committee of the European Parliament, 2020, 46 (arguing that, despite being almost 20 years old, Art 14 ECD does not seem outdated); Urban et al (n 3), 28 (answering the question whether the notice-and-action model is still relevant in view of the many changes over the past two decades with "*a resounding 'yes'*").

137 See eg European Parliament, Resolution on the Digital Services Act: improving the functioning of the single market, 20 October 2020, P9_TA(2020)0272, 57 (calling maintaining the liability regime of Art 14 ECD "*pivotal*").

relatively uncontroversial matters.[138] However, on the following three main points the DSA proposal would mark a more substantial change as compared to the current liability system applicable to hosting services set out in the ECD.

46 The first change, which consists of several elements, has to do with the scope of the proposed new regime. To begin with, the DSA, and therefore also the liability exemption contained in its Article 5, would apply to *all* providers that offer relevant services in the EU.[139] That means that the question whether the providers are based inside or outside the EU would no longer be relevant.[140] That is a logical yet important change, which, besides contributing to a level playing field, should help better protect EU users against illegal content.[141] In addition, the DSA proposal's recitals state that the liability exemption does not apply to hosting service providers that play an active role of such a kind as to give them knowledge of or control of the content that they store for their users.[142] This is a restatement of existing case law and thus not a substantial change.[143] It is important nonetheless, since the degree to which such providers can play an active role without losing the benefit of the liability exemption is an issue that has led to confusion and debate.[144] Retaining and codifying (although only in a recital) the standard developed by the Court of Justice improves clarity and implies that the clarifications resulting from over a decade worth of case law on the matter are retained. However, it also means that some uncertainty remains, especially when it comes to the *application* of the standard in specific cases.[145] Yet another (although related) element is the introduction of a so-called 'Good Samaritan' clause. The clause is meant to address concerns that EU law as it stands discourages hosting service providers from undertaking voluntary activities to tackle illegal content, because doing so could mean that they are seen as 'too active' to qualify for the liability exemption.[146] The clause indicates essentially that no such conclusion is to be drawn.[147] This proposed new rule is hardly surprising given that it is in line with earlier guidance provided by the Commission,[148] although opinions on the need for introducing it differ and some might find the protection that the rule would afford still insufficient.[149]

138 Eg, Recitals 17, 18, 19 and 22 DSA proposal state that the present rules are about exemption from liability and not about liability itself: that the liability exemption is 'horizontal' in nature; that it does not apply in respect of liability relating to the providers' own content; that the rules are activity-based and not provider-based; and that service providers can obtain knowledge of illegality in particular through own-initiative investigations and third-party notices. As regards the situation under current law, including references to the relevant case law, see section B above.

139 Art 1(3) DSA proposal. See also Art 2(d) thereof (defining the term 'offering services in the Union').

140 It is only relevant in relation to Art 11 DSA proposal (requiring providers based in third countries to designate legal representatives within the EU to facilitate enforcement).

141 Recital 7 DSA proposal.

142 Recital 18 DSA proposal.

143 See in particular CJEU, *L'Oréal v eBay* (n 19), 113. See further para 7 above.

144 See eg Commission, Impact assessment DSA proposal, SWD(2020) 348, 31 (pointing to diverging national case law); European Parliament Research Service, 'Reform of the EU liability regime for online intermediaries', 2020, 5 (arguing that the Court of Justice's current case law lacks clarity); Van Hoboken et al (n. 21), 33 (referring to confusion and complexity relating to the scope of Art 14 ECD's liability exemption).

145 See para 8 above.

146 See Commission, Impact assessment DSA proposal, SWD(2020) 348, 33. See further also J Barata, 'Positive intent protections: incorporating a Good Samaritan principle in the EU Digital Services Act', 2020, available via <https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf>, 12.

147 Art 6 DSA proposal. Recital 25 indicates that the voluntary activities must have been undertaken in good faith and in a diligent manner. Note that Art 6 differs from the 'Good Samaritan' protection afforded under Section 230(c)(2)(A) CDA especially in that the article does not entail a liability exemption in its own right, covers only activities aimed at tackling *illegal* user content and covers not only voluntary but also *legally required* activities of that kind.

148 See in particular Recital 26 Illegal Content Recommendation. Cf CJEU, *YouTube* (n. 20), 109.

149 See eg C Angelopoulos, 'On online platforms and the Commission's new proposal for a Directive on Copyright in the Digital Single Market', 2017, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2947800>, 43–44; Nordemann (n 132), 10 (arguing in favour respectively against introducing such a clause). See eg also Van Hoboken et al (n 21), 42 (arguing in relation to the Commission's earlier guidance that the approach does not protect providers against liability in case they failed to detect and remove content despite having taken certain voluntary measures to that end); S Stalla-Bourdillon, 'Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well', in M Taddeo and L Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2017), 290 (arguing that not an express 'Good Samaritan' clause is required, but rather a clause protecting intermediaries where they in good faith refuse to takedown user content).

47 The second change is the proposed express disapplication of the notice-based liability exemption for hosting service providers in certain circumstances involving claims based on consumer protection law. The new rule, contained in Article 5(3) DSA proposal, would apply only to a particular subcategory of hosting service providers: online platforms allowing consumers to conclude distance contracts with traders.[150] Under the rule it is not so much the latter's (objective) knowledge of or control over the user content in question that is decisive, as is the case under the 'ordinary' liability exemption of Article 5(1). It is rather the (subjective) impression of the consumer as to whether the content (or the 'underlying' product or service to which the content relates) is provided by the service provider that is decisive for the question whether the liability exemption can be relied on.[151] The rule aims to improve the protection of consumers when they engage in intermediated commercial transactions online.[152] Whilst certainly novel when considered from the viewpoint of the current liability system, it brings to mind case law of the Court of Justice issued in the context of EU consumer protection law.[153] Although some may fear that the proposed rule could undercut the certainty that the conditional liability exemption is meant to provide, others may feel it does not go far enough in better protecting consumers.[154]

48 The third change consists of the introduction of EU rules on notice-and-action mechanisms. As noted earlier, the ECD provides the basis for a system of notice and action. But when adopting this directive the EU legislator decided to leave it to self-regulation to work out the procedural arrangements on the sending and processing of notices, whilst allowing Member States to set national rules on these matters.[155] Such self-regulatory and national rules have been established only to a limited extent, however, and where they exist, they diverge.[156] Article 14 DSA proposal would require hosting service providers to establish mechanisms that allow individuals or entities to notify them about allegedly illegal content. The mechanisms would have to be easy to access, user-friendly and allow for the submission of notices exclusively by electronic means. Importantly, the notices are to relate to *specific* items of content – broad, general notices could therefore not be submitted under these mechanisms.[157] Article 14 incorporates the standard set by the Court of Justice that notices should be sufficiently precise and adequately substantiated for them to be able to give rise to knowledge within the meaning of the liability exemption.[158] The article goes into further detail by listing the elements that notices should contain, including the reasons why the notifier thinks the content is illegal, its name and

150 Cf Art 2(h) DSA proposal (defining the concept of 'online platform' essentially as a hosting service provider which not only stores but also stores user content). Cf also Art 2(j) DSA proposal (defining the term 'distance contract'). In practice, one should probably mainly think of e-commerce platforms.

151 Although the test under Art 5(3) DSA proposal is objectivised, in the sense that the belief of an average and reasonably well-informed consumer is decisive. See also Recital 23. Pursuant to Art 5(3), the consumer's belief must, moreover, be based on the acts or omissions of the service provider, such as the manner in which it presents the content in question.

152 Recital 23 DSA proposal.

153 See in particular CJEU, Case C-149/15, *Wathelet*, ECLI:EU:C:2016:840, 41. For a suggestion somewhat similar to Art 5(3) DSA proposal, see De Streel and Husovec (n 132), 48.

154 See eg C Busch, 'Rethinking product liability rules for online marketplaces: a comparative perspective', 2021, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784466>, 27 (criticising the DSA proposal for not taking a clear stance on whether and when online marketplaces are subject to product liability); C Cauffman and C Goanta, 'A new order: the Digital Services Act and consumer protection', 2021, available via <https://www.researchgate.net/publication/348787835_A_New_Order_The_Digital_Services_Act_and_Consumer_Protection>, 9 (questioning whether Art 5(3) DSA proposal would offer consumers sufficient protection).

155 See in particular Art 14(3) and 16 DSA proposal. See also Commission, First report on the ECD, COM(2003) 702, 14; E Crabit, 'La directive sur le commerce électronique: le projet "Méditerranée"', (2000) *Revue du droit de l'Union européenne* 4, 814; Commission, Proposal ECD, COM(1998) 586, 29. In 2018, the EU legislator inserted a (rather rudimentary) requirement of this kind in Art 28b(3)(d) 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, [2010] OJ L 95/1 (as amended by Directive (EU) 2019/1808) ('AVMSD').

156 Commission, Impact assessment DSA proposal, SWD(2020) 348, 31-32 (and Annex 6 thereto). See also Wilman (n 13), 48.

157 See also Recital 40 DSA proposal (indicating that it should be possible to notify *multiple* specific items of allegedly illegal user content). Cf CJEU, *YouTube* (n. 20), 112-113.

158 Art 14(2) and (3) DSA proposal. See CJEU, *L'Oréal v eBay* (n 19), 122 (implying that insufficiently precise or inadequately substantiated notices do not lead to knowledge within the meaning of Art 14 ECD). See also CJEU, *YouTube* (n. 20), 116 (adding that notices must contain sufficient information to enable the service provider to satisfy itself, without a detailed legal examination, that the content in question is illegal and that removing that content is compatible with freedom of expression).

e-mail address and a confirmation of its good faith belief that the notice is accurate and complete.[159] Service providers are to process notices in a timely, diligent and objective manner.[160] Article 14 does not establish a counter-notice procedure; the matter is covered by other provisions of the DSA proposal, notably those on the provision of information to users in case of removal and on providers' internal complaint-handling systems.[161] The proposed new rules on notice-and-action mechanisms should contribute to the aim of tackling illegal content more effectively, whilst also better protecting users against unjustified removals.[162] The rules are broadly in line with the guidance contained in the Commission's Illegal Content Recommendation of 2018. Most will probably welcome them.[163] That does not mean, however, that there is no scope left for debate. Opinions could differ, for instance, as to whether the right balance is struck between, on the one hand, ensuring that notices are precise and substantiated enough to be actionable and that abuses of the mechanisms are prevented and, on the other hand, not deterring 'ordinary' users from using the mechanism by imposing overly demanding or 'threatening' requirements.[164] Another question is whether notices that do not contain all elements listed in Article 14 could in certain cases still lead to knowledge within the meaning of Article 5.

II. Effectively tackling illegal user content

49 In light of the above discussion regarding the shortcomings of a knowledge-based liability model, the question arises of how, beyond liability-related matters strictly speaking, the DSA proposal should be assessed. When it comes to measures aimed at tackling illegal user content more effectively, what is *not* proposed is perhaps most noticeable. In particular, whilst the DSA proposal retains the prohibition on general monitoring obligations,[165] it contains no general requirement for hosting service providers to detect and tackle illegal user content on their services in a proactive manner. The latter is an important change as compared to certain other measures recently proposed and adopted in this domain. Most notably, Article 17 Copyright in the Digital Single Market (CDSM) Directive,[166] the Commission's proposal for the Terrorist Content Online (TCO) Regulation[167] and the Illegal Content Recommendation[168] all contain provisions on proactive measures. It is further noticeable that the DSA proposal does not contain any rules that would empower national courts or administrative authorities to issue injunctions involving measures

159 Art 14(3) DSA proposal. Strictly speaking, the provision does not state that notices *must contain* such elements; rather, it states that service providers are to *facilitate* the submission of notices containing such elements. This reflects the fact that the provision imposes obligations on the providers, not on the notifying parties.

160 Art 14(6) DSA proposal. This requirement comes on top of, and appears to apply independently from, the 'expeditious action' condition set as part of the liability exemption of Article 5. Notices submitted by 'trusted flaggers' – such as the aforementioned organisations combatting child sexual abuse or Europol – are, moreover, to be treated with priority (Art 19 and Recital 46 DSA proposal).

161 Art 15 and 17 DSA proposal, respectively. See also para 55 below (discussing redress-related provisions of the DSA proposal). This approach implies that, unlike under Section 512(g) DMCA, the counter-notice procedure is not crafted as a condition attached to a separate liability exemption for removal decisions that turn out to be unjustified.

162 As explained in para 41 above, the latter results especially from the reduction of uncertainty on the side of the service providers ('grey area') and from the strengthened redress possibilities of affected users.

163 Given the many calls made over the years for introducing EU rules on notice-and-action procedures (see n 90). See also European Parliament (n 133), 52 (calling for harmonised rules on notice-and-action mechanisms); Commission, Impact assessment DSA proposal, SWD(2020) 348, 42 (noting that, in response to the public consultation, the general public, online intermediaries and civil society organisations especially advocated for a harmonisation of notice-and-action procedures across the EU).

164 In this regard, see also Art 20 DSA proposal (requiring providers to suspend the processing of notices by parties that frequently submitted manifestly unfounded notices). Note that, in comparison, Section 512(c)(3)(A) and (f) DMCA are more demanding where it comes to the elements that notices must contain and more 'threatening' in view of the liability in damages for 'misrepresentations' in notices for which it provides.

165 Art 7 DSA proposal (essentially restating Art 15(1) ECD).

166 Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market, [2019] OJ L 130/92 ('CDSM Directive').

167 Commission, Proposal for a Regulation on preventing the dissemination of terrorist content online COM(2018) 640 (see in particular its Art 6, proposing introducing an obligation for hosting service providers to take certain proactive measures aimed at tackling terrorist content).

168 See Points 18, 36 and 37 Illegal Content Recommendation (encouraging hosting service providers to take proactive measure where appropriate and in any event in relation to terrorist content, including to prevent the resubmission of removed terrorist content).

such as staydown obligations or the provision of information on users suspected of illegal conduct, or temporarily barring infringers from using the services in question. This despite the fact that, notwithstanding certain challenges, there is no need to think that such forms of injunctive relief are legally precluded per se.[169] Apart from increasing effectiveness in terms of tackling illegal user content, they could help reduce the current heavy reliance on a system of 'privatised' enforcement, with which many feel uneasy.[170] Yet under the DSA proposal – as under the ECD – injunction-related issues would largely be left to be regulated under national law.[171]

50 The DSA proposal's comparatively modest approach on the matters discussed in the previous paragraph likely has to do with recent experiences showing how polemic possible EU rules on proactive measures, staydown obligations and injunctions can be.[172] Take the 2019 reform of EU's regime on the liability of certain service providers for online copyright infringements, which resulted in Article 17 CDSM Directive. Under the article service providers are, inter alia, to make 'best efforts' to ensure the unavailability of copyright-protected works and to prevent them from being re-uploaded after removal.[173] The reform was extremely controversial.[174] Probably largely because of the starkly diverging views, the new rules are seen as complex and unclear at best, if not plain inconsistent.[175] A case contesting their compatibility with the fundamental right to freedom of expression is currently pending.[176] Debates about the Commission's guidance on Article 17 CDSM Directive show that the matter remains highly sensitive.[177] Although generating somewhat less attention, the TCO Regulation, adopted in April 2021,[178] similarly generated strongly diverging views.[179] Its rules on

169 See eg CJEU, *Facebook Ireland* (n 20), 46 (on staydown obligations); CJEU, *L'Oréal v eBay* (n 19), 141 (on the suspension of the provision of services to users engaged in illegal conduct).

170 See European Parliament, Resolution on the Digital Services Act: adapting commercial and civil law rules for commercial entities operating online, P9_TA(2020)0273, G ("*delegating decisions regarding the legality of content or of law enforcement powers to private companies undermines transparency and due process*"). See eg also S Dusollier, 'The 2019 Directive on copyright in the digital single market: some progress, a few bad choices, and an overall failed ambition', (2020) *Common Market Law Review* 57, 1016; M Bassini, 'Fundamental rights and private enforcement in the digital age', (2019) *European Law Journal* 25, 186; Barata (n. 142), 10; Kuczerawy, *Intermediary liability and freedom of expression in the EU* (n 82), 5–6; K Kaesling, 'Privatising law enforcement in social networks: a comparative model analysis', (2018) *Erasmus Law Review* 12, 159–160.

171 See in particular Art 5(4) DSA proposal (echoing Art 14(3) ECD). Note that Art 8 and 9 DSA proposal provide for rules on orders addressed to hosting service providers to act against illegal content or to provide information, respectively. However, those rules do not actually *empower* national courts or administrative authorities to issue such orders, but rather set a framework within which any such powers attributed under national law (or other acts of EU law) are to be exercised. See also Recitals 29-33.

172 Cf also Commission, Impact assessment DSA proposal, SWD(2020) 348, 19 ("*The issue of the use of automated tools to automatically detect illegal content, services and goods is considered very controversial among respondents [to the public consultation]*").

173 Art 17(4)(b) and (b) CDSM Directive.

174 See C Angelopoulos and J Quintas, 'Fixing copyright reform: a better solution to online infringement', (2019) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 10, 147 ("*The proposal [for the CDSM Directive] was controversial from the start. Almost every step of the legislative process was the subject of intense lobbying and debate*"). See also G Spindler, 'The liability system of Art 17 DSMD and national implementation: contravening prohibition of general monitoring duties', (2019) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 10, 344; T Spoerri, 'On upload-filters and other competitive advantages for big tech companies under Article 17 of the Directive on copyright in the Digital Single Market', (2019) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 10, 174 (both making similar statements).

175 See eg Dusollier (n 166), 1008 and 1010-1011 (describing Art 17 CDSM Directive as a "*monster provision*" and as "*a complex construction and the outcome of many political compromises*"); Angelopoulos and Quintas (n 170), 153 (stating that the rules "*create more questions than they answer*"); Husovec (n 3), 537 (describing the new system as "*a mechanism with too many moving parts*"). See also Joint Statement by the Netherlands, Luxembourg, Poland, Italy and Finland, Council doc. 7986/19, 15 April 2019, 1 ("*we feel that [the CDSM] Directive lack legal clarity, will lead to legal uncertainty for many stakeholders concerned and may encroach upon EU citizens' rights*").

176 CJEU, *Poland v European Parliament and Council*, C-401/19 (pending).

177 See eg 'Commission and Parliament in 'secret talks' on EU copyright directive', Euractiv, 12 February 2021; 'EU civil society says Commission's copyright guidance violates 'fundamental rights'', Euractiv, 15 September 2020. For the guidance, provided pursuant to Art 17(10) CDSM Directive, see Commission, Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market, COM(2021) 288.

178 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 ('TCO Regulation').

179 See eg EU Agency for Fundamental Rights, Opinion on the

proactive measures and on the issuance of removal orders were among the main bones of contention.[180] The situation does not seem fundamentally different in the US, where bitter disputes linger over recent and potential future updates of Section 512(c) DMCA and Section 230 CDA.[181] It therefore appears that any suggestion to introduce measures of this kind leads almost by definition to controversy. That being so, whilst some may be disappointed in the comparatively modest ambitions of the DSA proposal in this regard,[182] others may well welcome the approach as more balanced or politically realistic.

51 The comparatively modest approach when it comes to tackling illegal user content contained in the DSA proposal also reflects the fact that the DSA is conceived as horizontally applicable 'baseline' measure. The DSA Regulation is meant to complement sector- or content-specific acts, such as Article 17 CDSM Directive, the TCO Regulation and the Audiovisual Media Service Directive (AVMSD) as amended in 2018.[183] Precisely because these other acts tend to provide for specific – and more demanding – requirements, there is arguably less of a need for the DSA proposal to go into these issues.[184] At the same time, relying on these specific acts also means that the overall picture is not always consistent or self-evident. Is it entirely logical, for instance, that EU law provides for staydown-like requirements only in respect of copyright-infringing content?[185] Such content can cause serious damage, but few would probably argue that the damage is more serious than that caused by, for example, child sexual abuse material or terrorist content. One could also wonder why it is that only video-sharing platforms are required to take certain measures to tackle hate speech contained in audiovisual content uploaded by users.[186] These platforms and the audiovisual content that they disseminate for their users surely are an important part of the broader problem of online hate speech. But so are, it would appear, social media companies and the written texts that they disseminate for their users, for instance.[187]

52 Despite this, it would be wrong to conclude that the DSA proposal does not contain any measures at all that aim at tackling illegal user content more effectively. The proposal would, in fact, subject hosting service providers[188] to what could be called an EU-level duty of care to this effect. This does not

proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications, 2/2019; European Data Protection Supervisor, Formal comments on the proposal for a Regulation on preventing the dissemination of terrorist content online, 2019; J Van Hoboken, 'The proposed EU Terrorism Content Regulation: analysis and recommendations with respect to freedom of expression implications', Transatlantic Working Group, 2019; J Barata, 'New EU proposal on the prevention of terrorist content online: an important mutation of the e-commerce intermediaries' regime', Center for Internet and Society, 2018; E Coche, 'Privatised enforcement and the right to freedom of expression in a world confronted with terrorist propaganda online', (2018) *Internet Policy Review* 7, 1–17.

180 See in particular European Parliament (n 105) (suggesting reserving the power to issue removal orders only to the Member State of establishment of the service provider concerned and deleting all references to proactive obligations for hosting service providers).

181 As regards Section 512(c) DMCA, see eg US Copyright Office (n 8), 73 (noting a "*stark division of opinion*" between the main stakeholders). As regards Section 230 CDA, see in particular the amendment of Section 230 CDA adopted in 2018 through a law known as FOSTA (Allow States and Victims to Fight Online Sex Trafficking Act, incorporated in Section 230(e)(5) CDA). See E Goldman, 'The complicated story of FOSTA and Section 230', (2019) *First Amendment Law Review* 17, 279–293, 292 ("*FOSTA may be one of Congress' worst achievements in Internet regulatory policy*"). See also Kosseff (n 37), 272; D Citron and Q Jurecic, 'Platform justice: content moderation at an inflection point', Hoover Institute Essay, Aegis series paper No. 1811, 2018, 3; D Keller, 'SESTA and the teachings of intermediary liability', Center for Internet and Society, 2017 (all containing critical assessments of FOSTA).

182 See eg Nordemann (n 132), 30 and 42 (arguing for provisions on injunctions and staydown).

183 See n 155 (regarding the AVMSD and its amendment in 2018). On the interaction between the DSA proposal and Art 17 CDSM Directive, see further J Quintais and S Schwemer, 'The Interplay between the Digital Services Act and sector regulation: how special is copyright?', May 2021 (draft), available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841606>.

184 See Art 1(5) and Recitals 9-11 DSA proposal (indicating that the DSA would "*complement, yet not affect*" said other acts).

185 Art 17(4) CDSM Directive.

186 Art 28b(1) AVMSD.

187 Art 1(aa) AVMSD defines the term 'video-sharing platform service' broadly, meaning that social media companies could in certain cases also be covered by the relevant rules. However, on the substance, the rules only apply to audiovisual material, not to written texts.

188 Note that most of the obligations mentioned here would in fact apply to a particular subcategory of hosting service providers, namely 'online platforms' (as defined in Art 2(h) DSA proposal). For reasons of consistency and simplicity, the general term 'hosting service provider' is nonetheless used here. Furthermore, references made to *very large* hosting service providers should be understood as references to very large online platforms within the meaning of Art 25 DSA proposal (setting the threshold at 45 million users in the EU).

only mean that mandatory (as opposed to ultimately voluntary) requirements for hosting service providers to take certain measures are introduced. It also marks a notable change as compared to the ECD in that the latter leaves it to the Member States to decide whether to impose such a duty under national law.[189] Three additional measures stand out, apart from the measures already mentioned (broadening the scope to also cover third country-based providers active in the EU; the new EU rules on notice-and-action mechanisms; the 'Good Samaritan' clause, which would not *oblige* but nonetheless *encourage* the taking of proactive measures to tackle illegal user content). First, the providers would be required to act against users who provide illegal content.[190] This is a sort of repeat infringer requirement. It implies that – at least to some extent – the focus is no longer solely on illegal content as such, but also on the users providing it. The DSA proposal seeks to address the aforementioned complexities that arise in this regard by limiting the obligation to content that is *manifestly* illegal and to users that *frequently* provide such content.[191] Providers would be required to assess that on a case-by-case basis and to set out their policies in this respect in their terms and conditions.[192] Second, the providers would be required to notify suspicions of certain serious criminal offences to the competent authorities.[193] Finally, very large providers would be obliged to annually assess any significant systemic risks stemming from their service provision, inter alia for the dissemination of illegal user content, and to take measures to mitigate any such risks.[194] These requirements are worded rather broadly, meaning their practical effects are somewhat uncertain. Nonetheless, they could play an important role in achieving the objective of tackling the type of illegal user content causing serious 'public' harm, mentioned earlier, in a more effective manner.

III. Protecting users' rights and interests

53 The DSA proposal's ambitions to better protect the rights and interests of EU users of hosting services – in particular to freely express themselves, to be able to access legitimate content and to be treated in a fair and transparent manner – are by no means modest. Indeed, when assessed at the general level it seems fair to say that this is the DSA's primary focus. This entails a notable change of approach as compared to earlier acts such as Article 17 CDSM Directive and the TCO Regulation. Unlike the DSA proposal, those earlier acts focus primarily at tackling illegal content, while seemingly considering the provision of safeguards to protect users' rights and interests more as secondary issue, instead of considering the latter as an objective in its own right. Thus, if the measures discussed in the previous subsection are seen as entailing an EU-level duty of care aimed at tackling illegal content, then the measures discussed in the present subsection could be seen as being aimed at ensuring that the duty is *doubled-sided* in nature, in the sense that the service providers concerned should also – and equally – take account of these kinds of rights and interests of the users when moderating the user content that they intermediate.

54 The DSA proposal would certainly not preclude content moderation as such, irrespective of whether the activities in question are aimed at tackling illegal content or terms of service-infringing content.[195] Thus, hosting service providers would in principle retain the possibility to set and enforce their terms of service, including where those terms of service are more restrictive than the applicable law when it comes to the types of content that they are willing to store and disseminate for their users. However, the DSA proposal would – on top of the limits that already result from generally applicable acts of EU law, such as the GDPR and the Unfair Terms Directive[196] – create an extra layer of user protection. In essence, the DSA proposal seeks to ensure that

189 Recital 48 ECD. Member States appear to make increasing use of that possibility. See eg the NetzDG in Germany and the so-called Avia law in France (although key parts of the latter bill were declared unconstitutional by the French Constitutional Council; see its Decision 2020-801 DC, 18 June 2020). See further D Savova, A Mikes and K Cannon, 'The Proposal for an EU Digital Services Act — A closer look from a European and three national perspectives: France, UK and Germany' (2021) *Computer Law Review International* 22, 38-45.

190 Art 20(1) DSA proposal. Pursuant to Art 20(2), providers would also be required to take measures against parties that frequently submit manifestly unfounded notices or complaints.

191 See para 36 above (regarding said complexities).

192 Art 20(3) and (4) DSA proposal. See also Recital 47 (expanding on the concept of 'manifestly illegal content').

193 Art 21 DSA proposal. Specifically, the proposed obligation relates to "*serious criminal offence[s] involving a threat to the life or safety of persons*". In this regard, see also Recital 48 (indicating that this term covers offences involving child sexual abuse, among other things).

194 Art 26 and 27 DSA proposal.

195 Cf Art 2(p) DSA proposal (defining the concept 'content moderation' essentially as any activities undertaken by providers to tackle content that is either illegal or violates their terms and conditions).

196 Directive 93/13/EEC on unfair terms in consumer contracts, [1993] OJ L 95/29.

content moderation takes place within a procedural framework set not by the providers themselves in view of their own commercial interests, but rather by the legislator in view of the public interests at stake. It is especially this aspect of the DSA proposal that is novel and may have the potential to become a sort of international standard, just as occurred with the GDPR in relation to the protection of personal data.[197]

55 Leaving aside the proposed rules already discussed above, again, three sets of provisions of the DSA proposal can be mentioned in particular. First, there is a strong emphasis on transparency, particularly in respect of content moderation-related matters. The proposed obligations range from providing clarity upfront in the terms and conditions, to the provision of reasons for the providers' decisions in individual cases, to ex post reporting to the public.[198] Such increased transparency is important for several reasons. It allows users to take informed decisions as to whether or not they wish to use the services in question, it reduces the scope for arbitrary decisions and it facilitates accountability. Second, users' redress possibilities would be improved, inter alia in relation to decisions to remove their content or suspend their account. Such redress would be possible not only through the aforementioned internal complaint-handling systems, but also through out-of-court dispute settlement and rules on the lodging of complaints to supervisory authorities and on representative actions.[199] As mentioned, the complaint-handling systems are essentially an EU version of the counter-notice procedures known in the US (although they are broader in scope). Finally, public oversight and enforcement would be significantly reinforced.[200] Rather extensive powers would be granted to national competent authorities, including to conduct on-site inspections, impose hefty fines (up to 6% of annual turnover) and block websites.[201] There is also a novel system of enhanced supervision of very large hosting service providers, the most notable feature of which is that it equips the Commission with direct investigatory and sanctioning powers.[202] Strengthening oversight and enforcement in this manner is important. That is due to the public interests at stake, but also because one should probably be realistic about what can be expected from users' redress mechanisms. The limited use made of the counter-notice procedure provided for in US law may be in part due to the design of that procedure,[203] but it probably also tells us something about the limited willingness or ability of users to actively defend their interests themselves. That does not mean that such redress mechanisms should not be provided for. But it does mean that the task of ensuring that the system works as intended cannot solely be left to users; public authorities may therefore need to step in.

I. Conclusion

56 In 1996 – that is, a few years before tabling the proposal for the ECD – the Commission stated that it sought to assist "*host[ing] service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability*".[204] A lot may have changed in the 25 years that followed, but the essence of the challenge remains unaltered. It is evident from the DSA proposal that the Commission considers that this path should continue to be founded on the knowledge-based liability model. This article has shown that that decision is understandable and perhaps even unavoidable. This finding constitutes, however, no more than a starting point for discussions on that proposal. Indeed, whilst the foundations of the proposed approach may be sound, room remains for diverging views on a range of matters relating to the liability of hosting service providers for stored user content. Especially if recent experiences are any guide, one can expect interesting and perhaps intense debates as to whether or not the measures that the Commission has put forward to refine and complement the existing model succeed in the ambition to steer a path for the next 25 years.

197 Savin (n 16), 16.

198 Art 12, 15, 13, 23 and 33 DSA proposal, respectively. In addition, very large hosting service providers are to provide, upon request, competent authorities or vetted researchers with access to data (Art 31 DSA proposal).

199 Art 17, 18, 43 and 68 DSA proposal, respectively.

200 The ECD does contain some provisions in this regard (Art 17-20), but those are, on the whole, neither very specific nor very demanding.

201 Art 41 and 42 DSA proposal.

202 Art 50-66 DSA proposal.

203 See para 41 above.

204 Commission, Illegal and harmful content on the internet, COM(96) 487, 12-13.

Exploring the limits of joint control: the case of COVID-19 digital proximity tracing solutions

by **Stephanie Rossello and Pierre Dewitte***

Abstract: Referring to the judgment of the CJEU in Fashion-ID, some scholars have anticipated that, "at this rate everyone will be a [joint] controller of personal data". This contribution follows this arguably provocative, but not entirely implausible, line of thinking. In the first part of the article, we highlight the ambiguities inherent to the concept of "joint control" and confront them with those pertaining to the notion of "identifiability". In the second part, we investigate the effects of the broad legal test for joint control on the role of the individual user of BLE-based COVID-19 digital proximity tracing solutions. This offers the possibility to examine, at a theoretical level, whether the impact of the broad notion of joint control differs depending on the architecture of the system (i.e. centralized or decentralized). We found out that the strict application of the joint controllership test could lead to unexpected and, most likely, unintended results. First, an app user could, in theory, qualify as a joint controller with a national health authority regardless of the protocol's architecture. Second, an actor could, again in theory, be considered as a joint controller of data that is not personal from that actor's perspective.

Keywords: Joint control; personal data; identifiability; COVID-19; digital proximity tracing; GDPR; decentralisation; centralisation

Recommended citation: Stephanie Rossello and Pierre Dewitte, Exploring the limits of joint control: the case of COVID-19 digital proximity tracing solutions, 12 (2021) JIPITEC 342 para 1

A. Introduction

1 In its opinion in *Fashion-ID*, Advocate General Bobek foresightedly stated that: "When pushed to an extreme, if the only relevant criterion for joint control is to have made the data processing possible, thus in effect contributing to that processing at any stage, would the internet service provider, which makes the data processing possible because it provides access to the internet, or even the electricity provider, then not also be joint controllers potentially jointly liable for the processing of personal data?".[1] Referring to the judgment of the Court of Justice of the European Union ("CJEU") in

* Stephanie Rossello is a researcher at the KU Leuven Centre for IT & IP Law, where she is involved in the European Union's Horizon 2020 research and innovation program under grant agreement No 824988 "Machine learning to augment shared knowledge in federated privacy preserving scenarios" (MUSKETEER); Pierre Dewitte is a researcher and PhD candidate at the KU Leuven Centre for IT & IP Law, where he is involved in the KU Leuven-C2 research project "Privacy by design Regulation in Software Engineering" (PRiSE). The authors wish to thank Marie Beudels, Ilaria Buri, Ivo Emanuilov, César Augusto Fontanillo López, René Mahieu and the two peer-reviewers for their insightful feedback on draft versions of this article.

1 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek ECLI:EU:C:2018:1039, para 74.

Fashion-ID, some scholars, similarly, anticipated that, "at this rate everyone will be a [joint] controller of personal data".[2] This contribution follows this arguably provocative, but not entirely implausible, line of thinking.

2 More specifically, in the first part of the article, we focus on the legal framework on joint control, by combining the ambiguities inherent to the notion of joint control with those pertaining to the notion of "identifiability" of personal data (section B). Next, we briefly describe and evaluate the scope of the household exemption (section C). In the second part of the contribution, we investigate the effects of the broad legal test for joint control on the role of the individual user of Bluetooth Low Energy ("BLE")-based digital proximity tracing solutions used in the fight against the COVID-19 outbreak ("COVID-19 apps").[3] This case-study was chosen because it offers the possibility to examine, at a theoretical level, whether the broad notion of joint control has different consequences depending on the architecture of the software system, i.e. whether it is centralized or decentralized. In relation to a case-study concerning security/privacy preserving edge computing solutions adopted in a smart home with Internet of Things, scholars have argued that the current broad notion of joint control, coupled with the narrow interpretation of the household exemption, may end up "unfairly burdening certain stakeholders in smart homes",[4] including the smart home user, and "disincentivise uptake"[5] of security/privacy preserving edge computing solutions. We are interested in knowing whether this conclusion could, in theory, also hold true in the case of privacy-preserving decentralized solutions such as those applied in COVID-19 digital proximity tracing. Therefore, after having set out the hypothesis, methodology, objective and limitations of the case-study (section D), we provide an overview of both the centralised and decentralised COVID-19 app ecosystems (section E), and subsequently apply the legal framework sketched out in sections B and C to the said case-study (section F). We then summarise our findings (Section G) and conclude the paper (Section H).

3 Notwithstanding the specific use case, we wish to stress from the outset that the present paper by no means provides a definitive answer as to the allocation of responsibilities for concrete digital proximity tracing solutions adopted in the fight against COVID-19. Neither does it attempt to confirm or deny an existing claim as to the potential role of COVID-19 app users as (joint) controllers. Rather, the analysis aims at illustrating how the lack of a coherent interpretation of key concepts delimiting the material and personal scope of application of EU data protection legislation, such such as the notions of "identifiability" of personal data and "joint controllership", may have arguably unintended consequences. Consequently, this contribution intends to pinpoint the concepts that need further clarification from the European Data Protection Board ("EDPB"), National Supervisory Authorities, the CJEU and domestic courts.

B. The ambiguous notion of joint control

I. Joint control under the GDPR

4 Article 4(7) General Data Protection Regulation ("GDPR") provides that the controller is the "natural or legal person, public authority, agency or other body which, *alone or jointly* with others, *determines* the *purposes and means* of the *processing* of *personal data* [...]" (emphasis added). This definition is the same as the one provided in the GDPR predecessor, Article 2 (d) of the Directive 95/46 ("DPD"). The latter provision has been further clarified by the Article 29 Working Party ("WP29") in its opinion 1/2010 on the concepts of controller and processor[6]—now replaced by the EDPB's guidelines 07/2020 on the concepts of controller and processor in the GDPR[7]—

2 Christopher Millard and others 'At This Rate, Everyone Will Be a [Joint] Controller of Personal Data!' (2019) 9 (4) International Data Privacy Law 217 <https://academic.oup.com/idpl/article/9/4/217/5771498> accessed 21 April 2021.

3 The development of these apps in Europe has indeed followed two main technical approaches, the so-called "centralised" versus "distributed" or "decentralised" approach. The technical protocols and accompanying security and privacy risks analyses of some of these COVID-19 apps have been made publicly available and easily understandable to a non-technical audience, including the authors of this contribution. The existence of this publicly available technical documentation rendered this legal analysis possible.

4 Jiahong Chen and others, 'Who Is Responsible for Data Processing in Smart Homes? Reconsidering Joint Controllership and the Household Exemption' (2020) 10 (4) International Data Privacy Law 293 <https://academic.oup.com/idpl/article/10/4/279/5900395> accessed 21 April 2021.

5 ibid.

6 Article 29 Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor" '(2010) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf> accessed 21 April 2021.

7 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR'

and by the CJEU in its judgments in the *Fashion ID*, *Wirtschafstakademie* and *Jehovah's Witnesses* cases. We start our analysis by investigating the object of joint control, *i.e.* the processing of personal data. Then, we examine the remaining building blocks of that definition and map the ambiguities surrounding the concept of joint control.

II. The notion of personal data as a gatekeeper

1. The legal test for identifiability

5 Before proceeding with the allocation of responsibilities, it is crucial to identify whether there is a processing of "personal data". Article 4(1) GDPR defines personal data as "any information relating to an identified or identifiable natural person [...]". Data that do not relate to an identified or identifiable individual will be considered anonymous and fall outside the scope of the GDPR. While other elements of this definition can also potentially pave the way for an extensive interpretation of personal data,[8] we limit the scope of our analysis to the controversial notion of "identifiability".

6 Recital 26 GDPR provides that "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly". In turn, according to Recital 26 GDPR, "to ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors such as the costs of and amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". As already discussed at length by several authors,[9] there is considerable legal uncertainty on the standard of identifiability set forth by the GDPR. This uncertainty concerns, among others, the perspective from which the nature of the data is to be assessed (the so-called "absolute" versus "relative" approach to personal data)[10] and the risk of (re-)identification that can be tolerated without data being considered as relating to an "identifiable individual" (the so-called "zero-risk" versus "risk-based" approach).[11]

2. Absolute and zero-risk versus relative and risk-based approach

7 Under the absolute approach, if *anybody* is theoretically able to identify a data subject on the basis of the data at issue (potentially combined with auxiliary information), that data would qualify as personal data.[12] Under the relative approach, the likelihood of re-identification would only be assessed from the perspective of a more *limited* number of parties, *i.e.* the controller or a third party that is reasonably likely to approach or be approached by

<https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf> accessed 13 July 2021. It is worth noting that the final version of these guidelines have been issued at the very end of the publication process. In light of the above, we have done our best to reflect the modifications and refinements implemented following the public consultation period.

8 Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 (1) Law, Innovation and Technology, 48–59 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176> accessed 21 April 2021.

9 See for a recent overview of the uncertainties surrounding the identifiability test set out in Recital 26 GDPR: Michele Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 (1) International Data Privacy Law, 14–19 <https://academic.oup.com/idpl/article/10/1/11/5802594?login=true> accessed 21 April 2021; Purtova (n 8) 46-48 <https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176>; Manon Oostveen, 'Identifiability and the Applicability of Data Protection to Big Data' (2016) 6 (4) International Data Privacy Law 299, 304–306 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipw012> accessed 21 April 2021; Worku Gedefa Urgessa, 'The Protective Capacity of the Criterion of "Identifiability" under EU Data Protection Law' (2016) 4 European Data Protection Law Review 521 <http://edpl.lexxion.eu/article/EDPL/2016/4/10> accessed 21 April 2021.

10 Finck and Pallas (n 9) 17–18; Gerald Spindler and Philipp Schmechel, 'Personal Data and Encryption in the European General Data Protection Regulation' (2016) 7 (2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 165-166 <https://www.jipitec.eu/issues/jipitec-7-2-2016/4440> accessed 21 April 2021.

11 Finck and Pallas (n 9) 14–16; Sophie Stalla-Bourdillon, 'Anonymous Data v. Personal Data a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Journal 286 ff < https://repository.law.wisc.edu/s/uwlaw/media/77051> accessed 21 April 2021; Sophie Stalla-Bourdillon, 'Anonymising Personal Data: Where Do We Stand Now?' (2019) 19 (4) Privacy & Data Protection Journal 5 <https://www.immuta.com/anonymizing-personal-data-where-do-we-stand-now-2/> accessed 21 April 2021.

12 Spindler and Schmechel (n 10) 165.

the controller.[13] Under a zero-risk approach, data would be personal as soon as there is a risk of re-identification, no matter how negligible, whereas, under a risk-based approach, this would be the case only if identification is considered to be reasonably likely in light of the efforts it would require in terms of factors such as costs, time, technological means and expertise.[14] Although the reasonably likely means of identification standard set out in recital 26 GDPR seems to imply a risk-based approach to personal data, the interpretation of the identifiability criterion by the relevant authorities does not unequivocally point in this direction.[15] Below, we present a selection of the main interpretative guidance on identifiability.[16]

8 In its 2007 opinion on the concept of personal data, the WP29 stated that the "mere hypothetical possibility to single out the individual is not enough to consider the person as 'identifiable'" and stressed that the possibility of identification should be (re-)assessed on a continuous basis, throughout the expected lifetime of the data.[17] What is to be considered "reasonable" is context-dependant.[18] This seems to plead in favour of a risk-based approach. The WP29 also stressed that identifiability should be assessed not only from the perspective of the controller but from the perspective of "any other person".[19] While this might appear as advocating for an absolute approach—and therefore in contradiction with the above—the WP29 clarified that statement in an example related to key-coded personal data used for clinical trials, where the re-identification of patients is explicitly envisaged in the scope of the trial. According to the WP29, key-coded data would be considered personal data for the controllers involved in re-identification, but not for "any other data controller processing the same set of coded data [...], if within the specific scheme in which those other controllers are operating, re-identification is explicitly excluded and appropriate technical measures have been taken in this respect".[20] This, again, seems to favour a relative and risk-based approach.

9 In its later opinion on anonymization techniques, the WP29 appears to have adopted a more radical stance towards the identifiability threshold. There, it stated that the outcome of anonymization—*i.e.* the process through which data becomes anonymous and *a fortiori* non-identifiable—should be" as permanent as erasure" with the aim to "irreversibly" prevent re-identification.[21] Like in 2007, the WP29 stressed that identifiability must be judged from the viewpoint of the controller or any other third person.[22] In a much criticized example,[23] however, it clarified that if a controller provides a dataset with individual travel patterns at event level to a third party after having removed or masked the identifiable data, such a dataset would still qualify as personal data "for any party, as long as the data controller (or any other third party) still has access to the original raw data".[24] Here, the absence of any reference to the likelihood of such re-identification happening seems to imply an absolute and zero risk approach to personal data.[25]

10 Later, the CJEU interpreted the notion of "reasonably likely" means of identification in the *Breyer* case, where it held that a dynamic IP address held by a

13 See for an example: Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016], Opinion of Advocate General Campos Sánchez-Bordona ECLI:EU:C:2016:339, para 67-68; For further explanation on these approaches see: ibid 165-166; Finck and Pallas (n 9) 17-18.

14 Finck and Pallas (n 9) 14–16.

15 ibid. 15-20.

16 The interpretative guidance presented above relates to recital 26 of the DPD, which contains an identifiability test similar to the one set out in recital 26 of the GDPR and, more specifically, provides that: "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person". Considering the similarity between the test of the DPD and the GDPR and the fact that recital 26 of the GDPR has not been interpreted yet by the EDPB or CJEU, the interpretation provided under the DPD is still relevant at the time of writing.

17 Article 29 Working Party, 'Opinion 4/2007 on the Concept of Personal data' (2007) 15 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 21 April 2021

18 ibid. 13.

19 ibid. 19. This mirrors the wording of recital 26 of the DPD which referred to "any other person", not "another person" as recital 26 GDPR.

20 Article 29 Working Party (n 17) 20.

21 Article 29 Working Party, 'Opinion 05/2014 on Anonymisation Techniques' (2014) 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf> accessed 21 April 2021.

22 ibid 9.

23 Finck and Pallas (n 9) 15; Stalla-Bourdillon, 'Anonymising Personal Data: Where Do We Stand Now?' (n 11) 2.

24 Article 29 Working Party (n 21) 9.

25 Finck and Pallas (n 9) 15.

content provider was personal data, even if that provider was not able, by itself, to link the address to a particular individual. The Court considered that, since German law allowed the content provider to combine the dynamic IP address with the information held by the internet service provider under specific circumstances such as cyberattacks, the content provider had a legal possibility to identify the data subject. This legal possibility was considered a "reasonably likely" means to be used. Conversely, the likelihood test would not have been met if identification was "prohibited by law or practically impossible on account of the fact that it requires disproportionate efforts in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[26] As such, it seems that the CJEU has embraced a risk-based approach to personal data, since it investigated the actual means of re-identification that were at the disposal of the content provider.[27]

11 As to the perspective from which "identifiability" should be assessed, the opinion of Advocate General Campos Sánchez-Bordona in *Breyer* points to a relative approach. According to him, a reference to "any third party" must be understood as referring to third parties "who, *also in a reasonable manner*, may be approached by a controller seeking to obtain additional data for the purpose of identification".[28] Otherwise, "[...] it would always be possible to imagine the hypothetical contingency of a third party who, no matter how inaccessible to the provider of services on the Internet, could — now or in the future — have additional relevant data to assist in the identification of a user".[29]

12 Like others,[30] we believe that the relative and risk-based approach is the only sensible way to interpret the identifiability criterion. In light of the increasing amount of publicly available information which could potentially be used to re-identify a data subject and the growing body of research disputing the possibility to irreversibly anonymize data,[31] favouring an absolute and zero-risk approach to personal data could *de facto* amount to admitting that almost all data could potentially qualify as personal. This would lower legal certainty and increase the burden on controllers to make sure that the data they collect do not, at any point in time, lead to the potential re-identification of individuals.[32]

III. The components of joint control

1. The notion of controller: a necessary first step

13 As highlighted by the EDPB, "the assessment of joint controllership should mirror the assessment of 'single' control [...]".[33] Before analysing the criteria used to establish joint control, it is therefore crucial to first identify which entities qualify as controllers in their own right. Only then is it possible to examine whether they would qualify as joint, or rather sole, controllers vis-à-vis certain processing operations. As such, the EDPB breaks down the definition of controller into the following building blocks.[34] A controller is the:

- "natural or legal person, public authority, agency or other body" that;
- "determines";
- "alone or jointly with others";
- "the purposes and means";
- "of the processing of personal data".

14 The first building block is self-explanatory for the purposes of this contribution. What needs to be highlighted is that a natural person can also qualify as a controller under the GDPR. As detailed

26 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C:2016:779 para 46.

27 See similarly: Finck and Pallas (n 9) 18; Daniel Groos and Evert-Ben van Veen, 'Anonymised data and the rule of law' (2020) 6 (4) European Data Protection Law, 1-11 < http://edpl.lexxion.eu/article/EDPL/2020/4/6> accessed 21 April 2021.

28 Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016], Opinion of Advocate General Campos Sánchez-Bordona (n 13), para 68.

29 ibid.

30 See for authors similarly arguing in favour of a risk-based approach to personal data: Finck and Pallas (n 9) 34–36; Groos and van Veen (n 27); Stalla-Bourdillon, 'Anonymising Personal Data: Where Do We Stand Now?' (n 11).

31 See authors quoted in Oostveen (n 9) 306, who correctly points out that, due to the recent social and technical developments, the categorization of data as "identifiable" and "non-identifiable" has become more difficult.

32 See for authors taking a similar stance: Groos and van Veen (n 27); WK Hon, C Millard and I Walden, 'The Problem of "personal Data" in Cloud Computing: What Information Is Regulated?--The Cloud of Unknowing' (2011) 1 (4) International Data Privacy Law 211-228 <https://academic.oup.com/idpl/article-lookup/doi/10.1093/idpl/ipr018> accessed 21 April 2021.

33 European Data Protection Board (n 7) 19.

34 ibid 9-10.

in section C, this also opens up the possibility for natural persons to rely on the so-called "household exemption" to avoid falling under the Regulation's scope of application.

15 Second, the capacity to "determine", stresses the EDPB, refers to "the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*".[35] As already clarified by the WP29,[36] the EDPB emphasises that such influence can stem from either legal provisions or an analysis of the factual elements surrounding the circumstances of the case. In the case of legal provisions, where a piece of domestic legislation lays down the purposes and the means of a specific (or set of) processing operation(s), the legislator can also appoint the controller or the criteria for its nomination (Art. 4(7) GDPR). This seems to suggest that the possibility for the legislator to allocate responsibilities is conditional upon the determination of the purposes and means of the processing. Those purposes must be explicitly and legitimately specified (Art. 5(1)b GDPR). However, the legislator also has the possibility to add specific provisions for the type of data to be processed and the data subjects concerned, where the processing is based on the performance of a task carried out in the public interest (Art. 6(3) second indent GDPR). Collectively, this prevents the legislator from allocating responsibilities in a vacuum. It also means that the legal designation only covers the processing operations that pursue a set of pre-defined purposes.

16 In the case of contextual analysis, where the law does not explicitly or implicitly allocate responsibility to a certain entity, a factual assessment is required "in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question".[37] The wording used by the EDPB therefore seems to suggest that such a factual assessment is not necessary where the controller or the criteria for its determination have been laid down by law.[38] In that case, the EDPB underlines that the legal designation "will be determinative for establishing who is acting as controller".[39] Nonetheless, the EDPB also states that the designation of the controller by law presupposes that the appointed entity "has a genuine ability to exercise control".[40] This seems to be a safeguard against overly artificial schemes allowing to challenge the allocation of responsibilities put in place by the legislator, should there be major discrepancies between the factual reality and the legal fiction.

17 Third, it appears from the wording of Art. 4(7) GDPR—"alone or jointly with others"—that more than one entity can determine the purposes and the means of the processing operations. This can lead to a situation of joint control, which will be extensively discussed below.

18 Fourth, as already pointed out by the WP29,[41] the EDPB states that determining the "purposes and means" amounts to "deciding respectively the 'why' and the 'how' of the processing."[42] It is necessary to exert influence over both those elements to qualify as a controller, although "some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing".[43] In short, one should distinguish between the essential means—which have to be determined by the controller—and the non-essential means—which can, to a certain extent, be delegated to another entity without shifting (or sharing) the burden of control to or with that entity. The essential elements of the means concern matters such as which data shall be processed, which third parties shall have access to the data or how long the data shall be processed.[44] The non-essential elements relate to more "practical aspects of implementation" such as which software or hardware to use.[45]

19 Fifth, when detailing the notion of "processing**"**, the EDPB emphasises that control is to be allocated with regard to specific processing operations. In other words, the assessment described above "may extend to the entirety of the processing at issue, but may also be limited to a particular stage in the processing".[46] In that sense, the EDPB accommodates both a macro and a micro-perspective when it comes to the identification of the relevant processing

35 ibid 11.

36 Article 29 Working Party (n 6) 8-10.

37 European Data Protection Board (n 7) 11.

38 ibid 11. The EDPB indeed states that "*in the absence of* control arising from legal provisions, the qualification [...] must be established on the basis of an assessment of the factual circumstances surrounding the processing" (emphasis added).

39 ibid 11.

40 ibid.

41 Article 29 Working Party (n 6) 14.

42 European Data Protection Board (n 7) 14.

43 ibid.

44 ibid 15

45 ibid.

46 ibid 17.

operations.[47] It fails, however, to provide any specific guidance as to the criteria to be used to identify the relevant set or stages of the processing operations. Moreover, as will be detailed below, the EDPB does not consider access to the data being processed as a determining factor when qualifying an entity as a controller.[48]

2. The notion of joint control in the CJEU case law

20 In its latest *Fashion ID* judgment, the CJEU was asked by the referring court whether the operator of a website like Fashion ID could qualify as a controller under the DPD when embedding a Facebook 'like' plug-in on its website. The plug-in caused the visitor's browser to transmit personal data to Facebook, regardless of whether that visitor had a Facebook account and whether they had clicked on the 'like' button or not. The personal data at issue consisted of the visitor's IP address and the browser string to which Fashion ID did not have access. The CJEU was not asked to rule on whether the data at issue were personal. Like Advocate General Bobek, who delivered the opinion in that case,[49] the Court probably took it as a given that they were. The Court did, however, specify that "joint responsibility of several actors for the same processing [...] does *not* require each of them to have *access* to the personal data concerned" (emphasis added).[50] When it comes to identifying the relevant processing operations in relation to which control has to be assessed, the Court stated that "the processing of personal data may consist in one or a number of operations, each of which relates to one of the *different stages* that the processing of personal data may involve" (emphasis added).[51] The Court deemed the "collection and disclosure by transmission"[52] of the website visitors' personal data by Fashion ID to Facebook as the relevant processing operations in relation to which Fashion ID's controller role should be assessed. Subsequent stages in the processing were, by contrast, deemed irrelevant.

21 After having stressed that the concept of controller is to be defined broadly in order to ensure "effective and complete protection" [53] of data subjects, the CJEU held that a "natural or legal person who exerts influence over the processing of personal data, *for his own purposes*, and who participates, as a result, in the *determination of the purposes* and *means* of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46" (emphasis added).[54] As to the means, the Court concluded that Fashion ID, by embedding the social plugin on its website, while being fully aware that it served as a tool for collection and transmission of personal data to Facebook, "exerts a decisive influence over the collection and transmission of the personal data of visitors to that website" to Facebook, "which *would not have occurred without* that plugin" (emphasis added).[55] As to the purposes, the CJEU considered that the collection and transmission of personal data to Facebook were "performed in the *economic interests* of both Fashion ID and Facebook Ireland, for whom the fact that it can use those data for its own *commercial purposes* is the consideration for the benefit to Fashion ID" (emphasis added).[56] The CJEU concluded that Fashion ID can be considered to be a joint controller with Facebook in respect of the "collection and disclosure by transmission of the personal data of visitors to its website".[57]

22 Earlier, in the *Wirtschafstakademie* case, the CJEU had to determine whether the administrator of a Facebook fan page, *i.e.* Wirtschafstakademie, could be considered a joint controller with Facebook in relation to the processing of personal data of the visitors of that fan page. When considering the role of the administrator of the fan page in relation to that processing, the Court attached importance to the fact that, by creating the fan page, the administrator "*gives* Facebook the *opportunity*" to carry out such processing (emphasis added).[58] It further held that the fan page administrator "contributes to the

47 European Data Protection Board (n 17) 17. This mirrors the approach taken earlier by the WP29, as also mentioned by Van Alsenoy in Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (KU Leuven Centre for IT and IP Law, 1st edn, Intersentia, 2019) 69.

48 European Data Protection Board (n 7) 17.

49 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek (n 1), para 58.

50 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629 para 69.

51 ibid para 72.

52 ibid para 76.

53 ibid para 50.

54 ibid para 68.

55 ibid para 78.

56 ibid para 80.

57 ibid para 84.

58 Case C210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECLI:EU:C:2018:388 para 35.

processing of the personal data of visitors to its page" by defining the criteria in accordance with which the statistics of the visits of the fan page were to be drawn and designating the categories of persons whose personal data would be made use of by Facebook.[59] The CJEU therefore considered that the fan page administrator was taking part in the determination of the purposes and the means of the processing of personal data of visitors of that fan page, "by its *definition of parameters* depending in particular on its target audience and the *objectives of managing* and *promoting its activities*" (emphasis added).[60] Like in *Fashion ID*, the CJEU stressed that it was not necessary for each controller to have access to the relevant personal data and that various operators may be involved at different stages of the processing of personal data and to different degrees.[61]

23 Similarly, in *Jehovah's Witnesses*, the CJEU confirmed that access to the personal data was not a necessary prerequisite for an actor to qualify as a (joint) controller.[62] Concretely, the CJEU considered that, although the Jehovah's Witnesses Community did not have access to the personal data and did not know the specific circumstances in which its members collected and further processed such data, it nonetheless "organized, coordinated and encouraged" the preaching activities in the framework of which the processing was taking place.[63] Moreover, "the collection of personal data relating to the persons contacted and their subsequent processing" was carried out to "help achieve the objective of the Jehovah's Witnesses Community, which is to spread faith".[64] The CJEU considered this to be sufficient to conclude that the Jehovah's Witnesses Community determined, jointly with its members, "the purposes and means of processing of personal data of the persons contacted [...]".[65]

3. The notion of joint control in the EDPB Guidelines 07/2020

24 Compared to the assessment of control in general (see section B.III.1), when it comes to assessing joint control, the EDPB appears to stress more the importance of a factual, rather than a formal analysis. Indeed, in the case of joint control, states the Board, it might be that "the formal appointment [laid down by the law or in a contract] does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to 'determine' the purposes and means of the processing".[66]

25 According to the EDPB, "the overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation".[67] The EDPB further states that two or more entities can be seen to jointly participate in the determination of the purposes and the means of a given (or set of) processing operation(s), when they take "common" or "converging" decisions.[68] A common decision means "deciding together and involves a common intention in accordance with the most common understanding of the term 'jointly' referred to in Article 26 of the GDPR".[69] Converging decisions, on the other hand, "complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and the means of the processing".[70] Echoing the CJEU's finding in *Fashion ID*, the EDPB adds that an important criterion to determine that the entities take converging decisions, is "whether the processing *would not be possible* without both parties' participation in the sense that the processing by each party is inseparable, *i.e.* inextricably linked" (emphasis added).[71] Moreover, like the CJEU in *Fashion- ID*,[72] the EDPB stresses that the "existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal

59 ibid para 36.

60 ibid para 39.

61 ibid para 38, 43.

62 Case -25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta*, [2018] ECLI:EU:C:2018:551 para 69.

63 ibid para 70.

64 ibid para 71.

65 ibid para 73.

66 European Data Protection Board (n 7) 19.

67 ibid.

68 ibid.

69 ibid.

70 ibid.

71 ibid 19-20.

72 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* [2019] (n 50) para 70.

data."[73] As correctly remarked by other scholars,[74] there are, however, no clear criteria according to which responsibility should be apportioned among joint controllers.

26 The EDPB subsequently clarifies the meaning of a jointly determined purpose, *i.e.* a purpose that is either identical, common, closely linked or complementary to the purpose pursued by another entity.[75] Echoing the reasoning developed in both *Fashion ID* and *Wirtschafstakademie*, the EDPB states that this could be the case "when there is a mutual benefit arising from the same processing operation, provided that each entity involved participates in the determination of the purposes and means of the relevant processing operation".[76] At the same time, however, the EDPB also specifies that "the mere existence of a mutual benefit (for ex., commercial)" is not sufficient to establish joint control, as the entity involved in the processing must "pursue [a] purpose of its own".[77]

27 The EDPB moreover points out that jointly determining the means does not imply that the entities need to determine the means to the same extent. With reference to the abovementioned *Fashion ID* and *Wirtschafstakademie* cases, the EDPB clarifies that the joint determination of means can follow from a situation in which a given entity makes use of a technology developed by another entity for its own purposes. In that sense, "the entity who decides to make use of [the means provided by another entity] so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing".[78]

73 European Data Protection Board (n 7) 20.

74 Rene Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World – On the Question of the Controller, "Effective and Complete Protection" and Its Application to Data Access Rights in Europe' (2019) 10 (1) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 91, 95-96 < https://www.jipitec.eu/issues/jipitec-10-1-2019/4879> accessed 21 April 2021.

75 ibid 19.

76 ibid.

77 ibid.

78 ibid 20.

IV. From one ambiguity to another: towards a broad notion of joint control

1. The relevant processing operations

28 The processing operation in relation to which joint control should be assessed could be defined at a micro-level, looking at one specific processing operation, or at a macro-level, with respect to a set of processing operations. As mentioned above, the EDPB's opinion seems, like the earlier WP29 opinion it replaces,[79] to accommodate both approaches. By contrast, as already noted in literature, the CJEU appears to have adopted a micro-level and so-called "phase-oriented"[80] approach to joint control in its recent case-law, and most recently in *Fashion ID*.

29 Remarkably, as noted by other scholars in relation to the CJEU's ruling in *Fashion ID*,[81] both the CJEU and the EDPB fail to provide any objective criterion on the basis of which the relevant phases of the processing should be identified. According to some commentators,[82] the key element to define the relevant processing operation would be the unity of purposes.[83] As explained below, this introduces an

79 Van Alsenoy (n 47).

80 Rene Mahieu and Joris van Hoboken, 'Fashion ID: Introducing a Phase-Oriented Approach to Data Protection?' 30 September 2019 European Law Blog <https://europeanlawblog.eu/2019/09/30/Fashion ID-introducing-a-phase-oriented-approach-to-data-protection/> accessed 21 April 2021; Mahieu, van Hoboken and Asghari (n 74).

81 Mahieu and van Hoboken (n 80).

82 Serge Gutwirth, *Privacy and the information age* (Lanham, Rowman & Littlefield Publ., 2002) 97, as quoted in Van Alsenoy (n 47) 69-70.

83 This approach was also adopted by the Advocate General Bobek in his opinion in *Fashion ID*, in which he highlights that "both the Defendant and Facebook Ireland seem to pursue commercial purposes in a way that appears to be mutually complementary". "In this way", he adds, "although not identical, there is unity of purpose: there is a commercial and advertising purpose". Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek (n 1), para 105; The 'unity of purpose' approach has also been recognised by the EDPB in the final version of its guidelines 07/2020, where it states that 'it is necessary to double check whether at 'macro-level' these processing operations should not be considered as a 'set of operations' pursuing a *joint purpose* using jointly defined means (emphasis added). See European Data Protection Board (n 17) 17.

additional layer of uncertainty as to the level of detail with which the purposes should be defined. Indeed, the degree of precision with which the purpose is scoped will directly impact the granularity of the processing operations, and *vice-versa*. Intuitively, the more general the purpose, the higher the likelihood to find that several processing operations share the same purpose and the larger the set of the processing operations in light of which control is to be assessed. Conversely, the more specific the purpose, the lower such likelihood.[84] The EDPB did not provide any explanation on this point in its recent guidelines. The WP29 did, however, briefly touch upon this issue in its Opinion 03/2013 on purpose limitation, where it stated that the purpose "must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied. For these reasons, a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'".[85] It remains uncertain, however, whether a consideration made in relation to the principle of purpose limitation also applies to the definition of purposes when delineating the relevant processing operation for assessing control.[86] As a consequence, the delineation of the relevant processing operations and consequent allocation of responsibilities might end up being an arbitrary, fluid exercise, as will be further illustrated in the second part of this paper.

2. Identifiability and access to data

30 Another key question emerging from the findings outlined above is whether the perspective through which identifiability is assessed under Article 4(1) GDPR predefines the candidates for the role of controller. In other words, whether the assessment as to the existence of "personal data" happens independently from the one conducted to identify the entity that "determines" the "purposes" and the "means" of the processing.

31 Since access to the data at stake is a *de facto* requirement for an entity to be able to "reasonably likely" (re-)identify the individuals, by clarifying that access is not a prerequisite for "joint responsibility" (which in the cases at hand, implied joint control), the CJEU seems to have (at least implicitly) accepted that a party may qualify as a joint controller of data that from that party's perspective, are in fact anonymous. Interestingly—although they were not issued under the GDPR—the European Data Protection Supervisor's ("EDPS") Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 seem to endorse this approach. Indeed, the EDPS states that: "The fact that a party only has access to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or not longer identifiable [...] does not influence the joint controllership situation."[87] However, the EDPS adds, "this may nonetheless matter when establishing the degree of responsibility of the parties involved".[88]

32 To the contrary, if one were to adopt a relative approach to personal data and consider that the perspective from which identifiability is assessed predetermines the potential candidates for the role of controller, it would not even be necessary to assess the role of the parties lacking access to the data as possible (joint) controllers. In that case, the data at stake would not be personal to these parties, as, by lacking access, they would *a fortiori* lack the means reasonably likely to be used to identify the individual.

33 An alternative explanation could be that, by stating that access to data is not a prerequisite for joint control under the GDPR, the CJEU meant *actual* access to data at the time of the processing, as opposed to *potential* and reasonably likely future access. This interpretation would reconcile the CJEU's statement on access to personal data when assessing joint control with the relative and risk-based approach to personal data. However, it would still be incompatible with the less nuanced position of the EDPB on the topic, which, as already mentioned, stated that "someone who outsources a processing

84 See similarly: Frank Robben, 'Toepassingsgebied en begripsdefinities', in Jos Dumortier and Frank Robben, *Persoonsgegevens en privacybescherming. Commentaar op de wet tot bescherming van de persoonlijke levenssfeer* (Brugge, Die Keure, 1995) 28, as quoted in Van Alsenoy (n 47) 256-257.

85 Article 29 Working Party, 'Opinion 03/2013 on Purpose Limitation' (2013) 15–16 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed 21 April 2021.

86 See similarly: Charlotte Ducuing and Jessica Schroers, 'The recent case law of the CJEU on (joint) controllership: have we lost the purpose of 'purpose'?' (2020) 6 Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht 429.

87 European Data Protection Supervisor, 'Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725' 24 <https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf> accessed 21 April 2021.

88 ibid.

activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing [...] is to be regarded as controller even though *he or she will never have actual access* to the data" (emphasis added).[89] Thus, the question that remains unanswered is whether lacking potential—as opposed to actual—access could preclude an entity from being regarded as a controller.

34 The analysis carried out in section F illustrates a major implication of this loophole: potentially, an actor could qualify as a (joint) controller of data that, from that actor's perspective, are not personal.

3. The meaning of (participating in) the determination of purposes and means

35 Next to assisting in the delineation of the relevant processing activities in light of which control is to be assessed, identifying the "purpose" of the activity is also necessary to determine whether the entity(ies) at issue can be said to jointly participate in their determination. As seen above, determining the purposes means ascertaining "why" data is processed. In *Fashion ID,* the key criterion to conclude that the entities at issue jointly determined the purposes seems to have been that the processing operation commercially benefitted both entities. Fashion ID benefitted from an "increased publicity for its goods" and Facebook was able to use the data collected for "its own commercial purposes".[90] The EDPB, however, clarified that mutual (commercial) benefit is only an example of, but not a sufficient condition for, two or more entities to be said to jointly determine the purpose. According to the EDPB, what is required is that each entity pursues a "purpose of its own", which is defined negatively: an entity which is "merely being paid for the services rendered" would not pursue a purpose of its own and hence be a processor, not a joint controller.[91] This explanation seems to suggest that "own purpose" is to be interpreted as the motivating factor driving the entity to engage in a certain processing activity. This interpretation could, again, leave the door open to a wide array of situations where a party could qualify as a joint controller. Indeed, depending on how granularly the purpose is defined, it would in theory always seem possible to attribute a distinctive commercial or other purpose to the entities involved in the processing operations at stake.

36 As to the "means", whereas the EDPB makes a clear distinction between essential and non-essential means when discussing sole control and unambiguously states that the controller must determine the essential elements of the means, this clear-cut demarcation seems to become less relevant in the case of joint control.[92] With reference to *Fashion ID*, the EDPB indeed states that the joint determination of the means could follow from an entity's choice to use a tool developed by another entity for "its own purposes". Again, this raises the same interpretative questions and ensuing potential broad interpretation as to the meaning of processing for "its own purpose" as set out in the preceding paragraph.

37 Finally, the meaning of "determining" also suffers from a lack of clarity in at least two ways. First, it is unclear whether the legal designation of a controller should supersede factual reality. On the one hand, when assessing control (in general), the EDPB seems to imply that a factual analysis should only be performed in case of major discrepancies between the law and the fact. On the other hand, as mentioned above in section B.III.3, when assessing joint control, the EDPB seems to be more nuanced, by presumably requiring a higher degree of factual scrutiny when analysing whether two or more entities could act as joint controllers. This raises the specific question analysed in section F as to whether a situation of joint control is possible between a legally designated controller, on the one hand, and a factual controller, on the other. More specifically, the question is whether the designation of one controller by law as such excludes a situation of joint controllership between that legally designated controller and a factual controller. Again, although not applicable to the case at hand, the aforementioned EDPS' Guidelines can provide some partial guidance in this respect. They indeed state that "joint controllership may also occur between an EUI [European Union Institution] and an external actor (such as an external provider of a management portal or a national public authority etc.)." [93] Nevertheless, the EDPS discourages this scenario and encourages EUIs to make sure that private companies act as processors.[94]

89 European Data Protection Board (n 7) 17.

90 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (n 50) para 80.

91 European Data Protection Board (n 7) 21.

92 ibid. The fact that a joint determination of the essential means is necessary to qualify as joint controllers nonetheless transpires from the examples mentioned in pp. 20-22 of the EDPB's guidelines.

93 European Data Protection Supervisor (n 87) 22-23.

94 Since Regulation 2018/1725 on the "protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data" explicitly leaves room (in article 28.1) for a situation of joint control between EUIs and

38 Second, if we perform a factual assessment, what seemed to have played a crucial role in the aforementioned CJEU case law, particularly *Fashion ID*, was not as much the capacity to determine "why" and "how" personal data were processed, but merely "if" personal data were processed at all. This approach, focusing on enabling the processing of personal data by another party,[95] is confirmed in the EDPB guidelines, which stress that joint determination arises in the case of converging decisions or, in other words, when the "processing would *not be possible* without both parties' participation" (emphasis added) (see section B.III.3). The perils inherent to such a broad interpretation of the term "determining" are eloquently explained by Advocate General Bobek in its opinion in *Fashion ID.* There it states that, if one looks at the joint control test critically, "it seems that the crucial criterion after *Wirtschafstakademie Schleswig-Holstein* and *Jehovah's Witnesses*" seems to be "that the person in question '*made it possible*' for personal data to be collected and transferred, potentially coupled with some input that such a joint controller has on the parameters (or at least where there is silent endorsement of them)". "If that is indeed the case", he adds, "then in spite of a clearly stated intention to that effect to exclude it in *Wirtschafstakademie Schleswig-Holstein*, it is difficult to see how normal users of an online (based) application, be it a social network or any other collaborative platform, but also other programmes would not also become joint controllers".[96]

(arguably public and private) non-EUIs entities, it is disputable whether and, if yes, to which extent, this answer also applies to situations of joint control between a public and private entity/ individual falling under the GDPR. We therefore do not further consider this document for the purposes of the case-study presented below.

95 Chen and others (n 4) 284 refer to this approach as "joint-controllership by technical configurations".

96 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV joined parties: Facebook Ireland Limited* [2018], Opinion of Advocate General Bobek (n 1) para 73.

Component of the definition of joint controller		Ambiguity	
#1	Relevant processing operation	Unity of purpose as a criterion to circumscribe the relevant processing operation? If so, how to define purpose (see also **#3**)?	
		Stage of the processing operation as a criterion to circumscribe the relevant processing? If so, how to identify the relevant stage?	
#2	Personal data	Identifiability	Risk based and relative or zero-risk and absolute approach to the notion of personal data?
			Does the perspective from which identifiability is as-sessed when defining personal data (under Article 4(1) GDPR) predefine the candidates for the role of controller (under Article 4(7) GDPR)?
#3	Joint determination of purposes and means	Purposes	Each actor to pursue its "own purpose"? If so, how to define purpose (see also **#1**) ?
			What is the meaning of (i) identical, (ii) common, (iii) closely linked or (iv) complementary" purposes?
		Means	Each actor to pursue its "own purpose", when using technology developed by other entity? If so, how to define purpose (see also **#1**) ?
		Determinations	Does the legal designation of one controller exclude per se joint controllership between the legally designated controller and a factual one?
			When it comes to the notion of "converging decision", how extensively should the criteria of "making the data processing possible" be interpreted?

C. The household exemption: a way out?

39 The so-called "household exemption" exempts a natural person processing personal data "in the course of a purely personal or household activity" from the GDPR's scope of application (Article 2(2)c GDPR). It applies to processing operations that have no connection to "a professional or commercial activity", which could include, for instance, "correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities" (Recital 18 GDPR). Both the WP29 and the CJEU have had the opportunity to clarify the contours of that exemption, the scope of which has not drastically changed since the DPD (Article 3(2), second indent and Recital 12 DPD).

40 In its judgment in the *Lindqvist* case, the CJEU held that the household exemption was to be interpreted narrowly as "relating only to activities which are carried out in the course of [the] private or family life of individuals".[97] As pointed out by the Advocate General at the time, this would only cover "confidential activities that are intended to be confined to the personal or domestic circle of the persons concerned".[98] The household exemption, the Court added, would then clearly not apply to the "processing of personal data consisting in publication on the internet so [they] are made accessible to an indefinite number of people".[99] This was later reiterated by the Court in the *Satamedia* case.[100]

41 More recently, the CJEU also clarified that video surveillance, if partially "covering a public space" and therefore "directed outwards [...] the private setting of the person processing the data" would not fall within the scope of the household exemption.[101] In its detailed opinion, Advocate General Jääskinen discussed the distinction between personal activities—"which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others" and "may take place outside the home"—and household activities—"that are linked to family life and normally take place at a person's home or in other places shared with family members, such as second homes, hotel rooms or private cars".[102] While both types of activities fall within the scope of the household exemption, he also highlighted that the processing operations at stake must "exclusively" relate to either personal or household activities in order to benefit from the exemption.[103] The CJEU recently applied the above-mentioned criteria in its *Jehovah's Witnesses* judgment to exclude the taking of notes by Jehovah's Witnesses during door-to-door preaching from the scope of the household exemption.[104]

42 In its Opinion 5/2009 on online social networking, the WP29 detailed additional elements that should be taken into account when determining whether end-users of social network services ("SNSs") could rely on the household exemption. Among others, it stated that when "an SNS user acts on behalf of a company or association, or uses the SNS as a platform to advance commercial, political or charitable goals", the said exemption should not apply. Echoing the reasoning developed by the CJEU in *Lindqvist* and *Satamedia*, the WP29 also held that, "when access to profile information extends beyond self-selected contacts, such as when access to a profile is provided to all members within the SNS [...]", it goes beyond the personal or household sphere.[105] Same goes for a user who takes the "informed decision to extend [such] access beyond self-selected 'friends'".[106]

43 As already remarked by other scholars,[107] there is a tendency to interpret the household exemption

97 Case C-101/01 *Bodil Lindqvist v* Åklagarkammaren *i* Jönköping [2003] ECLI:EU:C:2003:596 para 47.

98 Case C-101/01 *Bodil Lindqvist v* Åklagarkammaren *i* Jönköping [2003], Opinion of Advocate General Tizzano ECLI:EU:C:2002:513, para 34.

99 Case C-101/01 *Bodil Lindqvist* (n 97) para 47.

100 Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy* [2008] ECLI:EU:C:2008:727 para 44.

101 Case C-212/13 *František Ryneš v* Úřad *pro ochranu osobních* údajů [2014] ECLI:EU:C:2014:2428 para 33.

102 Case C-212/13 *František Ryneš v* Úřad *pro ochranu osobních* údajů [2014], Opinion of Advocate General Jääskinen ECLI:EU:C:2014:207, para 51.

103 ibid para 53. This, he added when discussing whether the collection of video footages could qualify as 'purely' household activities, would not be the case 'when the processing involves 'persons who have no connection with the family in question and who wish to remain anonymous' (ibid para 56).

104 Case -25/17 *Tietosuojavaltuutettu intervening parties: Jehovan todistajat — uskonnollinen yhdyskunta* (n 62) para 41-45.

105 Article 29 Working Party, 'Opinion 5/2009 on online social networking' (2009) 6 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf> accessed 21 April 2021.

106 ibid.

107 Chen and others (n 4) 279-293.

increasingly narrowly. As will be seen below, this can lead to an increase of situations where a natural person qualifies as (joint) controller under the GDPR.

D. The case study: hypothesis, objective, methodology and limitations

44 One of the distinctive features of a decentralised architecture is to distribute the processing of personal data across multiple devices, rather than centralizing everything through the use of a single server. Decentralised systems are often presented as more privacy-friendly alternatives to centralised solutions since they eliminate the need to trust a single entity.[108] Yet, such systems also scatter the processing operations across multiple parties, therefore raising the issue as to the role and qualification of these actors under EU data protection law. More specifically, as will be seen below, one of the main differences between centralized and decentralized COVID-19 proximity tracing solutions is that under the decentralized protocol more processing operations take place at the edge, i.e. on the app user's mobile phone, rather than on a central (back-end) server. As hinted above, in relation to a case-study concerning security/privacy preserving edge computing solutions adopted in smart home Internet of Things, scholars have already argued that the current broad notion of joint control, coupled with the narrow interpretation of the household exemption, may end up "unfairly burdening certain stakeholders in smart homes", [109] including the smart home user, and "disincentivise uptake" [110] of security/privacy preserving edge computing solutions. We inquire whether this conclusion could, in theory, also hold true in the case of privacy-preserving decentralized solutions such as those applied in COVID-19 digital proximity tracing.

45 We postulate that the more actors involved in the processing of personal data, the more parties are likely to bear a certain degree of responsibility under the GDPR including, potentially, end-users themselves. Applied to the case of COVID-19 apps, the hypothesis is hence that end-users will be considered joint controllers with the national health authority for certain processing operations in a decentralised approach. To understand whether the architecture of the protocol has an impact on the outcome, we also analyse the role of the app user under centralized solutions. We investigate this by applying the broad legal framework for joint control emerging from the analysis presented in sections B and C of the paper to the following use-cases: the ROBust privacy-presERving proximity Tracing ("ROBERT") protocol, which is an instance of a centralised COVID-19 app, and the Decentralised Privacy Preserving Proximity Tracing ("DP-3T") protocol, which adopts a decentralised approach. These publicly available protocols[111] and accompanying privacy and security impact analyses[112] were used to illustrate the main features of the centralised and decentralised approaches.

46 In light of the above, the following main research question is examined: given the broad interpretation of joint control, could app users qualify as controllers under the GDPR, jointly with the legally designated controller (*i.e.* in most cases, the national health authority), with regard to the processing of other app users' personal data? If the answer is positive, we examine the following additional questions. First, does the answer to the first question differ depending on the centralised or decentralised nature of the tracing solution? Second—given that, as mentioned above (section B), we believe that one should first assess whether the data at issue is personal (and more specifically, identifiable) in order to allocate (joint) control—do the processing operations with respect to which the (joint) controller exercises control always qualify as operations on personal (hence identifiable) data from the perspective of that controller?

47 The study admittedly suffers from the following limitations. First and foremost, we do not intend to cover the full spectrum of responsibilities arising

108 Primavera de Filippi, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' (2016) 9 Journal of Peer Production 4 < https://hal.archives-ouvertes.fr/hal-01382006/document> accessed 21 April 2021.

109 Chen and others (n 4) 293.

110 ibid.

111 PRIVATICS team INRIA and AISEC FRAUNHOFER, 'ROBERT: ROBust and Privacy-PresERving Proximity Tracing v.1.1' (2020) <https://github.com/ROBERT-proximity-tracing/documents/blob/aa1921f0006fcebd35bc30eeb765b22e45027a62/ROBERT-specification-EN-v1_1.pdf> accessed 21 April 2021; Carmela Troncoso and others, 'Decentralised Privacy-Preserving Proximity Tracing - Version 25 May 2020' (2020) < https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf > accessed 21 April 2021.

112 PRIVATICS team INRIA, 'Proximity Tracing Approaches Comparative Impact Analysis v1.0' (2020) <https://github.com/ROBERT-proximity-tracing/documents/blob/master/Proximity-tracing-analysis-EN-v1_0.pdf> accessed 21 April 2021; DP-3T Project, 'Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems' (2020) <https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf> accessed 21 April 2021.

from concrete digital proximity tracing solutions adopted in the fight against COVID-19. Indeed, we did not delve into any concrete implementation of the two abovementioned protocols by States. Similarly, the specific design features of each protocol were left out of the scope of the analysis. Our analysis focuses on the main differences between two distinct architectures, rather than on a specific app, and aims at highlighting the challenges and, at times potentially paradoxical consequences, stemming from the rigorous application of the criteria of joint control to the specific case of the app user in the two protocols under consideration. Second, we qualified the data as "personal" and allocated control on the basis of a selected list of processing operations on other app users' EphIDs and the assumption that the backend server is operated by the same public entity (*i.e.* the national health authority) that operates the overall application. Third, we do not have an academic or professional background in software engineering nor cryptography. The reasoning and findings presented in this paper are therefore entirely based on the documentation made available by the two consortia behind the selected protocols.

E. Centralized v. decentralized approach to digital contact tracing

48 Broadly speaking, COVID-19 apps work as follows. When two individuals cross each other's path, both apps (i) broadcast their own Ephemeral Identifiers ("EphIDs")—that is, the piece of information generated by either the backend server or the end-user's device to allow proximity tracing—and (ii) collect and store the EphIDs of nearby app users. If app users are tested positive to COVID-19, they have the possibility to inform the backend server that they are infected and, in a centralised approach, to share their recent encounters. This information is then used to (i) calculate the risk that someone has been infected following an encounter with an infected user and (ii) should that risk reach a certain threshold, inform that person of the procedure to follow. Below, we outline the necessary technical details that support the assessment performed in section F.

I. Who? The actors involved in BLE-based digital proximity tracing solutions

49 From an architectural point of view, the analysed COVID-19 apps rely on two main components: a terminal equipment (*i.e.* the app user's mobile device) and the back-end server.[113] In the present paper, we start from the postulate that the national health authority is operating the backend server, as part of the app system.[114] For the legal analysis deployed in section F, we therefore assimilate the national health authority with the app operator and the backend server, and consistently refer to the latter, as its role is extensively detailed in the documentation of both investigated protocols. The exact relationship between the national health authority, the backend and app operator(s) and other actors such as for example the app developer is, therefore, excluded from the scope of the present contribution. Instead, we focus on the following actors.

50 First, the *app users*, *i.e.* all the individuals who have downloaded and installed the app. For the purpose of our analysis, they can be further divided into the following categories:[115] (i) the *diagnosed* users, who are infected with COVID-19 and have been diagnosed positive to it; (ii) the *at risk* users, who have been in the proximity of a diagnosed user in the period during which the latter was contagious; (iii) the *exposed* users, who have been notified that they have been in the proximity of a diagnosed user.

51 Second, the *national health authority*, *i.e.* the entity that, in each country, is tasked with the implementation and supervision of the policies related to public health. According to the EDPB's Guidelines 04/2020, national health authorities could potentially be regarded as the controllers for the deployment of digital proximity tracing apps, although "other controllers may also be envisaged".[116] As highlighted

113 It is worth noting that both the centralised and decentralised approaches to digital proximity tracing described in this paper rely on a backend server. Its role within the functioning of the tracing system as well as the amount of information that transits through it, however, significantly differs depending on the approach.

114 This seems to be the approach adopted in Switzerland, where the backend(s) are "under the direct control of the Federal Office of Public Health (FOPH) and are operated technically by the Federal Office of Information Technology, Systems and Telecommunications (FOITT)". See FOPH, 'Data Protection Statement of the Federal Office of Public Health FOPH in connection with the use of the "SwissCovid app"' (2020) <https://www.bag.admin.ch/dam/bag/en/dokumente/cc/kom/swisscovid-app-datenschutz.pdf.download.pdf/FOPH_SwissCovid_Data_Protection_Statement_24_June2020.pdf> accessed 21 April 2021.

115 This taxonomy is mainly based on: PRIVATICS Team INRIA (n 112) 4.

116 European Data Protection Board, 'Guidelines 04/2020 on the use of location data and proximity tracing tools in the context of the COVID-19 outbreak' (2020) 7 <https://edpb.europa.eu/

above, we assimilate the national health authority with the *backend server*, *i.e.* the entity that manages the server used to support the functioning of digital proximity tracing, be it in a centralised or a decentralised solution.

II. How? The functioning of BLE-based digital proximity tracing solutions

52 Broadly speaking, the functioning of the digital proximity tracing solutions under consideration can be broken down into four distinct phases.[117] The decentralised and centralised approaches are illustrated in Figure 1 and Figure 2, respectively.

- *Phase 1 – Installation of the app.* In this initial stage, the users download the app on their mobile phone from an official app store. In the centralised protocol, the app users register with the backend servers which then generates a permanent identifier that does not, as such, reveal the identity of the individual.[118] On the basis of that identifier, the backend server then creates and pushes several EphIDs to the app user's device using its own, periodically renewed global key.[119] In a centralised scenario, the backend server uses its own rotating global key to derive the EphIDs from the permanent identifier created when the app user registered with the backend server for the first time. In the decentralised protocol, the EphIDs are generated pseudo-randomly by each app user's mobile phone on the basis of its own periodically changing secret key.[120]

- *Phase 2 – Broadcasting of the app user's own EphIDs and collection of other app users' EphIDs.* In this phase, each app user's phone broadcasts its own EphIDs and collects and subsequently stores the EphIDs of other app users in the vicinity. This process is identical under the centralised and decentralised approach.

- *Phase 3 – Testing and declaration of infection.* If users test positive to COVID-19, their phone transmits the information necessary for phase 4 to the backend server. The type of information provided differs depending on the nature of the tracing solution. Under the centralised protocol, the diagnosed users transmit the EphIDs of at-risk users collected during phase 2. Under the decentralised approach, however, the diagnosed users only upload their own EphIDs broadcasted during the infectious time window.[121]

- *Phase 4 – Matching and computation of the risk score.* The backend server then processes the information obtained in phase 3 in order to notify at-risk users. Again, this process differs depending on the nature of the app. Under the centralised approach, the matching of a diagnosed user and at-risk users and the computation of the risk-score are performed on the backend server.[122] Under the decentralised protocol, the matching and calculation occur on the phone of the at-risk users.[123]

sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf > accessed 21 April 2021.

117 Carmela Troncoso and others, 'Decentralized Privacy-Preserving Proximity Tracing – Overview of Data Protection and Security' (2020) 11 <https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf> accessed 21 April 2021; PRIVATICS team INRIA and AISEC FRAUNHOFER (n 111) 4.

118 The permanent identifier is defined by the ROBERT consortium as a "permanent and anonymous identifier associated to each registered user". See PRIVATICS team INRIA and AISEC FRAUNHOFER (n 111) 15.

119 ibid 4.

120 Troncoso and others (n 117) 6–7. In a decentralised scenario, the key on the basis of which the EphIDs are created is assigned by the app user's device itself, with no intervention from the backend server.

121 More specifically, under the DP-3T protocol, the diagnosed user provides the backend server with the secret key corresponding to the first day in which he was considered infectious. The backend server will then be able to retrieve all EphIDs broadcasted by the diagnosed user's phone during the contagious window. See Troncoso and others (n 111) 16–17.

122 More specifically, the backend server retrieves the permanent identifiers of the at-risk users whose EphIDs have been uploaded by the diagnosed user during phase 3. On the basis of several parameters such as the amount of time they were exposed to the diagnosed user, the backend server then calculates the risk-score of the at-risk users. If that risk reaches a given threshold, the backend server notifies them that they have been exposed to a diagnosed user and informs them of the procedure to follow.

123 Here, each app user's phone periodically downloads the diagnosed users' EphIDs from the backend server and verifies whether those EphIDs appear in the records of EphIDs collected and stored during phase 2. If this is the case, the at-risk user's phone computes the risk score on the basis of a number of parameters and, should the risk reach a certain threshold, notifies the app users that they have been in contact with a diagnosed user, together with further instructions.

Table 2 - Explanation of the pictograms used in the various figures

App user	Diagnosed app user	Backend server	Secret key used to generate EphIDs	Matching and computation of the risk score

Figure 1 - Decentralised approach to digital proximity tracing

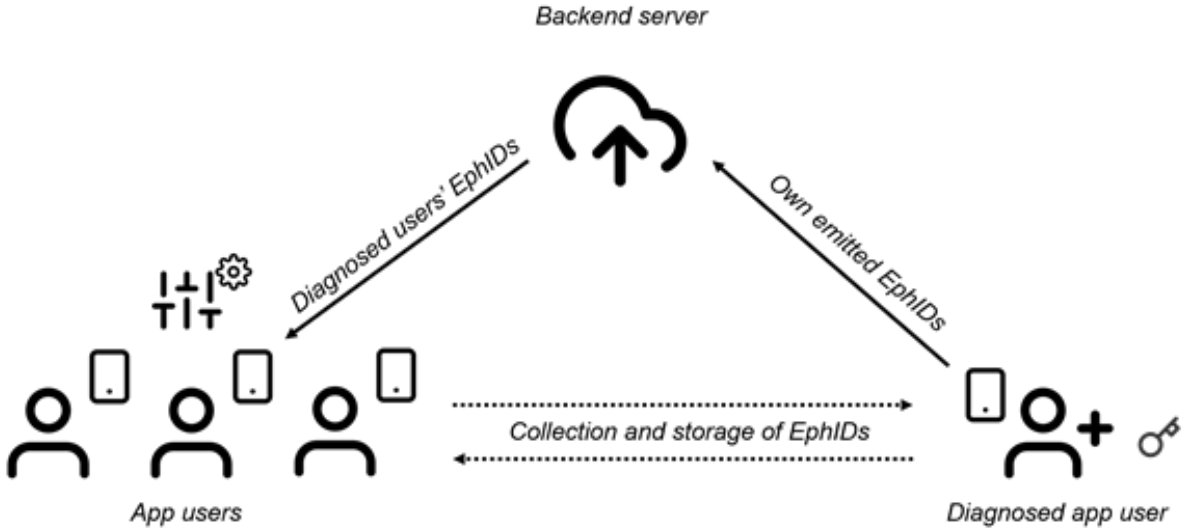
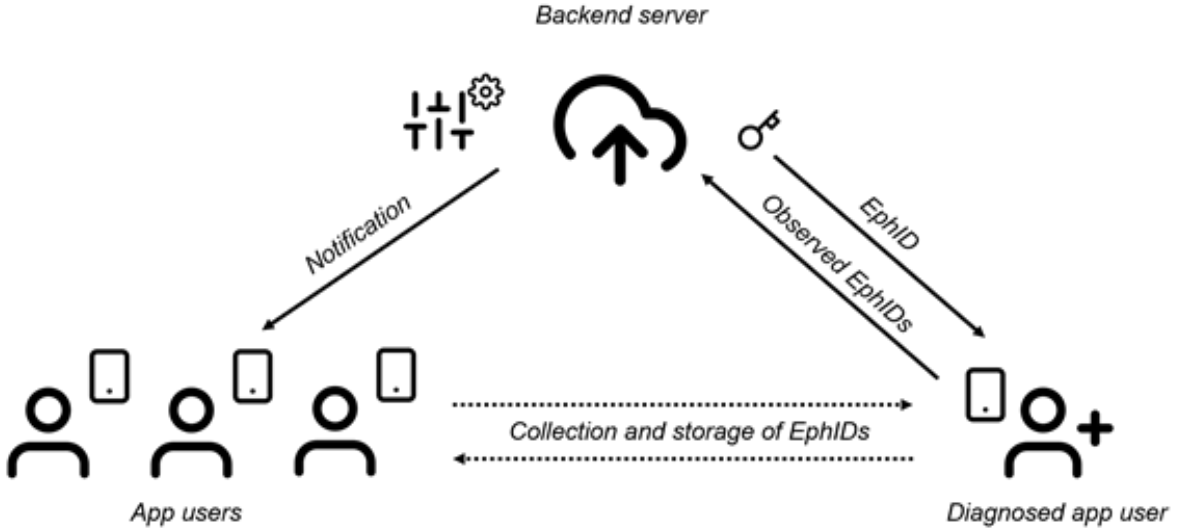


Figure 2 - Centralised approach to digital proximity tracing



F. The app user as joint controller ?

53 In the following section, we illustrate the complexities of the legal test for joint control, by focussing on the role of the app user under the GDPR in the ROBERT and DP-3T protocols. Although the appointment

of the controller is done by law in most European countries[124] (and coincides with the national health authority), we look at whether the app user could qualify as joint controller with the legally appointed controller, when it comes to the processing of other app users' EphIDs. Where pertinent (see section F.I.4 below), we also go beyond the legal fiction, to illustrate (as announced above, see in section B.IV.2) one of the implications of combining the assessment concerning the "identifiability" of personal data with the one relating to (joint) controllership. Namely, an actor could potentially qualify as a (joint) controller of data that, from that actor's perspective, are not personal.

54 Before delving into the following paragraphs, it is necessary to emphasise once again that the present contribution does not intend to confirm or deny any pre-existing claim as to the qualification of end-users as joint controllers in the context of COVID-19 digital proximity tracing apps. Rather, this eventually emerged from the application of the current regulatory framework and available guidance on the notion of joint control to the two protocols at stake.

124 Belgium, for example, has appointed Sciensano, the public institution tasked—at the federal, community and regional levels—with various missions related to public health, as the controller for the processing operations relating to the Coronalert app (Arrêté Royal n° 44 du 26 juin 2020, art. (14,§3,3°)). Switzerland, for instance, has designated the Federal Office of Public Health (Office Fédéral de la Santé Publique) to act as the controller with regard to the SwissCovid app (Ordonnance 818.101.25 sur le système de traçage de proximité pour le coronavirus SARS-CoV-2 du 24 juin 2020, art. 4). In France, the Health Ministry bears the controllership of the StopCovid app (Décret n° 2020-650 du 29 mai 2020 relatif au traitement de données dénommé "StopCovid", Art. 1). In Italy, the Ministry of Health is the controller for the processing operations happening in the context of the Immuni app (Decreto-Legge 30 aprile 2020, n. 28. Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19, Art. 6.1).

I. The processing of other app users' personal data

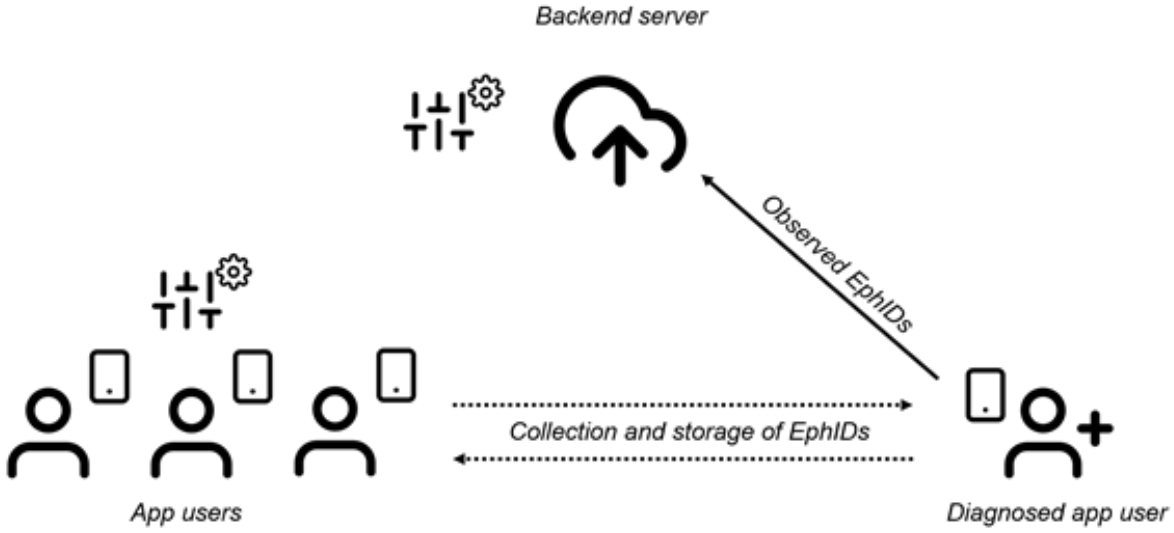
1. Step 1: the relevant processing operations

55 As a preliminary step, it is necessary to identify the processing operations in light of which the allocation of responsibilities is to be performed. Article 4(2) GDPR defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". To keep the scope of the investigation manageable, and since we want to assess the role of the app user in relation to the processing operations on other app users' personal data (not their own personal data), we limit ourselves to considering the processing operations that are performed on the other app users' EphIDs.[125] This narrows the scope of the analysis down to the following processing activities (Figure 3):

- In both the centralised and decentralised scenarios: the collection and storage by a given app user's phone of EphIDs of other app users (phase 2);
- In the centralised scenario: the transmission by the diagnosed app-user of EphIDs of at-risk app users to the backend server (phase 3) and the subsequent use of these EphIDs by the backend server to compute the at-risk users' risk-score (phase 4);
- In the decentralised scenario: the use by each app user's phone of the diagnosed user's EphIDs in order to match these EphIDs with the observed ones and the use by the at-risk app user's phone of the diagnosed user's EphIDs, in order to compute the app user's risk-score (phase 4).

125 Therefore, we discarded the following processing operations as irrelevant for the analysis: the generation of an app user's own EphIDs (and permanent identifiers in the centralised protocol) which occurs during the installation of the COVID-19 app (phase 1 above); the processing operations occurring during the upload of the diagnosed user's own EphIDs on the backend server (phase 3 of the decentralised protocol).

Figure 3 - Processing operations relevant for the analysis



56 It is crucial to determine whether all these processing operations are relevant when assessing control. This shows a first difficulty stemming from the application of the criteria for joint control mentioned above. On the one hand, if we approach the individual processing operations from a *macro-perspective* and adopt the unity of purpose as a criterion for identifying the relevant processing operations, it is plausible to argue that these operations all share the same purpose, namely notifying the app user of an exposure to a diagnosed user. This is the case in both the centralised and decentralised approaches. Such purpose serves both a public interest (*i.e.* preserving public health) but also a private one (*i.e.* preserving each individual user's health). As a result, all these processing operations would be considered as a set of operations and, provided they concern personal data, would all be relevant to assess the role of the app user under the GDPR.

57 On the other hand, it would be equally plausible to define the purpose of the processing operations more granularly, at a *micro-level*. For instance, in a centralised scenario, the purpose of the collection and storage of other app users' EphIDs (phase 2) is the transmission of these EphIDs to the backend server, should the user at issue become infected (phase 3). Similarly, in a decentralised protocol, the use by an app user's phone of the diagnosed user's EphIDs aims at matching these EphIDs with the observed ones and, should a match occur, calculating the risk-score (phase 4).

58 In short, it always seems possible to reduce the purpose of each processing operation to the subsequent stage of the processing that that operation is intended to enable, thereby losing sight of the overall purpose that connects each stage of the processing.[126] This exemplifies the problem identified in section B.IV.1 and table 1 above as to the level of granularity with which the purpose(s) of the processing should be defined.

59 The identification of the relevant processing operations is likely to become even more unpredictable if we abandon the unity of purpose as a criterion and adopt a "phase-oriented"[127] approach to identify the relevant processing operations, like the CJEU seems to have done in *Fashion ID*. In that case, limiting the relevant processing operations to any phase of the processing runs the risk of leading to an artificial representation of the processing operations that lacks any objective rationale.

2. Step 2.1: the qualification of other users' EphIDs as personal data - criteria

60 Next, it is crucial to determine whether the processing activities identified in the preceding paragraph are performed on "personal data". For the purposes of this contribution, we only focus on the identifiability criterion and hence assume that EphIDs can qualify as "any information relating to a natural person" (Article 4 (1) GDPR). Since, as

126 See similarly: Mahieu and van Hoboken (n 80).

127 ibid.

highlighted in section B.II.2, we consider the relative and risk-based approach as the most sensible approach to personal data, we assess the nature of the EphIDs under this approach. We do so on the basis of the criteria provided by the privacy and security risks analyses performed by the members of the ROBERT and DP-3T consortia, namely:

- The likelihood of re-identification threats assessed by the members of the ROBERT consortium under a centralised and decentralised approach on the basis of (i) their feasibility (which "depends on the weaknesses of the system and the technical means and expertise of the risk-source") and (ii) motivation of the attacker.[128] When the ROBERT consortium rated such likelihood as "significant" or "maximal", we considered that the EphIDs at issue could qualify as personal data. Moreover, when such likelihood was also implicitly assessed by the members of the DP-3T consortium, their assessment was also taken into account.[129]

- The risk source,[130] which refers to the actor that could pose the relevant threat, as identified by the members of the ROBERT consortium. When the source of the risk is another (tech-savvy or regular) app user, we considered that the EphIDs at issue could be personal data from the perspective of the app-user.[131] When such actor coincides with the operator of the back-end server or a person that could be deemed reasonably likely to be approached by the backend server, such as another State authority, we considered that the EphIDs at issue could qualify as personal data from the perspective of the backend server.

61 Based on these criteria, and without questioning the exactitude of the findings of the two consortia, the following EphIDs could qualify as personal data for the purposes of this analysis (see Table 3 below).

3. Step 2.2: the qualification of other users' EphIDs as personal data – perspective of the app user

62 Since we are interested in knowing whether the app user could qualify as a joint controller with the legally designated controller, we first consider the perspective of the app-user.

63 From this perspective, the diagnosed users' EphIDs could qualify as personal data. The ROBERT and DP-3T consortia point out that, in both the centralised and decentralised protocols, diagnosed users' EphIDs are vulnerable to re-identification attacks performed by *other app users*. The ROBERT consortium lists the following risks.[132] First, there is a risk that a "tech-savvy user" identifies "all infected individuals among encounters", which occurs "when the adversary is able to find diagnosed users among all persons he has encountered during [the] contagious period".[133] In this scenario, the attacker proceeds "by collecting pseudonyms of each person encountered, and then correlating this list of pseudonyms with the list of infected users' pseudonyms published by the authority to determine when she was in contact with an infected person and use this information to reveal the identity of the infected".[134] This attack, the members of the ROBERT consortium add, "only concerns the decentralised approach and is not possible in the centralised approach".[135] Second, there is a risk that a "regular user" identifies "a targeted infected individual".[136] This risk is materialised "by turning on the Bluetooth interface when in presence of the targeted individual, alone, then turning it off".[137] It is described as being "also possible in centralised approaches when the set of encounters of the user is limited to the target only"[138] or in other more costly scenarios, such as when the attacker creates "an instance of the application (registered on the server) for each encountered person".[139]

128 PRIVATICS Team INRIA (n 112) 5.

129 We specifically refer to the evaluation by the members of the DP-3T consortium of the nature of EphIDs as pseudonymous data vis-à-vis the backend server in a centralised scenario (DP-3T Project (n 112) 18).

130 PRIVATICS Team INRIA (n 112) 5.

131 The legality criterion as put forward in the *Patrick Breyer v Bundesrepublik Deutschland* case (see section B.II.2) is not taken into account for the purposes of this assessment, since it requires a knowledge of the national legal context in which the COVID-19 app is implemented, which is beyond the scope of this analysis.

132 PRIVATICS Team INRIA (n 112) 7–8.

133 ibid 7.

134 ibid. 7-8.

135 ibid 8.

136 ibid.

137 ibid.

138 ibid.

139 ibid 7,8.

64 Similarly, although they do not explicitly assess the likelihood of this attack and define it as a risk inherent to proximity tracing systems that notify users that they are at risk, the members of the DP-3T project state that there is a risk that a "motivated attacker identifies the infected people that he has been physically near".[140] This could be done by "combining two pieces of information: (1) who [he] interacted with at each time, and (2) that [he was] in close proximity to an infected person at a specific time".[141] To learn who he interacted with, "the attackers keep a log of personal interactions. To learn "at which time he interacted with an infected person, the attacker proceeds in two steps: first, [he] creates multiple accounts in the proximity tracing system and uses them only for a short time [...]; second, if a notification arrives, he examines the corresponding account. Since the account was only used during a fixed time window, the attacker now knows that he was in close proximity to an infected person during that period".[142] Then, "by combining information from multiple time windows, the attacker can narrow down their list to a small group of people and, in some cases, single out infected individuals".[143] In some cases (such as for example when the user had contacts with a very limited number of people), re-identification of the infected individual is even possible "without additional data gathering" .[144]

65 Since the ROBERT consortium rates the aforementioned attacks as "significantly likely" to be performed,[145] the diagnosed users' EphIDs could be considered as personal data from the perspective of both the *exposed* and the *at risk app users*, under both a centralised and a decentralised approach. *Exposed app users*, as discussed in relation to the *Breyer* case in section B.II.2, are actually able to perform the re-identification attacks outlined above given that they have received a notification of exposure. *At risk app users*, in turn, could potentially be notified of an exposure, thereby becoming an exposed app user and thereby acquiring the means to identify diagnosed users on the basis of their EphIDs. The functioning of digital proximity tracing indeed makes the latter possibility "reasonably likely" to happen, even though the EphIDs of diagnosed users would only actually become identifiable to the at-risk app users after they have received that notification (Table 3 below).

66 By contrast, since both the re-identification attacks described above can only be performed once an individual has been diagnosed positive to COVID-19,[146] the EphIDs of other app users would not qualify as personal data from the perspective of the app user.

67 It follows that, from the perspective of the app user, the following processing operations would qualify as processing operations on personal data:

- *in both the centralised and decentralised protocol: the collection[147] and storage by an at-risk or exposed app user's phone of diagnosed users' EphIDs (phase 2);*
- *in the decentralised protocol: the use by an at-risk or exposed app user's phone of the diagnosed users' EphIDs in order to (potentially) match these EphIDs with the observed ones, and, subsequently, for purposes of risk-score computation (phase 4).*

4. Step 2.3: the qualification of users' EphIDs as personal data – perspective of the backend server

68 While the backend server (as explained above) is usually appointed by law as the controller, and the rest of the analysis considers the backend server's role as a controller as a given, in this paragraph we go beyond that legal fiction, to assess whether the users' EphIDs would also qualify as personal data from the backend server's perspective. We do so to illustrate one of the implications of combining the assessment of the "identifiability" of personal data with the one concerning (joint) controllership: potentially, an actor could qualify as a (joint) controller of data that, from that actor's perspective, are not personal.

69 We first consider the diagnosed users' EphIDs. When it comes to the centralised approach, it

140 DP-3T Project (n 112) 5.

141 ibid.

142 ibid.

143 See, for a fictional example: ibid.

144 ibid 6.

145 PRIVATICS Team INRIA (n 112) 7–8.

146 ibid.

147 If, as argued by some authors such as Finck and Pallas (n 9) 17, one assumes that "data becomes personal [only] at the moment that identification becomes possible", then we would have to discard collection as a relevant processing operation since, at that stage EphIDs are not identifiable yet but become identifiable only once the at risk app user has received the exposure notification (which means that - by definition - there is no collection of relevant EphIDs anymore). However, to avoid further complicating the already complex analysis, we considered collection as a relevant processing operation for the purpose of this contribution.

seems that the two consortia disagree on whether the backend server would be reasonably likely to re-identify the diagnosed individuals. According to the authors of the DP-3T protocol, the backend server can associate the EphIDs with their corresponding permanent identifiers, which could then "easily be related back" to their real identities.[148] Although the DP-3T members do not assess the likelihood of this event occurring, it follows that diagnosed users' EphIDs would qualify as personal, albeit pseudonymous, data.[149] The ROBERT consortium does not specifically discuss the likelihood of such re-identification attacks in a centralized protocol. However, it estimates the likelihood of attacks that could potentially lead to indirect re-identification (e.g. linkability of identifiers on the server or location tracing through access to the sever) as "limited",[150] in which case the diagnosed users' EphIDs would not qualify as personal data. By contrast, while this contribution does not intend to assess the exactitude of the claims made by both consortia, it seems that, in a decentralised approach, the backend server is not in a position to link the diagnosed users' EphIDs back to their identifiable form, since those are generated pseudo-randomly using the secret key created and stored on the app user's phone itself.[151] As such, they would not qualify as personal data vis-à-vis the backend server.[152] While, one might argue that such a conclusion has been implicitly endorsed by the recent case law of the CJEU according to which access to the personal data is not a prerequisite to qualify as a controller, this nonetheless raises the issue as to the relationship between the entities through which the risk of re-identification must be assessed and the ones that determine the purposes and the means of the processing. As hinted in section B.IV.2, the findings of the CJEU and the EDPB seem to indicate that the question of the allocation of responsibilities should be dissociated from the one related to the existence of a processing of personal data. As a result, one might end up in a situation—like here—where a given entity determines the purposes and the means, and therefore acts as controller, of a processing of data that qualify as personal from the perspective of another entity, but not its own.

148 DP-3T Project (n 112) 18.

149 ibid.

150 See more specifically "LR2: Linkability of identifiers on the server" and "SR7: location tracing through access to a central server" in PRIVATICS Team INRIA (n 112) 12, 13.

151 Troncoso and others (n 117) 7. See similarly: "SR 11: Re-identification of all infected users [new]" in PRIVATICS Team INRIA (n 112) 11.

152 This conclusion is supported by the Data Protection Impact Assessment carried out on the DP-3T protocol: "Therefore, it must be considered, in line with the principles laid down above, and the test set out in Breyer (C-582/14, § 43), that the information stored on the backend server cannot be characterised as personal data from the point of view of the operator of the backend server." Id-Est avocats, 'Data protection impact assessment report" (2020) 17 < https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf> accessed 21 April 2021.

70 Second, the other app users' (*i.e.* the non-diagnosed users') EphIDs could qualify as personal data from the perspective of the *backend server*. Indeed, the conclusion drawn above as to the qualification of diagnosed users' EphIDs would be equally applicable to other app users' EphIDs.

Table 3- EphIDs as data relating to an identifiable individual

Data	Perspective	Centralised COVID-19 app	Decentralised COVID-19 app
Diagnosed users' EphIDs	Backend server	Yes (DP-3T) / No (ROBERT)	No
	At risk and exposed app user	Yes	Yes
Other app users' EphIDs	Backend server	Yes (DP-3T) / No (ROBERT)	No
	App-user	No	No

II. Step 3: the joint participation in the determination of the purposes and means

71 As stated above, we take it as a given for this part of the analysis that the backend server, which we assimilate with the national health authority, acts as a controller by virtue of its legal appointment. The question that we intend to answer is whether the app user can be said to determine the purposes and the essential means of the processing *jointly* with the authority and, hence, act as joint controller with the latter in relation to the relevant processing operations identified in section F.I.3. above.

72 As mentioned above, when it comes to assessing joint controllership, each entity must first pursue a purpose "of its own"[153] and, hence, qualify as a controller in its own right. Only then is it possible to analyse whether the entities might *jointly* exercise influence on the purpose and means of such processing and hence qualify as joint controllers. As argued in section B.IV.1 and B.IV.3, the definition

153 European Data Protection Board (n 7) 21.

of "purpose" and "determining" will significantly impact the outcome of that assessment. The purpose of the processing operations could be defined as notifying at risk app users of a potential exposure to the virus. It could be argued that, by merely engaging in the aforementioned processing operations, the app users simply participate to the functioning of a system that was designed and adopted by somebody else to achieve that goal.[154] In that sense, the app user would not exercise any influence on the said purpose.

73 However, "determining" could also be defined more broadly as in materially contributing to certain processing operations and, consequently, allowing them to take place. In that sense, it can be argued that digital proximity tracing, and more specifically, the abovementioned processing operations, "would not be possible"[155] without the participation of the app user, who needs to install the app and turn it on when they are in the presence of other app users. Moreover, instead of merely looking at the objective purpose of the processing operations at issue, the purpose could be interpreted as the motivating factor driving each entity involved in the processing, as suggested by the relevant case law of the CJEU and the EDPB (see section B.IV.3 above). In this case, the app users could be said to pursue a purpose "of [their] own", *i.e.* preserving their own health or limiting the spread of the disease across their private circle of friends and relatives. This purpose can be regarded as "closely linked" or "complimentary" to the purpose arguably pursued by the legally designated controller, *i.e.* containing the virus and/or protecting the public healthcare system from saturation. Consequently, the processing operations at issue appear to mutually benefit the app users and the legally designated controller.

74 When it comes to the joint determination of the essential means, it has been argued that, since the app user does not have any configuration option, they cannot determine the "how" of the processing.[156] In other words, and to establish a parallel with the decision of the CJEU in *Wirtschafstakademie*, the app user does not have a say regarding the criteria (*i.e.* in the context of digital proximity tracing, the type of data collected, the retention period or the elements used to calculate the risk score, for instance) surrounding the functioning of the proximity tracing solution. Again, while this may be true under a strict interpretation of "determining the means", it may be at odds with the approach put forward in *Fashion ID* and the EDPB's Guidelines. That approach indeed indicates that the joint determination of the means could follow from an entity's choice to use a tool developed by another entity for its "own purposes".[157] By analogy, it could be said that app users jointly determine the means of the processing, by choosing to use a proximity tracing tool which was developed by another entity and which triggers the processing of other individuals' personal data for their *own* (private) purpose.

75 To conclude, if we look at the processing operations identified in section F.I.3 as a set of operations and consider the backend server and the app user as pursuing distinctive "own" purposes, they could be said to take "converging decisions" within the meaning of the EDPB's guidelines. Indeed, the processing operations at stake "would not be possible"[158] without, besides the participation of the legally designated controller, the participation of the app user, who needs to install the app and turn it on when they are in the presence of other app users.

III. Step 4: the "household exemption"?

76 Since, given the outcome of the analysis performed in sections F.I and F.II, app users could potentially qualify as joint controllers in relation to certain processing operations on other users' personal data, it is necessary to verify whether they could benefit from the so-called "household exemption".

77 First, it is worth noting that the processing operations detailed in section F.I.3 are unlikely to fall within the scope of "household" activities since they extend far beyond the app user's home or other places shared with his family members.[159] This is inherent to the functioning of digital proximity tracing solutions that are based on an app designed to be used on the go and holds true under both a centralised and decentralised scenario.

78 Second, the same could be said when it comes to their qualification as "personal" activities, although following a different line of thinking. As

154 See, for instance: Kirsten Bock and others, 'Data Protection Impact Assessment for the Corona App' (2020) SSRN Electronic Journal 48 <https://www.ssrn.com/abstract=3588172> accessed 21 April 2021.

155 European Data Protection Board (n 7) 19.

156 Bock and others (n 154) 48.

157 European Data Protection Board (n 7) 21.

158 ibid.

159 Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014], Opinion of Advocate General Jääskinen (n 102) para 51.

highlighted in section F.II, the collection, storing and, in a centralised solution, transmission of at risk app users' EphIDs serves both a general, public health-related and a private, more individualistic purpose. For that reason, one could argue that those processing operations do not "purely" relate to personal activities, regardless of their qualification as "personal". Given the privacy risks stemming from the use of both centralised[160] and decentralised[161] solutions, it is also difficult to argue that those processing operations do not "impinge upon the personal sphere of others",[162] even though the EphIDs of at-risk app users transmitted by the diagnosed app users to the backend server in a centralised scenario are not made accessible to an indefinite number of people. While irrelevant given the dual nature of those purposes, the question as to whether the interference is "significant" enough as to rule out the applicability of the household exemption remains subject to a case-by-case analysis.[163] Given the above, it is fairly reasonable to assume that the app user would not be able to rely on the household exemption.

G. The patchwork of answers

79 The first research question of this case-study was whether, given the broad interpretation of joint control, app users could qualify as controllers under the GDPR jointly with the legally designated controller (*i.e.* the national health authority, in most cases), with regard to the processing of other app users' personal data. If, as argued under section F.II, we take the view that app users pursue a purpose of their "own" when using the COVID-19 app (*e.g.* preserving their own individual health), and consider this purpose as being closely linked or complimentary to the one pursued by the national health authority (*e.g.* preserving public health), app users could qualify as *joint controllers* with the national health authority with respect to the processing operations identified in section F.I.3 (Tables 4 and 5 below). In that case, it is unlikely that these users would be able to rely on the household exemption laid down in Article 2(2)c GDPR. By contrast, if we consider that the app users do not pursue a purpose of their "own", the national health authority would qualify as a *sole controller* vis-à-vis the relevant processing operations by virtue of its legal designation (Tables 4 and 5 below). In essence, a lot will depend on the interpretation of open-ended notions such as "purpose" and "determining".

80 Second, and since the answer to the first research question can, at least in theory, be positive, we also wanted to know whether that outcome could be affected by the centralized or decentralized architecture of the proximity tracing solution. This does, *prima facie*, not seem to be the case. In other words, a situation of joint control between the legally designated entity and the app user seems, in theory, to be possible not only in (privacy preserving) decentralized solutions but also in the centralized protocol.

81 Third, we were interested in knowing whether the data processed by the (joint) controller(s) always qualify as "personal data" from the perspective of those entities. In other words, whether the perspective through which identifiability is assessed under Article 4(1) GDPR predefines the candidates for the role of controller. The answer seems to be negative. As highlighted in Tables 4 and 5 below, there are indeed situations where the actor that qualifies as a controller does not overlap with the actor for which the data at stake are to be regarded as personal. Only considering the actors for which the data are to be regarded as personal as potential candidates for the controller role could, therefore, lead to situations where the controller designated by law does not qualify as a controller in fact. This would create a mismatch between the legal fiction and the factual reality. In the decentralized protocol for example, the backend server (alone or together with the app user) could qualify as (joint) controller with respect to the collection and storage of diagnosed users' EphIDs, even though these EphIDs would not qualify as personal data from the perspective of the backend server (see Table 5 below). Conversely, treating the risk of re-identification independently from the allocation of responsibility could, especially in situations where (unlike in this specific use-case) there is no legally designated controller, result in an entity being qualified as a controller of data which, from its perspective, are non-personal, without even being aware of it. Both situations fail to meet the standard of legal certainty.

H. Time to close Pandora's box?

82 As mentioned in the beginning, this analysis was conceived as a thought provoking experiment. It does not provide a definitive answer to the

160 PRIVATICS Team INRIA (n 112).

161 DP-3T Project (n 112).

162 Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* [2014], Opinion of Advocate General Jääskinen (n 102) para 51.

163 In our view, the mere risk for a diagnosed app user to be re-identified by an exposed app user following a unique notification should suffice to exclude the applicability of the household exemption.

question of the allocation of responsibilities under the GDPR in concrete digital proximity tracing solutions adopted in the fight against COVID-19. The purpose is rather to illustrate the complexities and ambiguities of the legal test for joint control under the GDPR. Following some scholars' line of thinking that "at this rate, everyone could be considered a [joint] controller of personal data",[164] we illustrated how, under a legally plausible interpretation of the existing test for joint control under the GDPR, even app users in the ROBERT and DP-3T COVID-19 proximity tracing protocols could, in theory, qualify as joint controllers. Considering the limitations of this study, further research, based on the concrete application of COVID-19 proximity tracing solutions in a specific national context is needed, in order to investigate whether this conclusion could hold true also in real life COVID-19 app use-cases. If that were the case, we would not consider this as a desirable outcome. First, it is difficult to imagine how an app user would be able to comply with all the obligations incumbent upon joint controllers. Second, Article 82 (4) GDPR suggests that that, in a case of joint controllership, both the national health authority and the app user could be held liable *vis-à-vis* the data subject for the entire damage caused by a possible infringement of the Regulation. The possibility (even if only theoretical) of facing liability claims under the GDPR might deter individuals from using the COVID-19 app and ultimately undermine the efficacy of the proximity tracing solution in combating the spread of the disease. This would be precisely the opposite of what countries deploying a COVID-19 app intended to achieve.

83 Unlike what we had hypothesized, the risk of running into joint-controllership situations seems to apply both to centralized and (so-called privacy-preserving) decentralized software architectures. As already argued by other scholars,[165] such risk may, however, discourage the adoption of privacy-preserving decentralized solutions.

84 Finally, and most importantly, the analysis revealed a fundamentally incoherent approach to key concepts delimiting the material and personal scope of application of the GDPR, such as the meaning of "identifiability" of personal data, "determining the purposes and means" and "access" to personal data when assessing (joint) control. We believe it is time for National Supervisory Authorities or, preferably, the EDPB, to start providing unequivocal and uniform guidance on these notions. If not, the lack of legal certainty, may end up endangering the credibility of the EU data protection system.

164 Millard and others (2).

165 Chen and others (n 4) 293.

Table 4- Outcome of the analysis – centralized protocol

Processing operation	**Joint determination of the purposes and means**	**Re-identification risk as assessed by the DP-3T consortium**	**Re-identification risk as assessed by the ROBERT consortium**
Collection and storage by an at risk or ex-posed app user of diag-nosed users' EphIDs	**Purposes:**"own", closely linked/complimentary **Means:** use of means dev-el-oped by another entity for own purposes	*Joint control*	*Joint control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server)
	Purposes: the app user does not pursue his "own" pur-pose	*Sole control* (even though diagnosed users' EphIDs also qualify as personal data from the perspective of the app user)	*Sole control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server, whereas they do from the perspective of the app user)

Table 5- Outcome of the analysis – decentralized protocol

Processing operation	**Joint determination of the purposes and means**	**Re-identification risk as assessed by the DP-3T consortium**	**Re-identification risk as assessed by the ROBERT consortium**
Collection and storage by an at risk or ex-posed app user of diagnosed users' EphIDs	**Purposes:** "own", closely linked/complimentary **Means:** use of means devel-oped by another entity for own purposes	*Joint control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server)	*Joint control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server)
	Purposes: the app user does not pursue his "own" pur-pose	*Sole control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server, whereas they do from the perspective of the app user)	*Sole control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server, whereas they do from the perspective of the app user)

Use by an at risk or exposed app user of the diagnosed users' EphIDs for matching and risk score compu-tation	**Purposes:** "own", closely linked/complimentary **Means:** use of means devel-oped by another entity for own purposes	*Joint control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server)	*Joint control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server)
	Purposes: the app user does not pursue his "own" pur-pose	*Sole control* (even though diagnosed users' EphIDs do not qualify as personal data from the perspective of the backend server, whereas they do from the perspective of the app user)	*Sole control* (even though diagnosed users' EphIDs do not qualify as per-sonal data from the perspec-tive of the backend server, whereas they do from the perspective of the app user)

Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU

by **Can Atik and Bertin Martens***

Abstract: The arrival of digital data in agriculture opens the possibility to realise productivity gains through precision farming. It also raises questions about the distribution of these gains between farmers and agricultural service providers. Farmers' control of the data is often perceived as a means to appropriate a larger share of these gains. We show how data-driven agricultural business models lock farm data into machines and devices that reduce competition in downstream agricultural services markets. Personal data protection regulation is not applicable to non-personal agricultural machine data. Voluntary data charters in the EU and US emulate GDPR-like principles to give farmers more control over their data but do not really change market-based outcomes due to their legal design. Third-party platforms are a necessary intermediary because farmers cannot achieve the benefits from applications that depend on economies of scale and scope in data aggregation. Data lock-in, combined with the low marginal value of individual farm data, puts farmers in a weak bargaining position. Neutral intermediaries that are not vertically integrated into agricultural machines, inputs or services may help farmers to circumvent monopolistic data lock-ins. However, unless these neutral intermediaries find a way to generate and monetise economies of scale and scope with their data, their business model may not be sustainable. Regulatory intervention that facilitates portability and interoperability might be useful for farmers to overcome data lock-ins, but designing data access rights is a complicated issue as many parties contribute data in the production process and may claim access rights. Minor changes in who gets access to which data under which conditions may have significant effects on stakeholders. We conclude that digital agriculture still has some way to go to reach equitable and efficient solutions to data access rights. Similar situations are likely to occur in other industries that rely on non-personal machine data.

Keywords: smart farming; agricultural data; data governance; non-personal machine data; data access rights; competition policy

Recommended citation: Can Atik and Bertin Martens, Competition Problems and Governance of Non-personal Agricultural Machine Data: Comparing Voluntary Initiatives in the US and EU, 12 (2021) JIPITEC 370 para 1

A. Introduction

1 In conventional agriculture, decisions on farm inputs and processes are taken by farmers, based on their personal know-how. Today, the introduction of sensor-based digital data, Internet-of-Things (IoT) technologies and big data analytics in Smart Farming or Digital Agriculture[1] result in machine-

* Can Atik is a PhD candidate at Tilburg Law School with affiliation to the Tilburg Law and Economics Center (TILEC) and Tilburg Institute for Law, Technology, and Society (TILT), 5037 DE Tilburg, the Netherlands. The PhD research is funded by the postgraduate scholarship program of the Ministry of National Education, Republic of Turkey. Bertin Martens is Senior economist at the Joint Research Centre of the European Commission, E-41092 Seville, Spain. *The views and opinions expressed in this paper are the authors' and do not necessarily reflect those of the Joint Research Centre or the European Commission*

1 Xuan Pham and Martin Stack, 'How data analytics is transforming agriculture' (2018) 61 Business Horizons, p. 127; Harald Sundmaeker and others, 'Internet of food and farm 2020' in Ovidiu Vermesan and Peter Friess (eds), *Digitising the Industry*

based applications and data-driven solutions that are more precise than human observations.[2] Large amounts of sensor data are used for benchmarking and predictive modelling[3] to improve and refine decision-making about planting, seeding depth, seed placement, plant disease and machinery diagnostics, tillage, scouting, spraying,[4] harvesting and even marketing.[5] Although there are still doubts about the potential benefits compared to the costs,[6] it is often argued that data-driven services can improve farm productivity[7] and induce significant changes in the operation, management, and structure of farms and their role in the agricultural supply chain.[8] Farmers' role as independent decision-makers in the agricultural production process may come under pressure as other parties start contributing to critical decisions and claim a share in the benefits of farm operations. In this context, data access and re-use rights will affect competition and may re-distribute welfare between farmers and service providers.[9]

2 The EU is a more active jurisdiction in regulating data issues compared to the US. The primary horizontal legislative instrument in the EU is the General Data Protection Regulation (GDPR).[10] It assigns exclusive rights over access and use of personal data to natural persons as data subjects and restricts the re-use and re-purposing of these data. We argue in this paper that most agricultural data are non-personal machine/sensor-generated data that do not fall under the purview of the GDPR.[11] While the data subject is the logical anchor point for inalienable personal data rights, there is no obvious anchor point for rights to non-personal data. Any party that intervenes in the agricultural production process might claim access and use rights over data collected on farms. This unregulated agricultural data market comes close to a free business-to-business (B2B) data market, governed only by bilateral contracts between the parties involved. However, competition in that free market is distorted in several ways. Agricultural machines and devices that collect data and implement data-driven services can be designed to give the manufacturer exclusive access to the data. Farmers, who buy these devices in a competitive primary market, are locked into data-driven service providers in aftermarkets. That weakens their bargaining position in aftermarket services. Data lock-in situations also occur when there is no possibility to switch digital services together with historical data sets.[12] We describe several agricultural business models that build on these data lock-in situations.

- *Internet of Things Connecting the Physical, Digital and Virtual Worlds* (River Publishers 2016), pp. 132-133; Sjaak Wolfert and others, 'Big Data in Smart Farming - A review' (2017) 153 Agriculture Systems, pp. 69-75; Michael E. Sykuta, 'Big Data in Agriculture: Property Rights, Privacy and Competition in Ag Data Services' (2016) 19 International Food and Agribusiness Management Review, p. 60; See also Case No COMP/M.8084 – *Bayer/Monsanto*, Commission Decision (29 May 2018), para. 2442.

2 Krijn J. Poppe and others, 'Information and Communication Technology as a Driver for Change in Agri-food Chains' (2013) 12 EuroChoices, pp. 60-63; Krijn Poppe and others, 'A European perspective on the economics of Big Data' (2015) 12 Farm Policy Journal, pp. 11-12.

3 Adam Lesser, 'Analyst Report: Big data and big agriculture' (*GIGAOM,* 2014) <https://gigaom.com/report/big-data-and-big-agriculture/> accessed 4 March 2021; Wolfert and others, n. 1, p. 73.

4 Keith Coble and others, 'Advancing U.S. Agricultural Competitiveness With Big Data And Agricultural Economic Market Information, Analysis, And Research' (The Council on Food, Agricultural and Resource Economics 2016), p. 3.

5 Wolfert and others, n. 1, p. 74.

6 See, for example, Iria Soto and others, 'The Contribution of Precision Agriculture Technologies to Farm Productivity and the Mitigation of Greenhouse Gas Emissions in the EU' (Joint Research Centre of the European Commission 2019) - JRC112505.

7 See 'Internet of Food and Farm 2020' (*iof2020eu*, 2020) <https://www.iof2020.eu/communication-materials/iof2020-booklet-2019-highres.pdf> accessed 4 March 2021; See also Poppe and others, n. 2, p. 18;

8 Poppe and others, n. 2, p. 12.

9 Data-driven service providers are commonly referred, especially in the US, as Agricultural Technology Providers (ATPs): *"The term "agricultural technology provider" or ATP generally refers to a company that aggregates farmer's data, combines it with other relevant data sets, and applies algorithms to analyze the data."* See Sykuta, n. 1, p. 58, footnote 1.

10 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1, 4.5.2016.

11 Some scholars argue that all data can be linked to a natural person. See, for instance, Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10 Law, Innovation and Technology.

12 See Marie-Agnes Jouanjean and others, 'Issues Around Data Governance in the Digital Transformation of Agriculture: The Farmers' Perspective' (OECD 2020), p. 18.

3 Aftermarket lock-in is a well-known classic problem in competition law and economics.[13] However, data economics adds additional complications that may further weaken farmers' bargaining position in aftermarkets. Many data applications depend on economies of scale and scope in data aggregation to achieve efficiency gains. This requires a third-party intermediary to collect, aggregate and analyse the data of many farms. Individual farmers cannot realise that collective or social value of data. The relatively low market value of raw farm data compared to processed data weakens the bargaining position of farmers in data-driven agricultural services. It explains why farmers pay fees for agronomic services but do not receive payment for their data contributions. The question is whether giving farmers specific non-personal data rights could change that situation.

4 Machine manufacturers and agronomic service providers with exclusive access to data are well-placed to occupy that intermediary position. Vertical integration with downstream data-driven services reinforces their position. Mergers can create larger data pools and data-driven agricultural conglomerates.[14] There is a role for competition policy to ensure an appropriate balance between potential efficiency gains from data aggregation and efficiency losses from reduced competition.

5 The lack of clear rules regarding control and access to agricultural data does not seem to satisfy agricultural industry stakeholders. In the EU[15] and the US,[16] they have independently created two data charters to fill the perceived regulatory gaps with voluntary rules and principles.[17] The charters seek to emulate the EU GDPR by assigning a primary data ownership right to farmers. We analyse the impact of the charters on farmers' ability to overcome monopolistic data and aftermarket lock-in problems. We find that, while the EU and US charters differ on a number of points, their legal design limits the potential of the proposed rules and principles. They generally accept the primacy of bilateral free-market contracts over proposed rights for farmers. Aftermarket lock-in, combined with economies of scale and scope in data aggregation, explain why free-market bargaining overrules the data ownership principles in the charters.

6 We then look at two alternative responses to overcome the lock-in problem and facilitate switching between alternative aftermarket service providers: a) the ability of neutral third-party data intermediaries to unlock farmers and b) regulatory intervention with mandatory data portability right and interoperability obligations. We show how neutral data intermediaries that are not vertically integrated with machine or input sales, face problems in collecting sufficient data to realise the value-added from economies of scale and scope in data aggregation and how this weakens the financial sustainability

13 See, for example, Richard A. Posner, 'The Chicago School of Antitrust Analysis' (1979) 127 University of Pennsylvania Law Review.

14 There has already been a merger trend in the agricultural inputs sector that has also affected the emerging Digital Agriculture sector (DAs). See Case No COMP/M.7962 – *ChemChina/Syngenta,* Commission Decision (5 April 2017); Case No COMP/M.7932 – *Dow/DuPont,* Commission Decision (27 March 2017); *Bayer/Monsanto*, n. 1 above. See discussions in the literature regarding this trend's effects on the DAs in Ioannis Lianos and Dmitry Katalevsky, 'Merger Activity in the Factors of Production Segments of the Food Value Chain: - A Critical Assessment of the Bayer/Monsanto merger' (2017) UCL-CLES Policy Paper Series: 2017/1; Maurice E. Stucke and Allen P. Grunes, 'An Updated Antitrust Review of the Bayer-Monsanto Merger' (2018) The Konkurrenz Group White Paper; Tom Verdonk, 'Planting the Seeds of Market Power: Digital Agriculture, Farmers' Autonomy, and the Role of Competition Policy' in Leonie Reins (ed), *Regulating New Technologies in Uncertain Times* (Springer 2019), pp. 112-115.

15 'EU Code of conduct on agricultural data sharing by contractual agreement' (*Copa and Cogeca at all*, 2018) <EU_Code_of_conduct_on_agricultural_data_sharing_by_contractual_agreement_update_2019.pdf> accessed 4 March 2021.

16 'Privacy and Security Principles for Farm Data' (*Fb.org*, 2016) <https://www.fb.org/issues/innovation/data-privacy/privacy-and-security-principles-for-farm-data> accessed 4 March 2021.

17 Apart from the US and EU, there are also initiatives in New Zealand and Australia, see respectively 'Farm Data Code of Practice' (*Advisory Group*, 2016) <https://www.farmdatacode.org.nz/wp-content/uploads/2016/03/Farm-Data-Code-of-Practice-Version-1.1_lowres_singles.pdf> accessed 4 March 2021 and 'Farm Data Code' (*NFF*, 2020) <https://nff.org.au/wp-content/uploads/2020/02/Farm_Data_Code_Edition_1_WEB_FINAL.pdf> accessed 4 March 2021. Also, there is a clear interest in generating data governance rules for the sector. See, for instance, an online tool to let stakeholders generate their own data governance rules 'The Codes of Conduct' (*GODAN*, 2020) <https://www.godan.info/codes/list> accessed 4 March 2021; See the literature review on existing codes of conduct and calls for agricultural data regulation from the perspectives of various fields from ethics to engineering in Simone van der Burg, Marc-Jeroen Bogaardt and Sjaak Wolfert, 'Ethics of smart farming: Current questions and directions for responsible innovation towards the future' (2019) 90-91 NJAS - Wageningen Journal of Life Sciences, p. 9.

of their business models. We argue that attributing data rights in the absence of an obvious "anchor" party opens the door to many parties involved in farming claiming access rights, not only farmers. It is unclear who should get access to which data and under which conditions.

7 The remainder of this paper is structured as follows. In Section B, we start with a description of the economic efficiency gains from agricultural data and how these are realised in several types of data-driven agricultural business models by also identifying prominent competition concerns including data lock-ins. Section C discusses the legal status of agricultural data as non-personal machine and sensor-generated data. Section D explores to what extent the EU and the US voluntary codes of conduct offer an effective solution to these aftermarket competition concerns. We focus on i) the attribution of original data rights, ii) the re-use of data and iii) data portability. We conclude that the codes do not really change market outcomes and market failures. Section E first discusses the role of third-party intermediary platforms as alternative market-based arrangements to circumvent monopolistic data lock-ins. We show that they depend on data portability and face problems finding a sustainable business model. Second, we explore the possibility of regulatory intervention to facilitate portability and mandatory access to agricultural data, and discuss the complexity of the attribution of data access rights. Section F concludes.

B. The Economics of Agricultural Data

8 In the first part of this paper, we take a closer look at the market-driven use of agricultural data to understand the competition concerns that need to be addressed before diving into comparing the voluntary data charters developed in the US and EU. We start from different types of agricultural business models that have emerged in digital agriculture. While some platforms have emerged as independent digital service providers without any links to existing agricultural firms, some major data platforms have developed out of existing agricultural firms, including machine manufacturers and agricultural inputs producers.[18] We compare the business models of these different types of firms, how they monetise and ensure exclusive control over the data that they collect and how they affect the welfare of farmers. We argue that the business models are confronted with a choice between cooperation and competition among complementary service providers. We then turn to some economic characteristics of data and discuss how they can contribute to economic efficiency gains in agricultural production. We highlight the aftermarket services lock-in and competition problems that occur in this data-driven setting.

I. Data-driven Business Models in Agriculture

9 Data is an input in the production of goods and/or services. They have no value on their own. They become valuable only when they can be used to generate revenue in product and services markets. Since data are non-rival, private monetisation of data requires some degree of excludability in their use. If not, they dissipate into the public domain and lose their private market value – but not necessarily their social value.

10 We identify two main business models to generate private market value through excludability. The first one builds on exclusive access to data in agricultural machines, both for upstream data collection through sensors and downstream product and services implementation through actuators. The second uses proprietary knowledge about the optimal use of inputs to maximise production efficiency: seeds, fertilisers and chemicals in crop production as well as feedstock and animal health products in livestock management. These services are provided through an excludable channel, for instance, through devices. The two models may overlap to some extent and require some degree of collaboration. We can also identify a third category of business models that revolves around smaller firms that are either specialised in data collection and analytics, or in product sales but without integrating the upstream and downstream part in a single business model. This includes, for example, data-driven start-ups that apply artificial intelligence and machine learning to generate better agronomic services.[19] These pure data analytics firms are not vertically integrated. We come back to this intermediate category when the occasion arises throughout the text.

18 See, for example, Kenney Martin, Serhan Hiam and Trystram Gilles, 'Digitalization and Platforms in Agriculture: Organizations, Power Asymmetry, and Collective Action Solutions' (2020) ETLA Working Papers 78.

19 A similar classification of data-driven agricultural firms is proposed previously. The authors distinguish five types of intermediary platforms. See Ibid.

1. Agricultural machine producers

11 Agricultural machines are equipped with digital data sensors and actuators. Sensors collect data on the mechanical movements and navigation position of the machine. Actuators use data inputs to activate mechanical movements and steer the machine. For example, a GPS signal sensor captures the precise location of a machine; actuators steer the machine on the basis of instructions received from a computer programme. This combination enables the collection of field-level data and implementation of agronomic advisory services, for example, for automated seeding, fertilising and chemicals inputs.[20]

12 While the market for agricultural machine sales is highly competitive, the market for data that drive aftermarket services is less so. Agricultural machinery manufacturers can design the machine in such a way that they have exclusive access to sensor data and actuators inputs. Once a farmer buys a particular machine, he is locked into the data channels controlled by the machine manufacturer. The manufacturer may use this monopolistic position in upstream data collection, or in access to the downstream implementation of data-driven agronomic services, to leverage his position in downstream services markets. [21] The lack of interoperability between data formats and devices from different manufacturers reinforces this monopolistic market structure. Agricultural machine producers and service providers deliberately segment the data standards in order to increase switching costs for farmers, reduce competition in aftermarkets and apply monopolistic pricing in aftermarket services.[22] This was emphasised by KWS (an agricultural company) in the market investigation of the *Bayer/Monsanto* case:

> *"It is difficult to switch from one platform to another, since the industry is not able to agree on one common data protocol (joint data format), therefore there is high incentive for the farmer to decide on only one platform. Even though farmers keep the ownership of provided data and they can contractually request that their data are returned to them, from the technical point of view, such data are not compatible with another platform and can therefore not be easily transferred to another platform from a practical point of view."*[23]

13 According to the "Chicago Critique",[24] there is no need to intervene in the aftermarket when farmers are rational. They will consider the combined costs and benefits in the primary and aftermarket before deciding on the purchase of a device. If farmers are myopic, however, they may struggle to combine cost and benefits in both markets. Lack of transparency at the time of purchase may be an obstacle to rational decision-making. For instance, with long machine lifetimes and a fast-evolving technology environment, mismatches may occur during the lifetime of the machine that are not predictable at the time of purchase.

14 This monopolistic lock-in position is not absolute. Data plug-ins and add-ons can circumvent the manufacturer's monopoly on mechanical access. For example, Bosch has developed, in collaboration with some partners including Bayer's Xarvio, Syngenta and AGCO, the Nevonex interface that seeks to overcome incompatibility problems between agricultural machines.[25] It consists of an interface that can take data input from various machines, brands and data formats, and send steering signals to a variety of machines, including retro-fitted mechanical devices on existing machines.[26] In agricultural machinery, there is the Isobus ISO technical standard initiative.[27] For example, Xarvio designed a data-driven sprayer that can be mounted on existing mechanical sprayers to give them data steering for precision spraying purposes.[28] These

20 Athanasios Balafoutis and others, 'Precision Agriculture Technologies Positively Contributing to GHG Emissions Mitigation, Farm Productivity and Economics' (2017) 9 Sustainability; See also a preliminary study in this regard Daan Goense, 'The Accuracy of Farm Machinery for Precision Agriculture: A Case for Fertilizer Application' (1997) 45 Netherlands Journal of Agricultural Science.

21 Mihalis Kritikos, 'Precision agriculture in Europe - Legal, social and ethical considerations' (European Parliamentary Research Service 2017), p. 19. See also 'Data revolution: emerging new data driven business models in the agri-food sector' (EIP-AGRI 2016), p. 14.

22 Ibid.

23 *Bayer/Monsanto*, n. 1, para 2842.

24 See Posner, n.13 above.

25 See 'Discover What NEVONEX is All About' (*NEVONEX powered by Bosch*, 2021) <https://www.nevonex.com/how-it-works/> accessed 4 March 2021.

26 Ibid.

27 The worldwide ISO 11783 (ISOBUS) standard defines the communication between agricultural machinery, tractors and implements, and data transfer between these machines and farm software applications. However, it suffers from "forking" problems that are typical for open standards. This has led to a great number of innovative but proprietary ISOBUS solutions that are not necessarily fully interoperable. See 'ISOBUS - AEF Online' (*Aef-online.org*, 2020) <https://www.aef-online.org/the-aef/isobus.html#/About> accessed 4 March 2021.

28 See 'NEVONEX' (*Xarvio.com*, 2020) <https://www.xarvio.com/global/en/partnership/nevonex.html> accessed 4 March 2021.

add-ons with open technical standards may help to overcome interoperability barriers between machines and data-driven agronomic advisory services. However, there are several limitations to these interoperability solutions. First, the Isobus standard suffers from "forking" into several proprietary versions that are not necessarily fully compatible. Second, interoperability does not ensure the transfer of historical farm data between machines and applications.[29] Third, it remains to be seen how successful interoperable data formats, such as the Isobus standard, will become in the market. Several economic models explain the ambiguity in incentives for firms to open up access to their exclusive data.

15 Incentives may vary according to firms' market shares. Big manufacturers that benefit from a strong market position may be reluctant to give up their advantages.[30] Smaller manufacturers or companies that have no entrenched position in the agricultural machine market may prefer an open data standard. Smaller firms stand to gain more from interoperability than large firms with strong market positions.[31]

16 Another economic model that explains the ambiguity of incentives is the "co-opetition" (cooperation-competition) model.[32] Machine manufacturers can choose to open access to their machine data and make data formats compatible with common standards. This makes it easier for farmers to switch between agronomic service providers in the aftermarket. It increases competition between aftermarket service providers and decreases prices. That will make the machines more attractive to farmers and increase the market share of manufacturers who sell interoperable machines in the primary machine market. On the other hand, it may decrease aftersales revenue for manufacturers who are vertically integrated into aftermarket services. The net effect of all these factors is a complex empirical question that is hard to predict.

2. Agricultural input producers

17 Large input producers have accumulated considerable knowledge in the use of inputs such as seeds, fertilisers, pesticides and other chemicals. Working closely with agricultural extension services, agronomic laboratories and big historical datasets, they have proprietary knowledge about the precise genetic composition and characteristics of seeds, and the biochemical interaction with chemical inputs, soil quality and weather factors.[33] Besides these large vertically integrated input providers, there are also smaller start-ups that are specialised in data-driven agricultural services only. They both require complementary data to generate tailor-made agronomic solutions. An individual farmer's experience and data cannot match the insights obtained from large data pools and economies of scale and scope in the analysis of these fine-grained farm-specific data about actual input use and crop yields. Some data can be obtained from the market, and some need specific contractual relationships. For instance, coarse-grained land maps can be obtained from free satellite services (scale 10x10 meters) while more fine-grained mapping (up to 30x30 cm) is available for a price.[34] Farm specific data, such as detailed irrigation and soil data, need to be collected from the target farm. Combined with detailed weather forecasts, they enable the production of very granulated agronomic advisory services tailored to the needs of individual farmers and fields.[35] Service providers store historical data collected from farms. They have exclusive *de facto* control over these farm-specific data sets.[36] New

29 On the various possibilities regarding farm data lock-ins and the importance of historical data sets, see Can Atik, 'Understanding the Role of Agricultural Data on Market Power in the Emerging Digital Agriculture Sector: A Critical Analysis of the *Bayer/Monsanto* Decision' in Michal Gal and David Bosco (eds), *Challenges to Assumptions in Competition Law* (Edward Elgar 2021), pp. 56-63.

30 Machine producers ensure their exclusive control of machine-generated data. For instance, John Deere, a major player in the agricultural machines market, applies end-user license agreements (EULA) that let it block a tractor if the data collection procedure is violated. See 'Vendor lock-in, DRM, and crappy EULAs are turning America's independent farmers into tenant farmers' (*boingboing.net*, 2018) <https://boingboing.net/2018/03/08/you-are-the-product-5.html> accessed 4 March 2021.

31 Jacques Crémer, Patrick Rey and Jean Tirole, 'Connectivity in the Commercial Internet' (2003) 48 The Journal of Industrial Economics.

32 See Adam M. Brandenburger and Barry J. Nalebuff, *Co-Opetition* (Doubleday 1998) as the standard work on this subject.

33 See *Bayer/Monsanto*, n. 1, paras 2453-2455 and 2715-2724.

34 Many firms are producing and selling land images based on satellite and drone pictures. For an overview of pricing according to scale, see for example, 'Buy Satellite and Drone Imagery | Our Imagery Pricing Plans' (*Geocento.com*, 2020) <https://geocento.com/imagery-pricing-plans/> accessed 4 March 2021.

35 See more about generating data-driven agronomic services/prescriptions/solutions for farmers in Wolfert and others, n. 1 above.

36 See this cross dependency of farmers and ATPs in Atik, n. 29,

market entrants will need to access these historical data to generate accurate prescriptions[37] when farmers desire to change service providers. This creates a data lock-in situation for farmers, which can jeopardise competition in the emerging markets of data-driven agronomic services.[38] Vertically integrated agronomic advisory services can be combined with agricultural inputs sales. This entails the risk of self-preferencing: the service provider can recommend its own upstream products even though they are not objectively the best or cheapest product to suggest. Self-preferencing may reduce competition in upstream inputs markets.

18 Integrated input producers can monetise their information advantage in the form of agronomic services. They can simply send the advice to the farmer and enable him to implement it manually on these fields. For instance, advice can be dispensed through apps on mobile devices. Combined with field navigation maps, the farmer can steer his machines as required. Alternatively, advisory services can be dispensed automatically by proprietary data interface devices that directly steer machines. Many companies have developed such interfaces. Monsanto's subsidiary, the Climate Corporation, has introduced FieldView, a service that makes agronomic advice available to farmers and interacts with agricultural machines.[39] Bayer generated a similar service called FieldManager.[40] BASF uses the Maglis interface[41] and DowDuPont has various digital products that are sold in the US through its subsidiaries Pioneer[42] and Corteva Agriscience.[43] These companies can negotiate agreements with machine manufacturers to create a direct data access gate. For example, in the US, agricultural machine manufacturer John Deere came to an agreement with the Climate Company to let machines from the former interact with advisory services from the latter.[44]

19 Proprietary devices that dispense agronomic services can be used to leverage these integrated giants' positions in the markets for data-driven agronomic services or inputs sales. Once farmers buy into a device that has special arrangements with a particular agronomic service provider, they are locked into the device and the agronomic aftermarket service, especially when it uses non-compatible and non-interoperable data formats and software design. This aftermarket lock-in enables firms to charge a monopolistic price for their advisory services and inputs sales. Firms can either choose a lock-in strategy to avoid farmers' switching between data platforms, or choose an open system strategy to attract more farmers. Another strategy to circumvent exclusive cooperation between machine manufacturers and service providers is the use of machine add-ons that by-pass the manufacturers' exclusive data channels. The above example from Nevonex illustrates the latter case.

20 Agronomic service providers face the same trade-off between competition and cooperation as machine manufacturers. They can perceive machines as complementary products because their customers may value agronomic services more when combined with the manufacturer's machine compared to having the service alone. They may also perceive

pp. 64-68

37 Based on retroactive patterns. See Keith H. Coble and others, 'Big Data in Agriculture: A Challenge for the Future' (2018) 40 Applied Economic Perspectives and Policy, pp. 87 and 91.

38 See Atik, n. 29, pp. 56-73.

39 See 'Digital Farming Decisions and Insights to Maximize Every Acre' (*Climate.com*, 2020) <https://climate.com/> accessed 4 March 2021.

40 It is now controlled by BASF in the scope of the remedy package of the *Bayer/Monsanto* decision. See "The BASF Divestment Package" in *Bayer/Monsanto*, n. 1, para 3069 and subsequent paras. See the current services of FieldManager at 'FIELD MANAGER' (*Xarvio.com*) <https://www.xarvio.com/nl/nl/FIELD-MANAGER.html> accessed 4 March 2021.

41 "BASF Launches Maglis, a New Online Platform to Help Farmers Improve Crop Management" (*BASF*) <https://www.basf.com/en/company/news-and-media/news-releases/2016/03/p-16-140.html> accessed 4 March 2021.

42 'Farm Management Software' (*Pioneer.com*, 2021) <https://www.pioneer.com/us/tools-services/granular.html> accessed 4 March 2021.

43 'Software and Digital Services' (*Corteva.us*, 2021) <https://www.corteva.us/products-and-solutions/software-and-digital-solutions.html> accessed 4 March 2021.

44 'John Deere and the Climate Corporation Expand Precision and Digital Agriculture Options for Farmers' (*Climate.com*, 2015) <https://climate.com/newsroom/john-deere-climate-corp-expand-precision-digital-ag-options/15> accessed 4 March 2021. However, this agreement was investigated by the US District Court of Illinois from the perspective of antitrust concerns. See US District Court of Illinois, case 1:16-cv-08515, the US Justice Department as plaintiff against Deer & Company and Precision Planting as defendants. Eventually, the parties cancelled this agreement. See 'Monsanto Terminates Agreement for Sale of Precision Planting Equipment Business' (*Climate.com*, 2017) <https://climate.com/newsroom/monsanto-terminates-agreement-for-sale-of-precision-planting-equipment-business/25> accessed 4 March 2021.

them as competitors if customers will pay less for the agronomic services when combined with the machine than when they buy the services separately. This is again a hard empirical question.

3. Complementary nature of business models

21 The machine-centred and the agronomic services-centred data-driven business models are complements, and there is some degree of convergence between the two. Machine manufacturers can either produce their own complementary agronomic advisory services or, alternatively, negotiate an agreement with other agronomic service providers to share these data channels for the purpose of dispensing agronomic services. The tension between competition and cooperation is always present. In line with the co-opetition model,[45] machine manufacturers seek collaboration agreements with inputs and advisory service providers, and vice versa. For example, John Deere, an agricultural machinery manufacturer, focuses on machine-based data collection while Bayer and Monsanto, agricultural input providers, focus on data-driven agronomic services in input markets.[46] There are many collaboration agreements between these companies. Monsanto (or Bayer, now), for example, has agreements with machine manufacturers John Deere, Agco and CNHI, through its subsidiary, the Climate Corporation, which specialises in data-driven agronomic services.[47] These collaboration agreements fall short of mergers, but they nevertheless involve coordination.

II. Economies of Scale and Scope in Data Aggregation and Re-use

22 In the previous section, we examined two private business models that seek to monetise the value of agricultural data through data lock-in, either by linking primary machine markets with aftermarket services or linking data-driven agronomic services with inputs markets. These lock-in situations are well-known in classic competition policy. In this section, we focus on the underlying sources of agricultural efficiency or productivity gains from digital data. This creates new competition problems in data markets, with spill-over effects to machine and agronomic services markets.

45 Brandenburger and Nalebuff, n. 32 above.

46 *Bayer/Monsanto*, n. 1, paras. 2774-2775.

47 Ibid., para. 2815.

1. Economies of scale in data aggregation

23 Statistical analysis requires large samples of data in order to extract insights. Economies of scale occur when adding more observations on the same variables in a sample increases the accuracy of the statistical predictions. For example, more observations on the response of crop yield to different types of fertiliser improve the prediction accuracy for fertiliser. More fine-grained soil maps allow for more precise application of fertiliser and chemicals in fields.[48] These improvements will, at some point, become subject to diminishing returns to scale or the number of observations.

24 Economies of scale constitute an argument in favour of data concentration in large databases, allowing firms to accumulate and combine data from many sources.

2. Economies of scope in the re-use of data

25 Contrary to ordinary goods that are rival and can only be used for one purpose at the time, data are non-rival. Many parties can use the same dataset at the same time for a variety of purposes. Economic efficiency gains occur when data collected by a firm can be re-used for other purposes. Economies of scope in re-use[49] can be realised either by the firm that collected the data and re-uses it in-house for other purposes or by sharing/selling the data to another firm that uses it for another purpose. For example, a tractor is a rival physical good and can only be used by one farmer at the time. If a tractor would be non-rival, all farmers could use the same tractor at the same time to work in different fields. The welfare gains would be enormous: it would suffice to invest in the production of a single tractor to cater to the needs of all farmers. This prospect can be achieved with data. For example,

48 Another example is the prevention of the spread of plant diseases. The aggregation of fragmented data sets from different farms can help to prevent that spreading and reduce costs for the economy. See Martin Parr, 'Who Owns Open Agricultural Data? - The Plantwise Blog' (*The Plantwise Blog*, 2015) <https://blog.plantwise.org/2015/12/04/who-owns-open-agricultural-data/> accessed 4 March 2021.

49 For a more detailed explanation of economies of scope in re-use of products in general, see John C. Panzar and Robert D. Willig, 'Economies of Scope' (1981) 71(2) The American Economic Review; David J. Teece, 'Economies of scope and the scope of the enterprise' (1980) 1(3) Journal of Economic Behaviour & Organisation; David J. Teece, 'Towards an economic theory of the multi-product firm' (1982) 3(1) Journal of Economic Behaviour and Organisation.

detailed farmland and soil survey maps can be used for precision farming applications for all types of inputs and services on that farm – but not on other farms. Collecting the data comes at a fixed cost. Re-use of the same non-rival data for another purpose entails quasi-zero marginal reproduction costs of an electronic data file. Economies of scope in re-use constitutes an argument in favour of wider access to data. Many applications of data in farming are re-use applications. Farmers share land and soil map data with agronomic services, or livestock health and production data with service providers.

26 Contrary to economies of scale, economies of scope in the re-use of data constitute an argument in favour of de-concentration of data, facilitating the distribution of data over many applications and allowing access by many firms for competing applications.

27 Data access may also come at a cost. Privacy and commercial confidentiality are important for the autonomy of private decision-making by firms and individuals and for extracting private value from these decisions.[50] When data are used by a competing firm to produce a substitute good or service, it may harm the interests of the original data collector. When data become widely available, it erodes the market value of the data for the original collector and may become a disincentive for continued investments for data collection.

28 An ideal data governance regime would thus seek an optimal combination of wider access and exclusive control, a balance between anti-competitive concentration and competitive decentralisation.[51] Data are not excludable by nature. They require technical and/or legal protection to ensure exclusive access for one party. That is what machine manufacturers and agronomic advisory services aim to achieve by channelling data-driven services through exclusively controlled devices.

3. Economies of scope in data aggregation

29 When two datasets are complementary, more insights and economic value can be extracted from the analysis of the merged dataset, compared to applying data analysis to each of the separate data sets.[52] Economies of scope in data aggregation constitute another argument in favour of large data pools and concentration of data. They are a critical factor in the success of digital farming.

30 At the same time they trigger concerns from competition authorities, as shown by the market investigation of the European Commission's *Bayer/Monsanto* merger decision:

> *"The more data (and the more specific data) you have, the more robust your algorithms will be and the more proven results you will have as references to your potential customers. (..) Covering more crop varieties, more climate areas, more soil types, etc allows you to expand your offering to other areas and cultures and because it is a complex system that constantly evolves, it is important to have different independent and broadly representative sources of information to build the necessary expertise."*[53]

31 The merger between Bayer, a chemicals producer, and Monsanto, mostly known for genetically modified seeds, was designed to generate more benefits from their combined agronomic research, including in the digital era where big data collection and the use of artificial intelligence to comb through these datasets would have become primary tools to advance research. The merger decision package sought to reduce economies of scale and scope in data aggregation in order to maintain competition.[54]

32 Economies of scale and scope are two distinct measures. In our fertiliser example, economies of scale are related to the number of observations on a particular fertiliser. Economies of scope occur when more variables are added to estimate the impact of fertilisers on yields, such as soil and weather conditions and the use of different chemicals.

50 See John G. Palfrey and Urs Gasser, *Interop: The Promise and Perils of Highly Interconnected Systems* (Basic Books 2012).

51 This balance between competitive and anti-competitive forces has become a major issue in recent policy debates on anti-competitive behaviour by all kinds of digital data platforms. See for example Luis Cabral and others, 'The EU Digital Markets Act A Report from a Panel of Economic Experts' (Joint Research Centre of the European Commission 2021) - JRC122910.

52 Economies of scope in aggregation goes back to insights from the economics of learning. See Sherwin Rosen, 'Specialization and Human Capital' (1983) 1(1) Journal of Labor Economics. Rosen observed that when a person has a choice between learning two skills, specialisation in one skill is always beneficial when the costs of learning both skills are entirely separable. However, when learning costs are not separable and learning one skill decreases the cost of learning another, then there are economies of scope in learning both skills, provided that the benefits from interaction exceed the additional learning costs.

53 *Bayer/Monsanto*, n. 1, para. 2726.

54 The BASF divestment package, as the main remedial condition of the decision, aimed to keep the merging parties' Digital Agriculture operations and data sets separate. See more details in Ibid., para. 3046 and subsequent paras.

33 Realising economies of scale and scope in data aggregation requires "big" datasets, usually across many farms, inputs, outputs and production conditions. Individual farmers cannot realise these benefits. It requires a third-party intermediary who collects and aggregates data from many sources in order to extract more insights from the pooled data compared to the insights that farmers could extract from their own datasets.[55]

34 Intermediaries are not necessarily large firms. Small start-up firms may be able to collect a sufficiently large data sample and reach a high level of economies of scale and scope in selected data domains. However, specialisation in one specific area is not sufficient to be competitive in a wide range of agronomic services markets that span many complementary and substitute products and crops.[56]

35 An important consequence of economies of scale and scope in aggregation is that the collective or social value of farm data is usually higher than the private value of data for individual farmers.[57]

36 The existence of a gap between private and social value implies an inherent market failure. Purely private data ownership rights may therefore not be an optimal allocation mechanism. Neither is purely public and common access to data because that would eliminate any market value for data. All benefits would be dissipated as user surplus and would dis-incentivise investment in data collection. This constitutes an argument in favour of regulatory intervention to overcome data market failures and put in place alternative data access regimes that seek to realize the social value of data while preserving competition in data-driven services markets.

37 Another source of market failure occurs when data aggregation generates negative externalities for farmers. Economies of scale and scope in data aggregation are subject to diminishing returns.[58] Once an agricultural service provider has collected a dataset that is sufficiently large to produce algorithms with a high level of prediction accuracy, the marginal value of collecting additional data from farms is low or zero. This depresses the market value of individual farm data[59] and puts farmers in a weak bargaining position with regard to their data. Even if they did not face data portability or interoperability obstacles, they would not be in a position to monetise the value of their data. Conversely, it explains to a certain extent why intermediary platforms cannot give farmers a meaningful remuneration for their data. They can only ensure their financial sustainability by charging for the data-driven services that they offer.[60]

38 Several digital economy studies[61] already highlighted how the data-driven platform economy is torn between efficiency and welfare gains from data aggregation in intermediary platforms and anti-competitive behaviour by these monopolistic data giants.

C. The Legal Status of Agricultural Data

39 In the *Bayer/Monsanto* decision, the Commission classifies agricultural data in three types: (i) farm data collected from fields or barns via sensors in machines or provided by farmers, (ii) complementary data from specialised providers outside the farm (such as land and soil maps, weather, satellite and other environmental data), and (iii) proprietary data from agricultural inputs producers and data analytics service providers.[62]

55 For more details on the role that data platforms play in realising the social value of data, see Bertin Martens, 'Data Access, Consumer Interests and Social Welfare: An Economic Perspective' (2020) <https://ssrn.com/abstract=3605383> accessed 4 March 2021.

56 *Bayer/Monsanto*, n. 1, paras. 2758-2762.

57 Dirk Bergemann, Alessandro Bonatti and Tan Gan, 'The Economics of Social Data' (2020) Cowles Foundation Discussion Paper – N. 2203R.

58 Economies of scale and scope in data aggregation are easily confused with network effects. We do not think this terminology is appropriate in the case of agricultural data. Social media users, for example, are attracted by network effects because they want to be able to contact many other users. By contrast, farmers are not necessarily interested in contacting each other. They are interested in getting more efficient services. See similar considerations in Atik, n. 29, pp. 72-73. That requires data aggregation across many farms, products and circumstances, up to the point where diminishing returns to scale and scope in data aggregation set in.

59 For an application to personal data, see Daron Acemoglu and others, 'Too Much Data: Prices and Inefficiencies in Data Markets' (2019) NBER Working Paper – N. 26296.

60 See the discussion on the prominent business model in the emerging Digital Agriculture sector and cross dependency of farmers and service providers in Atik, n. 29, pp. 65-68.

61 See Cabral and others, n. 51. More explanations are provided in Bertin Martens 'An economic perspective on data and platform market power' (Joint Research Centre of the European Commission 2021) - JRC122896.

62 See *Bayer/Monsanto*, n. 1, para 2453 and subsequent paras.

All three categories are mostly machine-generated, either as raw data or as the outcome of data processing.

40 To identify their legal status, the first question is whether they can be considered as personal data within the scope of the GDPR. Article 4 of the GDPR defines personal data as "*any information relating to an identified or identifiable natural person ('data subject')...*". The GDPR gives the data subject a number of rights to the data collected by a service provider or hardware manufacturer, including the right to consent for collecting the data or re-using them for other purposes; the right to access and delete personal data; and to retrieve or transfer (portability) data.[63] As such, the GDPR automatically links personal data collected by a device to the data subject, irrespective of device ownership. Device owners, renters and operators, or service performers using the device as an intermediary, always require the consent of the data subject before they can collect personal data. The data subject retains inalienable non-tradable rights to the collected personal data. He can share data with other parties, but fundamental rights to the data will always remain attributed to the data subject, unless the data are anonymised in such a way that the link between the data and the data subject is irreversibly broken.

41 There are several legal reasons to consider agricultural machine-generated data outside the scope of the EU GDPR. Kritikos is very prudent in this regard as he states that "*not all categories of data involved in precision agriculture such as agronomic data, compliance data and meteorological data, actually qualify as personal data...*" apart from explicitly identified[64] or easily identifiable[65] data that are already under the protection of GDPR framework.[66] We argue that it is usually not possible to link machine/sensor-generated farm data with an *identified or identifiable natural person* as most data are directly collected from fields, greenhouses or barns via IoT technology. They provide information about, for instance, machines, soil, plants, products and animals, not about the state or the behaviour of natural persons. Similarly, other components of agricultural data, i.e. complementary data and proprietary data sets, are not related to an identified or identifiable natural person. They are about environmental conditions or performances of agricultural inputs such as seeds or pesticides. Any human identification data that might be collected besides machine data has no relevance for the purpose of farm decision making. The identity of the human farm worker, even if known, is usually not relevant for the purpose of agricultural services. Human intervention in data collection does not necessarily change the legal status of farm data. The applicability of the GDPR in farms is limited because only natural persons can be beneficiaries of the GDPR.[67] So, farms as legal entities cannot institutionally benefit from the GDPR.[68]

42 A number of EU documents confirm the classification of precision farming data as non-personal data. The Commission defines machine-generated data as "*created without the direct intervention of a human ... by sensors processing information received from equipment, software or machinery, whether virtual or real*",[69] and cites agricultural data as an example.[70] Recital 9 of the Regulation on the Free Flow of Non-Personal Data confirms that it applies to agriculture: *"... Specific examples of non-personal data include ... data on precision farming that can help to monitor and optimise the use of pesticides and water."*[71] Unlike the GDPR, this regulation does not define rights for non-personal

63 For a discussion on the limitations of the data portability right under the GDPR from the competition perspective, see Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19(6) German Law Journal. See also Jan Krämer, Pierre Senellart and Alexandre de Streel, 'Making Data Portability More Effective for The Digital Economy: Economic Implications and Regulatory Challenges' (Centre on Regulation in Europe 2020).

64 such as "*financial/economic data and staff data or other data derived from people's behaviour*" see Kritikos, n. 21 above, p. 14-15.

65 such as drone images which cover humans. Ibid.

66 OECD working paper also considered agricultural data sets are mostly outside the scope of the GDPR framework. See Jouanjean and others, n. 12 above, pp. 10-11.

67 See Article 1 of the GDPR, n. 10 above.

68 See more in Atik, n. 29, pp. 57-58.

69 See the Communication from the Commission 'Building a European Data Economy' COM(2017) 9 final, p. 9.

70 *"In general, data can be personal or non-personal. For example, data generated by home temperature sensors may be personal in nature if it can be related to a living person,* ***while data on soil humidity is not personal****. ... Where data qualifies as personal data, the data protection framework, in particular the GDPR, will apply."* Emphasis added. Ibid. The Commission has a similar understanding for IoT data. See, for instance, *"****non-personal*** *data generated by Internet of Things objects in an automated manner."* Emphasis added. See the Communication from the Commission 'Towards a common European data space' COM(2018) 232 final.

71 See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018.

data.[72] It is only a general framework for sectoral codes of conduct and possible future regulatory interventions.[73] There is no binding data portability provision for non-personal data sets.

43 Portability is only possible when standard terms and conditions let farmers do so. However, practice is not in favour of farmers.[74] For example, the FieldView farmer interface, produced by the Climate Corporation, restricts the definition of personal data to name, address and other personal details of the farmer.[75] Although the farmer is confirmed as the owner of all non-personal data, portability is limited to other FieldView users or platform partners only. This is further restricted because hardware and software that store the data are licensed, not sold. That includes the FieldView Drive, the hard disk that collects and stores all data. Data are accessible anytime, but the hardware should be returned at the end of the contract.[76] In this environment, there is no way for farmers to transfer their (historical) data to another platform. It locks them in the existing service provider or machine producer.

44 We conclude that most agricultural data are non-personal and fall outside the scope of the EU GDPR and its right to data portability. For non-personal data, there is no *de jure* allocation of legal rights, neither in the EU nor in the US. Also, there is no undisputed *ex-ante* legal framework that can unchain farmers from the data lock-ins.[77]

45 In this almost regulation-free data environment,[78] stakeholders can negotiate claims to data in bilateral contracts to determine access and use rights to the data. Market forces and bargaining power will determine the outcome. Technology may also play a role because device manufacturers and agricultural technology providers can design the data collection and storage processes in such a way to ensure their *de facto* exclusive access to the data.

D. The US and EU Agricultural Data Charters

46 The absence of a clear legal framework for non-personal agricultural data has been perceived as a shortcoming and motivated agricultural stakeholders in the US and EU to draft voluntary data rules.[79] They are not legally enforceable but are meant to be guiding principles in data transactions. The US Privacy and Security Principles for Farm Data (the US Principles, henceforth) were signed by a number of companies and organisations on April 1, 2016.[80] It covers ownership, transparency, portability, collection, access and control. The signatories formed the Ag Data Transparency Evaluator Inc. that audits companies' ag-data contracts and issues the Ag Data Transparency Seal, a certificate of conformity with the principles for data-collecting agri-tech companies.[81] Two years later, the EU Code

72 Article 1 of the Regulation (EU) 2018/1807 "*aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users.*"

73 See Ibid., Article 6. However, as we discuss in detail at section D below, existing voluntary codes have significant limitations in their design to achieve the policy goal of enhancing free flow of non-personal data not only in the EU, both also in other jurisdictions such as the US, New Zealand and Australia.

74 Kritikos, n. 21, p. 17; Jop Esmeijer and others, 'Data-driven innovation in agriculture: Case study for the OECD KBC2-programme' (TNO 2015) - R10154, p. 27; See also Matt McIntosh, 'Data Ownership Questions – and Why They're Important' (*Future Farming*, 2018) <https://www.futurefarming.com/Tools-data/Articles/2018/10/Data-ownership-questions--and-why-theyre-important-340743E/> accessed 4 March 2021.

75 'Climate Fieldview™ Terms of Service' (*Climate.com*, 2020) <https://climate.com/fieldview-terms-of-service> accessed 4 March 2021.

76 Ibid.

77 The Directorate General for Communications Networks, Content and Technology of the European Commission released a report that investigates the EU acquis that is potentially applicable to sharing of non-personal data. See "Analytical Report on EU Law Applicable to Sharing of Non-Personal Data' (DG CONNECT 2020). However, there is no mechanism equivalent to a portability right.

78 See a detailed discussion of recent EU proposals to regulate data and digital markets in Section E below.

79 in addition to other voluntary attempts in other jurisdictions such as in Australia and New Zealand.

80 See n. 16 above.

81 'About — Ag Data Transparent' (*Ag Data Transparent*) <https://www.agdatatransparent.com/about> accessed 4 March 2021. This might be a factor that compensates the voluntary nature of the rules to a certain extent because, at least, this might be a mechanism to track whether companies abide by the proposed principles or not. The limitation of this seal is also related to the contractual superiority design in the US principles. As the US rules keep a significant leeway to deviate from the principles with contractual agreements, blocking portability by a company might not be incompliant with the principles per se, and thus, seal requirements. In sum, the general limitation of the contractual superiority approach in the Principles also blocks the potential of this verification

of Conduct on agricultural data sharing (the EU Code, henceforth) was released by a coalition of EU agri-food associations on 23 April 2018 in Brussels.[82] The EU Code is a more comprehensive report with not only definitions of rules but also case examples.

47 Both the EU and US data charters take inspiration from the EU GDPR and seek to introduce GDPR-like data rights for farmers such as consent, access, portability, purpose and re-sale limitations. They are farmer-centric in the sense that they try to establish a direct link between data rights and the operator of the farm – although the EU Code is a bit ambiguous on this aspect. They aim to portray the farmer as the equivalent of the "natural person" in the GDPR. Unlike the GDPR that assigns certain inalienable rights to natural persons, both data charters introduce tradable data ownership and alienable data rights. We compare both data charters in this section. In particular, we inquire to what extent they are able to overcome the lock-in and foreclosure data market failures identified above.

I. Attribution of Original Data Rights – Ownership Rights

48 The US document distinguishes between farmers and service providers (called Agriculture Technology Providers or ATPs), and attributes original rights (ownership of data) to farmers:

> *"Farmers own information generated on their farming operations. However, it is the responsibility of the farmer to agree upon data use and sharing with the other stakeholders with an economic interest, such as the tenant, landowner, cooperative, owner of the precision agriculture system hardware, and/or ATP etc. The farmer contracting with the ATP is responsible for ensuring that only the data they own or have permission to use is included in the account with the ATP."*

49 The US text unambiguously attributes the 'ownership of data' to farmers[83] who generate data on their farming operations. Data ownership[84] is divorced from machine, device or land ownership, including from external parties that perform services on the farm. Ownership is attributed to the party that decides and manages the farming operations. The data are not considered as the product of device ownership, but rather of the farming operation: farmers' efforts and practices. The text makes farmers responsible for any data sharing with other stakeholders with an economic interest by means of contracts, but this responsibility is ambiguous. There is no clarification in the text that implies rights for stakeholders or any mechanism to be used by them to access the data. This looks more like an advisory statement for farmers. The text uses ownership as the central legal concept when designing data rights. However, ownership rights are tradable/alienable. Although some parts of the text seem to provide inalienable consent rights to data re-use (see section 3.2. below), the data ownership design behind the US Principles limits the potential of the proposed rights with their alienable/transferable nature.

50 The EU Code has a more ambiguous wording. It distinguishes between data originators, providers and users.[85] It attributes data ownership rights to data generated during farming operations to data originators, i.e. the right to benefit from and/or be compensated for the use of data created as part of their activity. However, when data are produced by a service provider or external operator on the farm in the course of their activity, the operator might be considered as the data originator, not the farmer:

> *The originator (owner) - "the person or entity that can claim the exclusive right to licence access to the data and control its downstream use or re-use"*[86]

> *"The data originator of all the data generated during the operation is the one who has created/collected this data either by technical means (e.g. agricultural machinery, electronic data processing programs), by themselves or who has commissioned data providers for this purpose."*[87]

> *"This Code recognises the data originator's right, whether they are a farmer or another party..."*[88]

51 Clearly, the data originator may be different from the farmer, especially in automated data collection.

of compliance design to a large extent.

82 See n. 15 above.

83 Note the ambiguity of the use of the word "farmer". It may refer to the farm as a legal entity but also to a natural person who is in charge of the farming operations. The former interpretation might have been intended here in order to reinforce the similarity with personal data rights.

84 There is some research on data ownership in agricultural data. See the literature review by van der Burg, Bogaardt and Wolfert, n. 17, pp. 3-5.

85 See the EU Code, n. 15, pp. 5-9.

86 Ibid., p. 6.

87 Ibid.

88 Ibid., p. 8.

It is not clear whether the operator would be the owner of the device, the device controller, or possibly the farmer who may have rented a device. Data collection may be conducted by a third party, commissioned by the farmer and with the aim to facilitate farmers' decision-making. If data-collecting sensors in machines are not owned by farmers, the sensor/machine owners are the data providers, not the data originators:

> *"It can be assumed that the data originators are the farmers, also from data of sensors that are owned by the farmer. If sensors are not owned by the farmers, the sensor owners are seen as data providers."*[89]

52 The notion of data provider refers to a natural or legal person who, under an agreement, delivers data to the data user and/or data originator.[90] Although these extra definitions (data user and data provider) create confusion regarding the attribution of original rights, the owner is data originator.

53 An additional provision in the Code adds to the confusion because it seemingly reverses the provision that data rights can be owned by other parties than the farmer:

> *"Rights regarding data produced on the farm or during farming operations are owned by the farmer and may be used extensively by them."*[91]

54 The attribution of original rights emphasises data on "*the farm or during farming operations*". This may be interpreted as indicating raw farm data only, not processed data. The text may be intentionally silent on processed data, leaving it out of the data charter and subject to the free market.

55 Both data charters have repetitive statements that indicate that related rights can be alienable and transferable, i.e. they can be traded through bilateral contracts. This is compatible with the concept of ownership. Bilateral negotiations imply that bargaining power will play an important role in deciding who ends up with the effective ownership right of the data. For example, powerful data aggregators who can extract more value from large data pools could end up acquiring the data. This may be beneficial for farmers if it allows them to obtain the highest value for their data. It may also be detrimental when farmers are locked-in machine data and data-driven services markets are foreclosed. For example, machine manufacturers or service providers may have exclusive control over access to the data that enables them to foreclose the market for downstream use of the data for the purpose of agricultural services. That leaves no other option to the farmer than to accept the proposed terms and conditions that may contain provisions to transfer ownership rights from farmers to machine producers or technology providers. Portability rights would open the door to circumvent lock-in situations, but it is unlikely to be enforced together with the alienable and exclusive data ownership understanding.

56 Despite the fact that the EU and US agricultural data charters were inspired by the GDPR,[92] the introduction of tradable data ownership rights shows how the charters represent a clear departure from the underlying principles of the GDPR, where rights to personal data are considered as fundamental and inalienable human rights.[93] Even if the data rights are allocated initially to the farmers, bargaining power determines which party eventually ends up with the rights to use the data. Consequently, data ownership as conceived in both the EU and US charters is not able to address lock-in concerns and broader data access problems in the sector. Inalienability might protect farmers from powerful service providers or machine producers in terms of controlling collected raw farm data in a sustainable way.[94] Also, inalienable data rights do not necessarily exclude other stakeholders from using the data. For instance, while farmers can have rights to data portability when changing services, the same data can also be used for training algorithms by the previous technology provider, or the new tenant of a rented farm field might benefit from the historical data sets.

57 However, since farms are tradable assets, all the rights that they acquire should be by definition tradable as well. So, inalienable rights should stay with the farm, not with the farmer as an individual. Otherwise, it may create problems when farms are sold while rights remain with the farmer. Inalienable

89 Ibid., p. 15.

90 Ibid., p. 7.

91 Ibid., p. 8.

92 As it can be seen from the following part of this section, they both used GDPR concepts, but sometimes this transplantation approach does not match the non-personal agricultural data.

93 With regards to the Australian and New Zealand ag-data codes, it has to be noted that they do not mention ownership of farm data as they solely revolve around particular principles such as data security, data access and retention. In this regard, it has to be stated that they adopt a less problematic approach when designing their texts.

94 See the previous arguments in this regard at Can Atik, 'Data Ownership and Data Portability in the Digital Agriculture Sector: A Proposal to Address Novel Challenges' (*Florence School of Regulation*, 2019) <https://fsr.eui.eu/atik-c-how-big-data-affects-competition-law-analysis-in-online-platforms-and-agriculture-does-one-size-fit-all/> accessed 4 March 2021.

rights for farms not only protect the farmer while he owns the farm, but also allow him to sell the rights together with the farm. Alienable rights imply that the rights to data can be sold separately from rights to the legal entity of the farm. Big data firms might hoover up farm data rights without owning farms. That would handicap future owners of farms and diminish the value of farms.

II. Data re-use, Access and Consent Rights

58 Under the title "Collection, Access and Control" the US Principles state that;

> *"An ATP's collection, access and use of farm data should be granted only with the affirmative and explicit consent of the farmer. This will be by contract agreements, whether signed or digital."*

59 This gives farmers an exclusive decision right over data access and re-use by third parties, as an attribute of their data ownership right. This clause aims to restrict onward data sharing by ATPs. At first sight, it gives farmers inalienable control rights vis à vis third parties. However, farmers can give their consent in the agreement to leave it up to the ATP to decide on sharing data with third parties. Unlike in the GDPR, there are no details regarding the modalities of the consent. Is a general consent statement valid, and is there a right to withdraw consent? This might result in ambiguities with regard to the alienability of the right to consent. The primacy of contracts implies that withdrawal and data retention rights can also be restricted by agreements, i.e. they are alienable. Repetitive statements throughout the text in favour of contractual superiority may be an indicator of the ATPs' influence in designing the charter.[95]

60 The EU Code is again more ambiguous. Consent for data access and re-use may be given by the data originator or the operator. This boils down to the farmer's consent only if the farmer and originator coincide. Contract dominates, however, which implies that consent and re-use rights are alienable, as in the US charter.

> *"The collection, access, storage and usage of the collected agricultural data can only occur once the data originator has granted their explicit, express and informed permission via a contractual arrangement."*[96]

> *"The data originator must give permission for their data to be used and shared with third parties, including circumstances in which decisions are made based on data."* [97]

> *"Right to determine who can access and use the data is attributed to this operator."* [98]

> *"Parties ... should establish a contract clearly setting the data collection and data sharing conditions..."*[99]

> *"Parties may not use, process or share data without the consent of the data originator."*[100]

61 Like in the US Principles, details of the consent conditions are not mentioned, apart from a reference to GDPR based principles such as being *explicit, express and informed.* Therefore, it is unclear if a general consent statement in the contract is valid or whether there is a right to withdraw consent. This example demonstrates the limitations of the contract-based design in the charters. The validity of contractual relationships can be challenged by using the *explicit, express and informed permission* argument as most of the service providers' terms and conditions are standard texts. So, the existing design is open to a number of problems in practice.

> *"Data originators must be given the possibility to opt-out of the contract and terminate or suspend the collection and usage of their data, provided that the contractual obligations have been met. This must be clearly stated in the contract..."*[101]

62 This statement signals that the consent rights could be inalienable and can be cancelled at any time by the data originator. Not surprisingly, this general statement is again subject to contractual provisions. Unless stated in the contract, there is no right to opt-out or terminate.[102] This problematic design is repeated all over the EU Code. It is difficult to see how these data principles could change anything if they would become law, compared to free and unregulated data markets, since contracts and market forces prevail over the principles.

95 One may expect that industry stakeholders favour the *status quo*. They benefit from the existing non-regulatory environment with their *de facto* data control. The design of the EU and US charters that prioritise contractual freedom over the principles of the charters ensures this *status quo*.

96 The EU Code, n. 15, p. 9.

97 Ibid.

98 Ibid., p. 8.

99 Ibid.

100 Ibid.

101 Ibid., p. 10.

102 Ibid.

63 Another rule mentions *pseudonymisation or anonymisation* of agricultural data in the EU Code;

> *"Data originator must give permission for their data to be used and shared with third parties... Information should only be given to third parties as aggregated, pseudonymized or anonymised data unless it is required to deliver the requested service and/or the conditions specified in the contract. Unless specified in the contract, the data user must take all precautions to avoid re-identification."*[103]

64 The concepts of *pseudonymisation* and *anonymisation* are related to the privacy and identifiability of natural persons. They do not have any meaning for non-personal agricultural data in this regard. Data could be anonymised with respect to the identification of the farm. Farmers might not be happy about other parties accessing data on their farming practices because it may affect the asset value of their farm, their credit score, etc. This may imply that farm identification and physical location coordinates should be eliminated from the data. It would be more appropriate to link the clear aims and the re-use consent requirements such as to protect farms' trade secrets, instead of using privacy law concepts.

65 Other principles in the US charter might also play a role in consent for access and re-use. For example, under "Transparency and consistency", it states that;

> *"ATPs shall notify farmers about the purposes for which they collect and use farm data, third parties to which they disclose the data and the choices the ATP offers for limiting its use and disclosure."*

66 This formulation is not clear about the consequences of notification. Does the farmer have a right to object? The text is silent about this. The notification principle can become functional only if it is related to an inalienable consent right. Inalienability, in nature, is strictly related to binding legal rules that have clear enforcement mechanisms.

67 Under "Disclosure, Use and Sale Limitation" the US charter states that;

> *"An ATP will not sell and/or disclose non-aggregated farm data to a third party without first securing a legally binding commitment to be bound by the same terms and conditions as the ATP has with the farmer. Farmers must be notified if such a sale is going to take place and have the option to opt out or have their data removed prior to that sale. An ATP will not share or disclose original farm data with a third party in any manner that is inconsistent with the contract with the farmer. If the agreement with the third party is not the same as the agreement with the ATP, farmers must be presented with the third party's terms for agreement or rejection."*

68 This statement implies an extension of contractual terms to third parties. Since there is no *in rem* legal framework for data that is enforceable towards third parties, the US charter attempts to use contracts as an enforcement tool for these principles.

69 Both charters also have rules that prevent unilateral contractual changes without the consent of farmers.

70 The US Principles include the following statements:

> *"An ATP's principles, policies and practices should be transparent and fully consistent with the terms and conditions in their legal contracts. An ATP will not change the customer's contract without his or her agreement. "*

71 The EU Code has the following consent rule:

> *"Contracts must not be amended without prior consent of the data originator. If data is to be sold or shared with a third party that is not initially mentioned in the contract, the data originator must be able to agree or refuse this, without financial or other repercussions."*[104]

72 This protects farmers from unilateral actions. Service providers are obliged to maintain services under older terms and conditions (T&C). Provisions that forbid unilateral changes are indeed stating the obvious because both of the charters are designed to be enforced via contracts, and unilateral changes are not compatible with the mutual assent principle in contractual relations in any case.

73 Apart from this general statement in the texts, the EU Code provides a specific obligation to take consent for the new data-sharing situations that are not specified in the contract beforehand. The originator can refuse new sharing. The obligation for service providers is not to impose any response to this refusal that would result in negative consequences for farmers. Although it is not clear what the scope of this obligation or the meaning of the negative repercussions exactly is, it is a positive intention to protect the weaker party in case of refusal decision for the third-party access. The prohibition of financial or other repercussions plays an important role to compel service providers or machine producers not to limit machine functionality, for instance, if new T&C are rejected. The US text has no statement regarding the consequences of such an action.

74 The EU Code brings an interesting obligation for third parties' access to data;

103 Ibid., p. 9.

104 Ibid., p. 10.

"The data user can only sell or disclose data to a third party if she/he has secured the same terms and conditions as specified in the contract between user and originator."[105]

75 However, it is unclear whether this is an additional obligation above the ones discussed before or an alternative one to share data, or whether the farmer and third party enter into a direct contractual relationship or this is only between companies, i.e. data user and third party. In the case of the latter situation, it is difficult to see how a farmer can enforce its rights against the third party as the farmer would not be a part of the contract between companies. The idea seems to protect farmers with the same contractual conditions, but the existing form of the text is ambiguous.

76 In general, there are various consent rules to collect, access or re-use of data, especially in the EU code. However, neither their scope and enforcement mechanisms nor their effects on the competitive dynamics in the sector are undisputedly clear. Also, contractual superiority emphasis throughout the text further limits the potential of the proposed rules and rights, if any. Apart from the discussed ambiguities and limitations of the texts, the core question, indeed, might be whether we really need consent-based rules and rights in the non-personal agricultural data setting from the competition policy perspective. On the one hand, consent rights for collection, access and re-use of data might increase farmers bargaining position if they are inalienable and binding. On the other hand, this may create another set of barriers against the free flow of data in the sector. This balance should be carefully considered when designing the sectoral consent rules. Instead of transplanting personal data concepts from the GDPR, rights need to be designed in accordance with sectoral conditions. Data protection law serves a more human rights-oriented policy preference that might not always be compatible with the needs of the sector, which is predominantly based on non-personal agricultural data.

III. Data Portability Designs and Lock-in Situations

77 In the US Principles, data portability is considered as a privacy-related issue, not a competition issue because there is no portability right for anonymous or unidentifiable data sets. Also, only primary data can be ported, not 'aggregated' data;

"Within the context of the agreement and retention policy, farmers should be able to retrieve their data for storage or use in other systems, with the exception of the data that has been made anonymous or aggregated and is no longer specifically identifiable. Non-anonymized or non-aggregated data should be easy for farmers to receive their data back at their discretion."

78 As discussed above, anonymisation or identifiability are incompatible when discussing non-personal farm data as they are privacy law concepts. Protecting commercial confidentiality might have a certain rationale, but it is not related to the portability provision. When it comes to portability right, these nuances do not make sense. This indicates that the US Principles did not have a clear framework of failures to address them with their rules. It seems more like privacy-centric legal transplantation to an incompatible context, i.e. non-personal farm data.

79 The reference to *"within the context of the agreement and retention policy"* indicates that this is not an inalienable right. Farms can trade this right away in a contract, and market power will determine the eventual outcome of the negotiations. The US Principles actually do not change the *status quo* of the free B2B data market setting apart from its advisory statements in favour of contractual portability clauses.

80 In the EU Code, the rule regarding portability is as follows:

"Unless otherwise agreed in the contract, the data originator has the right to transmit this data to another data user. If agreed between the parties, the data originator shall have the right to have the data transmitted directly from one data user to another, where technically feasible."[106]

81 This demonstrates the approach of the EU Code in favour of the primacy of contracts over principles again. However, this clause has a different design compared to other rules in the text. In situations where contracts remain silent on portability, the Code could be invoked to assume portability by default. This makes the scope of portability right somewhat broader in the EU Code compared to the US Principles. This is still an alienable design as this right can be removed by contractual clauses. However, the following sentence repeats the same right by saying that *if agreed between the parties.* This makes the approach of the text confusing because this jeopardises the possible legal interpretation of default portability right in the case of contractual silence. The text could have been clearer in this regard.

82 Portability is only possible in the EU Code "*where technically feasible*" – again an explicit transposition from Article 20 (2) GDPR. Technical feasibility

105 Ibid.

106 Ibid., p. 9.

might be problematic, especially when different and incompatible standards create an obstacle to the transfer.[107] Differentiation in standards is sometimes an intentional business strategy to prevent portability of data to competitors.[108] This may prevent farmers from enforcing their right even though the portability clause is not waived in the contract.

83 Indeed, the EU Code is aware of technical barriers to data portability and asks for transparency in this respect in the contract:

> *"The means through which they may migrate data pertaining to their farming operations to other service and the electronic data interchange standards and formats which are supported shall also be made clear."*[109]

84 Even though there is an obligation on service providers to be clear about standards and interoperability, this falls short of a sector-wide standard and interoperability obligation. This rule is more about a transparency obligation for service providers. Therefore, even though the proposed rule in the EU Code becomes binding, this will not be effective in removing potential technical barriers to the free flow of data and will not ensure interoperability in the sector.

85 The portability rule is complemented by the following paragraph;

> *"This should be done without compromising restricted access to machine data or sensitive data (only relevant to the correct functioning of the machinery). This should be clearly specified in the contracts between farmers/contractors and device manufacturers."*[110]

86 This statement caters to the wishes of machine manufacturers to protect their proprietary, sensitive and confidential data collected, stored and processed in machines, including data regarding the operations of the machine itself. Service providers or machine producers' 'proprietary data' fall outside the data originators' rights to portability.

87 The EU Code also mentions the data formats when receiving data from service providers;

> *"The data originator shall have the right to receive the data concerning their operation as specified in the contract, in a structured, frequently used and machine-readable format."*[111]

88 The reference to "*the right to receive the data concerning their operation"* associates data rights with farming operations, not with the machine or device ownership. As noted before, this is important in a sector where renting machines and outsourcing of services is a common practice. It somewhat reduces the ambiguity in the attribution of original rights to data originators. It is obvious that stakeholders in the EU are aware of technical challenges to transfer data due to lack of standards and fragmentation in data formats, and this general principle could have been helpful to mitigate this problem to a certain extent, if it had been binding.

89 As a general consideration, although existing forms of portability related provisions in both the EU and US charters are not adequate to mitigate sectoral concerns deriving from farmers' lock-in situations, one can expect that these voluntary portability rules might become a sector trend to implement more lenient data policies by service providers in terms of enabling the transfer of data to rivals when farmers desire to do so, especially for the EU Code as the US Principles are more focused on transplanting privacy principles rather than promoting competition in the market. However, it might not be realistic to expect that service providers will voluntarily renounce their exclusive control over the collected data. They have no incentive to weaken the advantages they derive from their exclusive data access. Still, the design of the EU Code, with a default portability right for farmers,[112] unless repealed by contract, could be an important step towards inalienable and binding rights for farmers, compared to the US Principles in which contractual clauses are always considered superior to the proposed rules and principles.

IV. Other Rights and Rules on Data

90 Our main focus in this section is to compare the attribution of original rights, data re-use/access rights and portability rights in these voluntary initiatives from a competition policy perspective. These rights could have major implications for data access related problems in the sector. However, it is also interesting to briefly evaluate other

107 The technical feasibility of ag-data transfer/combination is discussed by computer scientists at Wageningen University. See 'DATA FAIR' (*WUR*, 2020) <https://www.wur.nl/en/article/DATA-FAIR-EN.htm> accessed 4 March 2021. The authors state that portability is possible and meaningful if the data is findable, accessible, interoperable, and reusable.

108 This is one of the problems in the sector: *"Every provider is building his own little kingdom."* See Esmeijer and others, n. 74, p. 34; See also at Kritikos, n. 21, p. 10.

109 The EU Code, n. 15, p. 10.

110 Ibid., p. 10.

111 Ibid., p. 9.

112 despite the ambiguity in the following sentence of *"If agreed between the parties"*. Ibid., p. 9.

provisions in the charters, such as data retention/retrieval rights, purpose/storage limitation rules or prohibition of speculation and price discrimination. These may also affect the data access puzzle in this emerging sector. This sub-section discusses whether they are suitable for the non-personal machine ag-data setting and address the identified concerns.

1. Data Retention/Retrieval Rights

91 In the US text, the following principle is proposed:

> *"Each ATP should provide for the removal, secure destruction and return of original farm data from the farmer's account upon the request of the farmer or after a pre-agreed period of time."*

92 This statement seems inspired by the "right to be forgotten" in the EU GDPR. Farmers may want to exercise this right, for example, when they change service providers along with their portability right that is separately mentioned in the text. However, it is unclear what this provision aims to protect since farm data is not personal.

93 In the EU Code, there is a general statement about access and retrieval rights:

> *"Data originators should be granted appropriate and easy access and be able to retrieve their attributed ("own") data further down the line, unless the aggregated data is not linked to the attribution as it is not only based on the data of the data originator. It is essential to make the data provider ("collector") responsible for making the data easily available to the data originator in a format that they will find accessible and readable, where technically feasible. If not technically feasible, the data provider should provide justification."*[113]

94 Data retrieval is applicable only to the original "attributed" farm data, not to the processed data sets that have been enrichened by other data sources. The rule is limited by technical feasibility constraints.

95 The EU Code also has a specific rule on 'right to be forgotten' beyond the general statement of retrieval rights;

> *"There must be the option to remove, destroy (e.g. right to be forgotten) or return all original data (e.g. farm data) upon the data originator's request."*[114]

96 The "right to be forgotten" exists in the GDPR for personal data, including farmers' personal data. That right may be meaningful for non-personal business data to preserve commercial secrecy and prevent third-party access that could be harmful to the commercial interests of the farm. Indeed, the EU Code states that:

> *"Protecting trade secrets, intellectual property rights, and protecting against tampering are the main reasons as to why information is not shared and why even business partners in joint projects are not permitted to receive data."*[115]

97 However, the intention to address commercial concerns could have been stated more directly in both texts without using GDPR terminology.

2. Purpose and Storage Limitations

98 In the US Principles:

> *"An ATP will not share or disclose original farm data with a third party in any manner that is inconsistent with the contract with the farmer."*

99 In the EU Code:

> *"Data must be collected and used for the specific purpose agreed in the contract. The datasets should only be kept for as long as is strictly necessary for the relevant analyses to be carried out. In addition, data should only be accessed by those with the required authorisation."*[116]

100 Purpose and storage limitations are again legal transplants from the GDPR. The EU Code links it with an implicit obligation for service providers to destroy the data after use. This may create complications when farmers store their historical data sets only in databases of service providers. Contracts will normally define retention periods. There is no explicit duty to inform farmers when data are about to be destroyed. This might be problematic. Purpose limitation rules may strengthen farmers' positions vis-a-vis service providers or machine producers, but this may also limit the potential societal welfare effect deriving from full data exploitation. Personal data related principles borrowed from GDPR should be carefully considered in the non-personal farm data setting when designing the related rules.

113 The EU Code, n. 15, p. 9.

114 Ibid., p. 11.

115 Ibid., p. 12.

116 Ibid., p. 9.

3. Prohibition of Speculation and Price Discrimination

101 Both the US Principles and EU Code contain prohibitions to use the data for unlawful and anti-competitive activities. They also go further and contain somewhat moralizing statements.

102 In the US Principles:

> *"ATPs should not use the data for unlawful or anti-competitive activities, such as a prohibition on the use of farm data by the ATP to speculate in commodity markets."*

103 In the EU Code:

> *"Collectors and users of farm data must therefore not use this data for unlawful purposes or take advantage of it to speculate or for other such purposes."*[117]

104 The inclusion of speculation "or other such purposes" is strange. Speculation is not an unlawful activity. It may actually induce transparency and efficiency gains. Futures markets in agricultural commodities are an essential part of agricultural markets. We can infer that the statement in the EU Code intends to cover unfair behaviours such as the use of data for price discrimination purposes.[118] It contains a prohibition of price discrimination:

> *"The data must not be used to assess the originators' ability to pay for a service."*[119]

105 Farm data may be used to assess farmers' willingness to pay for goods and services. This, in turn, can lead to price discrimination. Price discrimination is not a *per se* an infringement of competition law.[120] Moreover, it can, under certain conditions, be welfare-enhancing[121] for farmers and service providers. Obviously, farmers fear that powerful data companies could use the data against their interests, to manipulate or exploit them in inputs and outputs markets. Price discrimination is a strategy that allows sellers to extract more profits from buyers. It may reduce buyers' welfare but may also enable new buyers to come into the market when they receive more attractive price offers. As such, price discrimination induces equity concerns because of changes in welfare distribution. It may also generate additional welfare for society as a whole. The net balance between these two effects is an empirical question.

V. General Considerations

106 Although there are some positive considerations,[122] attempts by the US and EU agricultural data charters to transpose some basic GDPR principles of personal data protection to non-personal machine-generated data run into several problems. For instance, notions of pseudonymization and anonymization or the right to be forgotten are related to the privacy of natural persons. They are not relevant for non-personal agricultural data. If the aim was to protect commercially sensitive data, it could have been stated more clearly without transplanting the GDPR concepts. In general, the absence of an obvious anchor for these rights in a natural person creates ambiguity with regard to the rights-holder: is it the farm or the farmer, or other parties?

107 These voluntary charters are naturally limited in terms of sector-wide validity and enforcement, except for the external auditing system in the US Principles.[123] An additional limitation in both data charters is the primacy of contracts over principles. Rights can be limited and alienated from farmers by contracts even though a company declares its participation in the charters. Markets and bargaining power in contractual negotiations will determine the outcome despite the proposed rules/principles. Even if the EU and US regulators would turn the voluntary

117 Ibid., p. 11.

118 Here, exploitative abuse can come to mind as the fear seems to be related to charging higher prices for agricultural commodities according to the farmers' dependency on those particular products or inputs with the help of insights generated through aggregated farm data sets.

119 The EU Code, n. 15, p. 11.

120 Post Denmark I -Case C-209/10 EU:C:2012:172, para 30. See the situations where price discrimination can be exploitative of customers in Richard Whish and David Bailey, *Competition Law* (9th edn, Oxford University Press 2018), pp. 779-782. For an empirical study about price discrimination by powerful intermediaries, see, for example, Lauren Falcao Bergquist and Michael Dinerstein, 'Competition and Entry in Agricultural Markets: Experimental Evidence from Kenya' (2020) 110 American Economic Review.

121 Whish and Bailey, n. 120, pp. 777-778.

122 See, for instance, Jouanjean and others, n. 12 above, pp. 10 and 14-15.

123 There is a criticism about the ongoing practices of the Ag Data Transparent. See Mark R. Patterson, 'Ag Data Transparent, or Not' (*antitrust.online*, 2020) <https://antitrust.online/commentary/> accessed 4 March 2021.

principles proposed in the data charters into legally binding text, it is hard to see how they could correct B2B agricultural data market failures.[124]

108 These initiatives were not designed with a list of market failures and aftermarket competition concerns in mind. Instead, they transplanted rules designed to protect the privacy of individuals. One can, therefore, not expect these voluntary data governance initiatives in the US and EU to effectively address competition-related problems in this emerging sector.

E. Alternative Ways Forward

109 So far, we focused on situations where ag-tech machines are equipped with proprietary interfaces that collect data on devices and servers exclusively controlled by machine manufacturers or agronomic service providers. In the absence of data portability, farmers are locked into aftermarket services. They lose control over current and historical farm data. This monopolistic relationship distorts the market for data and related services.

110 In the previous section, we explored to what extent voluntary data governance initiatives based on agreements between farmers and agro-industry stakeholders could give farmers more choices. Our analysis demonstrated that contractual negotiations prevail in these agreements and leave farmers dependent on the goodwill of the providers of the services and devices that collect their data.

111 In this section, we first explore a market-based option: storing farm data with neutral third-party intermediary platforms[125] or data cooperatives[126] that are not vertically integrated with machine or inputs producers. We then discuss the possibilities for regulatory intervention in agricultural data markets by assigning mandatory data rights, including data portability right for farms.

I. Neutral Third-party Data Intermediaries

112 There is a wide variety of third-party intermediaries that operate in the agricultural data market. Some of them behave in a "neutral" way: they are not vertically integrated with machine producers, inputs suppliers or agronomic services providers. As such, they have no stake in the sales of these products and no incentive to use the data to promote these sales. Of course, there are various shades of neutrality: some are more neutral than others. They range from not-for-profit to purely commercial data intermediaries. Their common characteristic is that they offer farmers some degree of control over the management of their data, sometimes combined with the promise that they can monetise farm data or appropriate a larger share of the benefits that data can generate. These intermediaries have been referred to as "Agri-Business Collaboration and Data Exchange Facility" (ABCDEF),[127] i.e. "neutral" B2B data platforms where farmers and agri-businesses can collaborate and exchange data in standardized formats. This could purportedly strengthen the position of farmers in the data market. The European Commission announced its support for the creation of *"a common European agricultural data space to enhance the performance and competitiveness of the agricultural sector through the processing and analysis of production and other data, allowing for precise and tailored application of production approaches at farm level"*.[128] This agricultural data space might also fall in the category of neutral intermediaries. However, no further details are known yet on this project.

124 It is important to note that the Australian Farm Data Code does not allow contractual freedom to overrule the principles of the Code. Participating companies have to follow the declared rules. However, it has its own limitations deriving from legal design and preferred wording. For instance, in the Australian Code's 'Portability of farm data', there is no obligation for service providers to directly transfer data to rivals. Another principle of the Code obliges providers to preserve farmers' ability to determine who can access and use data. It is not clear if this is a one-shot access to historical data or it also covers access to real-time data flows. See Australian Code, n. 17, pp. 3-4. The New Zealand initiative is more related to transparency than a list of principles or data rights. There is an obligation for participating companies to disclose their practice regarding matters such as data security, rights to data and access rights. It does not intervene in contractual relations between companies and farmers. See New Zealand Farm Data Code of Practice, n. 17. In this regard, it falls behind the other initiatives.

125 See Eric A. Posner and E. Glen Weyl, *Radical Markets: Uprooting Capitalism And Democracy For A Just Society* (Princeton University Press 2018). The authors argue that data providers should create data unions, similar to labour unions, in order to extract a large value for their data contributions.

126 Apart from their potential to address competition concerns identified in this paper, there might also be other potential benefits as well as drawbacks of data cooperatives in agriculture. See Jouanjean and others, n. 12, p. 16.

127 See more in Poppe and others (2015), n. 2 above.

128 Communication from the European Commission "A European Data Strategy" COM (2020) 66.

113 The intermediary would act as a Farm Information Management System (FIMS),[129] comparable to Personal Information Management Systems (PIMS)[130] that have been suggested for personal data. They fulfil several roles: data storage, identity and permissions management, service and monetization management, standardized and secure data transfers through APIs, compliance management and accountability.

114 Large agri-business firms with vertically integrated data services are a step ahead of FIMS because they already have a large user base that they can leverage to generate network effects in data collection and better service production. It is not easy for FIMSs to overcome this disadvantage, unless they have a large and vertically integrated market side too. Some agricultural cooperatives may be in that situation as they sell agricultural inputs and rent machines. However, that makes them commercial stakeholders in at least one market and undermines their neutral third-party status. In France, for example, the InVivo agricultural group has started from its strong market position in agricultural products to add a data management and analytical dimension to its business.[131] There are many other examples of such intermediaries.[132] Some of these intermediaries have vertically integrated with data analytics firms. In the US, for example, GISC (Growers Information Services Cooperative) is an agricultural data cooperative that teamed up with IBM for data storage in the cloud to produce data analytics services that generate value-added on top of handling raw data.[133] Farmers pay for these services. This cooperative data business model retains some degree of neutrality with respect to products and services markets; it avoids self-preferencing in these markets. IBM has no stake in selling agricultural machinery or inputs, and it is neutral in this regard. As such, it may allocate a larger share of data-driven value-added to farmers. However, we do not have any information on the possibility for farmers to switch their data to other service providers than IBM.[134]

115 Other intermediaries have opted to stay neutral with regard to data analytics and use. They facilitate access and exchange of data but do not store or extract value from the data. For example, in the Netherlands, Join-Data is a not-for-profit agricultural data platform where farmers share their data with various agro-industry partners and companies that want to access data.[135] JoinData is set up by some large Dutch dairy and meat cooperatives involved in processing and distribution of agricultural inputs and livestock products. Some commercial firms are also members, including a bank and an IT services company that created the technical platform.[136] The platform manages data access authorisations for farms, but it does not store or analyse farm data. That is left to application providers. It is a mere passive and neutral data access & distribution platform, not an active data-driven agronomic services provider. It facilitates the transmission of data between farm machines and data users, including distributors of inputs and outputs, downstream industries, data-based agricultural service providers, with the authorisation of the farmer. JoinData membership terms & conditions do not say anything on ownership or access to data because it takes no responsibility for the handling of data. JoinData seeks to improve farmers' trust by giving them more control over the use of their data at any time, by means of

129 This notion has been discussed in the more technical data literature since 2012. See Alexandros Kaloxylos and others, 'Farm Management Systems and the Future Internet Era' (2012) 89 Computers and Electronics in Agriculture; Alexandros Kaloxylos and others, 'A Cloud-Based Farm Management System: Architecture and Implementation' (2014) 100 Computers and Electronics in Agriculture cited in Jan W. Kruize and others, 'A Reference Architecture for Farm Software Ecosystems' (2016) 125 Computers and Electronics in Agriculture, p. 14.

130 See 'Personal Information Management System' (*edps.europa*, 2020) <https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_en> accessed 4 March 2021.

131 'Big Data and Agriculture | Invivo' (*Invivo-group.com*, 2020) <https://www.invivo-group.com/en/big-data-and-agriculture/> accessed 4 March 2021.

132 Just to list a few: API-AGRO (https://api-agro.eu/en/) in France, DjustConnect (https://djustconnect.be/en/) in Belgium, DKE agrirouter (https://my-agrirouter.com/en/) in Germany, Agrimetrics (https://agrimetrics.co.uk/) in the UK, Farmobile (https://www.farmobile.com/) and Farm Business Network (https://www.fbn.com/analytics/data-storage-integration) in the US accessed 4 March 2021.

133 See 'Home - Grower's Information Services Coop' (*Grower's Information Services Coop*, 2020) <https://www.gisc.coop/> accessed 4 March 2021.

134 See also potential limitations of farmers' data cooperatives from the perspective of the data lock-in problem. Atik, n. 29, pp. 67-68.

135 See, for instance, Join-Data at 'Data Sharing in the Agricultural Sector | Support Centre For Data Sharing' (*Eudatasharing.eu*, 2020) <https://eudatasharing.eu/examples/data-sharing-agricultural-sector> accessed 4 March 2021.

136 It has several members including Friesland Campina (dairy) and Royal Agrifirm (a large cooperative provider of agricultural inputs), CRV, LTO, Royal Cosun, Avebe, Rabo Frontier Ventures, EDI-Circle (an IT firm in data management). See 'About Joindata – Joindata' (*Join-data.nl*, 2021) <https://join-data.nl/en/about-joindata/> accessed 4 March 2021.

authorisations. Farmers do not pay for the service. Data users pay a fee for data communication, not for the data itself. It does not build data interfaces to facilitate data portability. Application providers have to build their own interfaces. It uses the AgroConnect data standard for data transmission and for its APIs.[137] Most members of AgroConnect are active in downstream data-driven services; some are manufacturers of machines and sensor devices.[138]

116 This model comes closest to a neutral third-party data intermediary. It gives farmers more control over who can access and use their data, reduces switching costs and avoids data lock-in for farmers. Farmers gain more subjective control over their data. That does not necessarily translate into capturing more value-added from agronomic services. That still depends on the farmer's bargaining power with agro-service providers. It does not overcome the restrictions imposed by contracts between farmers and machines producers that may prevent them from accessing or porting their data, or may lock them into incompatible data formats. JoinData can only work when the original agreement with the data source (machine producer) allows it.

II. Neutral third-party data intermediaries face two major hurdles:

117 First, they require access to data sources. For example, the JoinData model works to the extent that data sources (machine producers) allow JoinData to manage the portability of their machine data. What would be their incentive to give away their exclusive access and allow other service providers to use their data? We can find some tentative answers to that question when looking at the membership list of JoinData's data interoperability standard, AgroConnect. Members are mostly downstream agricultural services providers,[139] not upstream producers of data collection machines. The few exceptions are small machine and sensor producers that have very little to gain from maintaining data exclusivity. Their business model consists of selling machines and sensors, not selling data-driven analytics. We find the same pattern in membership of the more widely used Isobus interoperability standard for agricultural machines: only smaller machine manufacturers adhere to it while none of the larger ones do, except for a few of their machines in markets where they are not leaders.[140] This is in line with the predictions from economic theory.[141] When a platform is small, it can only gain from interoperability. Conversely, if the platform is large, gain from interoperability will be limited while its competitor will gain more. Consequently, dominant platforms' incentives to accept interoperability will be low.

118 Second, they need to overcome several economic hurdles, similar to PIMS.[142] The parties (farmers, companies and platform operator) must find a sustainable data business model. That may be problematic. Farmers may not be willing to pay for storing and managing their raw data through FIMS, unless they receive well-defined monetary benefits in return. Some farmers may be motivated by the subjective feeling of more control over their data, independently of any monetary gains. Farmers may expect payment for the use of their raw data by agro-industry firms. This is unlikely to happen because the marginal value of individual farm data may be close to zero for a service provider as soon as it has reached a sufficiently large data pool where the marginal return to economies of scale and scope in aggregation come close to zero. That is why farmers usually have to pay a price for access to data-driven services, even if they deliver their own data to that service provider. New entrants in the data-driven services markets may subsidise data control services for farmers in order to attract more clients. This may be the case for JoinData. Eventually, however, full costs will have to be reflected on one or the other side of the market.

119 For data cooperatives, the only viable business model seems to require the production of data-based value-added services on top of the raw data delivered by farmers. This requires investment in data analytics as, for example, the case of the GISC in the US that collaborates with IBM to produce data-driven insights. Only large cooperatives with a sufficient volume of data collection can achieve the necessary economies of scale and scope in data aggregation to produce efficient data-driven services.

120 These economic considerations lead us to the conclusion that neutral third-party intermediaries are likely to remain outside the mainstream agricultural data market. It also raises questions

137 See 'Member List' (*Agroconnect.nl*, 2020) <https://www.agroconnect.nl/overagroconnect/ledenlijst.aspx> accessed 4 March 2021.

138 See Ibid.

139 Ibid.

140 See 'Members' (*CC-ISOBUS*, 2020) <https://www.cc-isobus.com/en/das-cci/> accessed 4 March 2021.

141 Crémer, Rey and Tirole, n. 31 above.

142 See more about PIMS, for example, in Krämer, Senellart and de Streel, n. 63, pp. 66-75.

about the potential benefits and limitations of voluntary interoperability and whether mandatory standards are necessary to overcome data-related competition bottlenecks in agricultural markets. We address this question in the next section.

III. Regulatory Intervention with Mandatory Rules

121 In this section, we explore regulatory intervention as an alternative to overcome exclusive data access by device manufacturers and agronomic service providers. Data portability and/or interoperability is a necessary technical condition to unlock farm data.[143] However, it does not answer the question of who can use the portability or access rights and under which conditions. That is an important question because it affects the welfare of stakeholders in the agricultural production process. Policymakers can introduce mandatory portability to increase the joint welfare of farmers, agricultural industry and service providers, and consumers. The impact on these groups may not be evenly distributed, however, and can create equity and fairness concerns.

122 For personal data, the data subject as a natural person and originator of the data is the obvious rights holder and the basis for data protection rights in the GDPR. We argued in Section C that there is no equivalent for non-personal farm data, unless there is only one single data originator. When several parties contribute to an agricultural production process, they may all claim access rights to at least part of the data. Landowners may claim access to land use data from tenant farmers. Machine rental companies may compile usage data. Machine producers may collect data from all their machines. Agronomic service providers may collect data from all their client farms. Data analytics and other external service providers may claim use rights on the data that they process.

123 Some authors have suggested to distinguish between volunteered, observed and inferred data as a way to allocate data access rights.[144] Volunteered data have been willingly contributed by a user to service providers. For example, farms share their land and soil maps with rented seeding, fertilizer and harvest machines. Observed data are the result of interactions between users and the service provider. For example, combine harvesters collect data on the quantity of crops harvested. Fertilizer machines observe the type and quantity of chemicals used. Volunteered and observed are raw primary data. Inferred data are derived from raw data and produced by a data service provider by means of algorithms or other calculations and transformations. For example, raw land & soil maps and cropping pattern data are inputs for algorithms that recommend chemicals for crop protection. Combined with harvesting data, they can evaluate the productivity of a farm. Apart from the fact that the distinction between these three categories is not always clear, this categorisation does not resolve the question of who should get access to which type of data and under what conditions.

124 Currently, in the EU, portability right exists only for personal data in the GDPR. Even this right has significant limitations.[145] A very limited legal notion of portability right for non-personal data is mentioned in the Free Flow of Data Regulation,[146] only for cloud-based data services and on a voluntary basis through sectoral codes of conduct to be negotiated between industry stakeholders. In other words: it merely endorses the existing EU agricultural data charter. Other sectoral precedents for portable machine data exist, for example, in automotive,[147] energy[148] and payments services.[149]

143 See, for instance, Jouanjean and others, n. 12, p. 18.

144 Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, 'Competition Policy for the digital era - Final Report' (Publications Office of the European Union 2020), pp. 24-29.

145 See, n. 63 above.

146 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, Article 6.

147 Regulation 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC, OJ L 151/1, 14.6.2018, Articles 61-66.

148 Directive 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast), OJ L 158/125, 14.6.2019, Article 23.

149 Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337/35, 23.12.2015, Articles 66-67.

125 The proposed Data Governance Act[150] includes regulation of data sharing services. Article 9 restricts the application of the regulation to three categories of data intermediaries: providers of bilateral or multilateral data exchange services, personal data sharing services and data cooperatives. Recital 22 explains that providers of data sharing services are specialised intermediaries that are independent from both data holders and data users. They assist both parties in their transactions of data assets. It covers services that intermediate between an indefinite number of data holders and users, not closed groups or an exchange platform that is exclusively linked to services provided by one data holder. It also excludes IoT data platforms that connect machines and devices, and services that generate value-added from the transformation and analysis of data without a direct relationship between data holders and users. We could not find any type of agricultural data service provider that would still fall within this very narrow definition of data sharing services. This leaves the category of data cooperatives as an alternative option. However, this category is not defined in the regulation. Even if there would be any agricultural data platforms that could be considered as data intermediary services under Article 9, the conditions that apply to these platforms under Article 11 are very general and do not go beyond what is already foreseen in the EU code of conduct that is investigated in detail in the section above.

126 The Digital Markets Act (DMA)[151] defines mandatory B2B data sharing obligations for (non-personal) commercial data. This applies only to very large "gatekeeper platforms" that provide "core platform services". Agricultural data services are not covered by these DMA definitions. However, it is worth noting that DMA Article 6(h) introduces a real-time data portability right for business users on gatekeeper platforms. Article 6(i) mandates free access for business users to non-personal commercial data provided and generated by their activities on the platform. These articles introduce data access and portability rights for legal entities (i.e. businesses). Moreover, they go beyond the GDPR by abolishing any delays and mandating real-time access.

127 These clauses constitute a first step towards portability rights for non-personal commercial business data in the EU. While the DMA does not apply to agricultural data platforms, the European Commission announced its intention to prepare proposals for a Data Act in 2021. It would include general regulatory provisions for B2B sharing of non-personal and machine-generated data.[152] The details of this proposal are not known yet.

128 We can explore the conditions under which non-personal data portability rights could work for farms as business entities[153] and how this could increase competition in aftermarket services. In a simple one-to-one relationship between a farm and a machine or device producer, real-time portability and interoperability of machine data would separate primary machine markets from aftermarket services. It would enable farmers to select any aftermarket service provider of their choice. This would increase competition in aftermarkets. For example, a tractor or seeding machine could be steered by data-driven services from any provider. However, it would not prevent service providers from re-using the data for other purposes or sharing them with other businesses, unless re-use would be subject to consent from the farm to which the data pertain. One could think of a farm-centric portability and re-use right, limited to farms only and excluding other parties.

129 Exclusive rights for farms become complicated when more parties are involved in the agricultural production process. The farm's central role in data collection may be eroded by competing data access claims from other parties. For example, machines can be owned by leasing firms, farmland can be owned by another party, farm data analytics and agronomic advisory services can be performed by a third party, etc. Leasing firms can claim access to machine data to monitor the use and performance of their machines; land owners may claim access to data on agricultural activities to monitor the quality of their land; and agronomic advisory services firms may claim rights over the service data that they produce. This leads to a debate on who gets access to which data under which conditions. Leasing firms may be granted access to mechanical machine data only, not to the quantity and quality of agricultural inputs and outputs. Land owners may, however, want to access data on the quantity and quality of inputs and outputs because that affects the quality and value of their land. Once these parties obtain a right to access these data, they may also claim the right to re-use the data without the consent of the farm.

150 Proposal for a Regulation (COM/2020/767 final) of the European Parliament and of the Council on European data governance (Data Governance Act), 25.11.2020.

151 Proposal for a Regulation (COM/2020/842 final) of the European Parliament and of the Council of on contestable and fair markets in the digital sector (Digital Markets Act), 15.12.2020.

152 See 'Legislative Train Schedule | A Europe Fit For The Digital Age' (*European Parliament*, 2021) <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-data-act> accessed 4 March 2021.

153 Focusing on farms as legal persons instead of farmers as natural persons is important for the effectiveness of the portability design in the sector. See section D.I above.

130 Data access and re-use by other parties is valuable from a social welfare perspective. It enables these parties to improve the efficiency and economic value of their activities. At the same time, re-use may also impact the farm. Detailed land use data can affect the value of farmland and the creditworthiness of the farm. More reliable valuations are beneficial for society but not necessarily for the farm as a private undertaking. They may be used for price discrimination and speculation that are explicitly rejected in the EU code of conduct.

131 Like intellectual property rights, data need to have some degree of excludability in order to retain their market value. Making them widely available reduces their value to near-zero.[154] However, it may increase competition in downstream services markets, reduce prices and increase service quality. That may have positive welfare effects on farms via the services price channel. More competition in data-driven aftermarket services would help farmers to appropriate a larger share of data-driven productivity gains through lower prices and better service quality.[155]

132 The design of data access regimes is squeezed between two extremes. On the one hand, granting exclusive rights to farms when many parties contribute to the agricultural production process is not an optimal solution. On the other hand, generalised data portability and re-use for all is not ideal when negative externalities occur between parties. An intermediate solution that keeps some restrictions may be required to preserve the rights and welfare of some parties. All this indicates that a data access regime should be tailored to specific situations.

133 Smith warns us that the cost of intermediate data governance or data pooling regimes can be very high compared to the much lower costs of private ownership rights or fully open public domain regimes.[156] However, each of these cheaper regimes has its own costs. Public domain or full data sharing regimes may lead to underinvestment for lack of private incentives while exclusive private ownership data regimes lead to underutilisation of resources. Expensive data governance regimes should only be implemented if the benefits to society exceed the cost of governance.

F. Summary and Conclusions

134 The arrival of digital data in agriculture opens the possibility to realize productivity gains through precision farming. It also raises questions about the distribution of these gains between farmers and agricultural service providers. It is tempting to believe that farmers can appropriate a large share of these gains when they remain in control of farm data. The reality of data-driven agricultural business models is that manufacturers of agricultural machines and devices design the data architecture in such a way as to retain exclusive control over access to the data. That enables them to foreclose downstream agricultural services markets that depend on these data. Also, agricultural technology providers' *de facto* control on the historical farm data sets locks their customer farmers in their systems due to the lack of a clear mechanism to force these companies to transfer the related data when farmers desire to switch service providers. This reduces competition in these markets and may increase prices which eventually reduces farmers' welfare.

135 Personal data protection regulation with its right to data portability is not applicable to non-personal agricultural machine data. Other existing regulations do not have any undisputedly equivalent mechanism to unchain farmers. Attempts to introduce voluntary data charters in the EU and US that emulate GDPR-like principles and purport to give farmers more control over their data have not been successful so far. Market-based outcomes still take precedence over farmers rights enshrined in the contracts. Farmers' bargaining power is reduced because third-party data platforms are a necessary intermediary to realize economies of scale and scope from data aggregation in addition to the fact that farmers need tailored data-driven prescriptions/solutions generated through these intermediaries' advanced algorithms. Farmers cannot achieve these benefits on their own. The low marginal value of individual farm data and farmers' need for tailored data-driven services put farmers in a weak bargaining position. For-profit and non-profit intermediaries that are not vertically integrated into agricultural machines, inputs or services, or pure data cooperatives, have tried to offer better deals to farmers. However, they can only circumvent monopolistic data lock-ins when they can access the data sets. That depends on the goodwill of the machine manufacturers or agronomic service providers. Moreover, they may

154 Dirk Bergemann and Alessandro Bonatti, 'Markets for Information: An Introduction' (2018) CERP Discussion Paper – N. DP13148; Bergemann, Bonatti and Gan, n. 57 above.

155 For a theoretical economic model that arrives at this conclusion, see, for example, Paul Belleflamme and Martin Peitz, 'Platforms and Network Effects' in Luis C. Corchón and Marco A. Marini (eds), *Handbook of Game Theory and Industrial Organization, Volume II* (Edward Elgar 2018).

156 Henry Smith, 'Toward an Economic Theory of Property in Information' in Kenneth Ayotte and Henry E. Smith (eds), *The Research Handbook on the Economics of Property Law* (Edward Elgar 2011).

have a hard time to achieve economies of scale and scope in data analytics and generate additional data-driven value-added. Without that, their business model may not be sustainable.

136 This leaves regulatory intervention as a last resort with mandatory data portability and interoperability to overcome data lock-in and monopolistic market failures. That inherently raises the question of the allocation of access rights: who should get access rights to which data and under which conditions? This is complicated when many parties contribute data to the production process and may claim access rights. Minor changes in who gets access to which data under which conditions may have significant effects on stakeholders. There is no clear answer yet to these questions. We conclude that digital agriculture still has some way to go to reach equitable and efficient solutions for detailed data access rights.

137 The European Commission's forthcoming proposals for a Data Act will have to address these issues in order to set the conditions for access to and sharing of non-personal machine data in a wide range of industries where hardware devices are used in Internet-of-Things settings. Regulators should design regimes with a view to maximise social welfare for society as a whole, not the private welfare of individual stakeholder groups.

COVID-19, Pandemics, and the National Security Exception in the TRIPS Agreement

by **Emmanuel Kolawole Oke***

Abstract: As a result of the COVID-19 pandemic, a number of scholars and commentators have suggested that states can invoke the national security exception in Article 73(b)(iii) of the TRIPS Agreement to enable the suspension of patent laws in order to facilitate the production and importation of patented medicines and vaccines. This article therefore critically assesses the extent to which states can realistically invoke the national security exception in response to the COVID-19 pandemic. Drawing on two recent rulings by WTO Panels in both Russia – Traffic in Transit (2019) and Saudi Arabia – Intellectual Property Rights (2020) where the nature and scope of the national security exception wasanalysed, the article acknowledges that states may be able to invoke the national security exception in response to pandemics such as COVID-19. However, the article contends that the invocation of the national security exception in this context may not actually be helpful to states that do not possess local manufacturing capacity. Furthermore, the article argues that the national security exception cannot be used to obviate the strictures contained in Article 31bis of the TRIPS Agreement. It is therefore doubtful whether the national security exception in the TRIPS Agreement is a realistic option for states that do not possess local manufacturing capacity.

Keywords: COVID-19; security exception; TRIPS Agreement; manufacturing capacity; medicines; vaccines, pandemics

Recommended citation: Emmanuel Kolawole Oke, COVID-19, Pandemics, and the National Security Exception in the TRIPS Agreement, 12 (2021) JIPITEC 397 para 1.

A. Introduction

1 Article 73 of the World Trade Organization's (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)[1] provides for security exceptions that states can invoke to defend their non-compliance with the TRIPS Agreement. This is a unique provision in the context of international intellectual property law. Crucially, the major intellectual property treaties that were in existence before the TRIPS Agreement i.e. the Berne Convention for the Protection of Literary and Artistic Works (Berne Convention)[2] and the Paris Convention for the Protection of Industrial Property (Paris Convention)[3] do not contain any security exceptions.

* Lecturer in International Intellectual Property Law, Edinburgh Law School, University of Edinburgh. Email: emmanuel.oke@ed.ac.uk

1 Agreement on Trade-Related Aspects of Intellectual Property Rights, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, April 1994, 1869 U.N.T.S. 3; 33 I.L.M. 1197 (1994).

2 Berne Convention for the Protection of Literary and Artistic Works, 1886, as last revised at Paris in 1971 and as amended in 1979, 828 U.N.T.S. 221.

3 Paris Convention for the Protection of Industrial Property, 1883, as last revised at Stockholm in 1967 and as amended in 1979, 828 U.N.T.S. 305.

Article 73 of the TRIPS Agreement mirrors similar provisions in Article XXI of the WTO's General Agreement on Tariffs and Trade (GATT) and Article XIV *bis* of the General Agreement on Trade in Services (GATS) and it provides that:

> *Nothing in this Agreement shall be construed:*
>
> *(a) to require a Member to furnish any information the disclosure of which it considers contrary to its essential security interests; or*
>
> *(b) to prevent a Member from taking any action which it considers necessary for the protection of its essential security interests;*
>
> *(i) relating to fissionable materials or the materials from which they are derived;*
>
> *(ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment;*
>
> *(iii) taken in time of war or other emergency in international relations; or*
>
> *(c) to prevent a Member from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.*

2 The recognition of the need to permit states to be excluded from their obligations under the TRIPS Agreement in order to protect their essential security interests confirms the central role of the principle of territoriality in international trade law generally and in international intellectual property law specifically. This principle is connected to the concept of state sovereignty in international law and it is the foundational principle in international intellectual property law.[4] Article 73 of the TRIPS Agreement therefore reaffirms the ability of states to take steps to secure their sovereign interests even in the context of international intellectual property law.[5]

3 Nevertheless, the precise scope of these security exceptions has been unclear until very recently. Fortunately, Article XXI of the GATT and Article 73 of the TRIPS Agreement have been considered and interpreted by two WTO dispute settlement panels.[6] Prior to these two decisions, a number of states took the view that these exceptions were "self-judging" and could not be subject to adjudication via the

4 See, Susy Frankel, 'WTO Application of the Customary Rules of Interpretation of Public International Law to Intellectual Property' (2006) 46(2) *Virginia Journal of International Law* 365, 371 (noting that, "[d]espite the growth of intellectual property in international trade, intellectual property remains a territorial creature and an owner of an intellectual property right must claim that right on a territory-by-territory basis."). See also, Lydia Lundstedt, *Territoriality in Intellectual Property Law* (Stockholm University, 2016) 91; Hans Ullrich, 'TRIPS: Adequate Protection, Inadequate Trade, Adequate Competition Policy' (1995) 4(1) *Pacific Rim Law & Policy Journal* 153, 159 (noting that, "...intellectual property, whether it is a patentable invention or a copyrightable work, is national by nature. Therefore, it must be acquired, maintained, and defended independently from one country to the other. In fact, the conditions governing the acquisition, existence, maintenance, validity, scope, and termination of intellectual property vary widely from one country to the other. The privilege granted to the owner of the intellectual property to exclusively exploit a right, extends to the entire territory of the state granting protection, but is also limited to this territory."); Peter Yu, 'A Spatial Critique of Intellectual Property Law and Policy' (2017) 74(4) *Washington & Lee Law Review* 2045, 2064 (stating that, "Territoriality is the bedrock principle of the intellectual property system, whether the protection concerns copyrights, patents, trademarks, or other forms of intellectual property rights. This principle not only carefully identifies the prescriptive jurisdiction, but also helps set boundaries for protection within and outside the country. Strongly supported by the principle of national sovereignty, the territoriality principle aims to address concerns about international comity.").

5 See also, UNCTAD-ICTSD, *Resource Book on TRIPS and Development* (CUP, 2005) 801 (noting that, "Although there is a relatively widespread tendency among scholars to perceive international trade law as a concept differing from the classical idea of state sovereignty and to regard national security, borders and territory as state interests difficult to reconcile with liberalization of markets, the provision of Article 73, almost identical to Article XXI of the GATT and Article XIV *bis* of the GATS, proves that these traditional state interests continue to be a major concern of WTO Members.").

6 See, WTO, *Russia – Measures Concerning Traffic in Transit*, Panel Report, WT/DS512/R (5 April 2019) (interpreting Article XXI of the GATT); WTO, *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, Panel Report, WT/DS567/R (16 June 2020) (interpreting Article 73 of the TRIPS Agreement). It should be noted that Saudi Arabia has launched an appeal against this decision to the WTO's Appellate Body. This means that the panel report in this case cannot be considered for adoption by the WTO's dispute settlement body until the conclusion of the appeal. As the Appellate Body is currently non-functional due to disagreements among WTO members regarding the appointment of members to the Appellate Body, it is not yet clear as at the time of writing when this appeal will be resolved. See, WTO, *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights*, Notification of an Appeal by the Kingdom of Saudi Arabia, WT/DS567/7 (30 July 2020).

WTO dispute settlement system.[7] In this regard, it is worth noting that the most relevant exception in the context of pandemics is the one contained in Article 73(b)(iii) of the TRIPS Agreement which permits a state to take "any action which it considers necessary for the protection of its essential security interests" during the "time of war or other emergency in international relations". Thus, Article 73(b)(iii) and how it has been interpreted and applied will be the focus of the analysis in this article.

4 In the light of the coronavirus (COVID-19) pandemic of 2019/2020, Article 73(b)(iii) has gained some prominence. This is because some scholars and commentators have suggested that states could invoke this provision in defence of measures aimed at suspending the protection and enforcement of intellectual property rights in order to facilitate the purchase, importation, or production of diagnostics, vaccines, and medicines that they need to address the COVID-19 pandemic.[8] Therefore, this article will also critically consider the extent to which states can invoke Article 73(b)(iii) to facilitate access to diagnostics, vaccines, and medicines during a pandemic such as COVID-19. While the discussion in this regard is focused on COVID-19, the arguments made here are equally applicable to other pandemics that may occur in the future.

5 The rest of this article is structured into three main sections. Section B will focus on the historical approach of states to the security exceptions as "self-judging". In this regard, attention will be paid to how the security exceptions were construed in the pre-WTO era. Section C will focus on the recent jurisprudence emanating from the WTO dispute settlement panels regarding the interpretation of Article XXI of GATT and Article 73 of the TRIPS Agreement. Attention will also be paid to the question of whether states can, in theory, invoke Article 73(b)(iii) of the TRIPS Agreement in response to pandemics such as COVID-19. Section D will thereafter critically assess whether the invocation of Article 73(b)(iii) is a realistic option for states in the fight against pandemics, especially those states that do not possess local manufacturing capacity.

B. The Historical Approach to the National Security Exceptions in International Trade Law

6 Prior to the adoption of the WTO Agreement that created the WTO in 1994, security exceptions were contained in Article XXI of GATT 1947 which was meant to be part of the Havana Charter for an International Trade Organisation that never came into force. However, the provisions of GATT 1947 remained in force provisionally until it was incorporated (with some adjustments) into GATT 1994 which is a component of the current WTO Agreement. Thus, the "provisions of the GATT 1947, incorporated into the GATT 1994, continue to have legal effect as part of the GATT 1994, itself a component of the WTO Agreement."[9] There was, however, no legal interpretation of Article XXI of GATT 1947 prior to its transformation into the current Article XXI of GATT 1994 although a number of states took the view that it was a "self-judging" provision.

7 For instance, during the accession of Portugal to GATT in 1961, Ghana invoked Article XXI(b)(iii) in support of its decision to impose a ban on goods entering Ghana from Portugal and it noted that "under this Article each contracting party was the sole judge of what was necessary in its essential security interests."[10] According to Ghana:

7 See, GATT, *Analytical Index: Guide to GATT Law and Practice* (1995) 599-610. See further, Tania Voon, 'The Security Exception in WTO Law: Entering a New Era' (2019) 113 *AJIL Unbound* 45.

8 See, South Centre, 'COVID-19 Pandemic: Access to Prevention and Treatment is a Matter of National and International Security: Open Letter from Carlos Correa, Executive Director of the South Centre' (4 April 2020) available at <https://www.southcentre.int/wp-content/uploads/2020/04/COVID-19-Open-Letter-REV.pdf> (urging the Director-Generals of the WHO, WIPO, and WTO to "support developing and other countries, as they may need, to make use of Article 73(b) of the TRIPS Agreement to suspend the enforcement of any intellectual property right (including patents, designs and trade secrets) that may pose an obstacle to the procurement or local manufacturing of the products and devices necessary to protect their populations."); Henning Grosse Ruse-Khan, 'Access to Covid-19 Treatment and International Intellectual Property Protection – Part II: National Security Exceptions and Test Data Protection' *EJIL:Talk!* (15 April 2020) available at <https://www.ejiltalk.org/access-to-covid19-treatment-and-international-intellectual-property-protection-part-ii-national-security-exceptions-and-test-data-protection/>; Nirmalya Syam, 'Intellectual Property, Innovation and Access to Health Products for COVID-19: A Review of Measures Taken by Different Countries', South Centre Policy Brief No. 80 (June 2020) 4; Frederick Abbott, 'The TRIPS Agreement Article 73 Security Exceptions and the COVID-19 Pandemic', South Centre Research Paper 116, (August 2020).

9 See, WTO, 'GATT 1947 and GATT 1994: What's the Difference?' available at <https://www.wto.org/english/docs_e/legal_e/legalexplgatt1947_e.htm>

10 GATT, Contracting Parties Nineteenth Session, 'Summary Record of the Twelfth Session' SR.19/12 (21 December 1961) 196.

> *There could therefore be no objection to Ghana regarding the boycott of goods as justified by its security interests. It might be observed that a country's security interests may be threatened by a potential as well as an actual danger. The Ghanaian Government's view was that the situation in Angola was a constant threat to the peace of the African continent and that any action which, by bringing pressure to bear on the Portuguese Government, might lead to a lessening of this danger, was therefore justified in the essential security interests of Ghana. There could be no doubt also that the policy adhered to by the Government of Portugal in the past year had led to an emergency in international relations between Portugal and African States.*[11]

8 Also, during the GATT Council discussions in 1982 of the trade restrictions imposed on Argentina for non-economic reasons by the European Economic Community (EEC), Canada, and Australia, similar sentiments were expressed by these states to justify their restrictions against imports from Argentina into their territories.[12] In this regard, the EEC took the view that it had acted on the basis of its inherent rights "of which Article XXI of the General Agreement was a reflection" and that the "exercise of these rights constituted a general exception, and required neither notification, justification, nor approval" because "every contracting party was - in the last resort - the judge of its exercise of these rights."[13] Canada contended that "the situation which had necessitated the measures had to be satisfactorily resolved by appropriate action elsewhere, as the GATT had neither the competence nor the responsibility to deal with the political issue which had been raised."[14] Australia also argued that its "measures were in conformity with the provisions of Article XXI:(c), which did not require notification or justification."[15]

9 In addition, apart from taking the view that the security exceptions in GATT 1947 were self-judging, some states also took the view that the invocation of this exception could neither be reviewed by members of GATT nor by a dispute settlement panel. Thus, after the United States imposed a trade embargo against Nicaragua in 1985, a panel was established to examine the measures of the United States but the terms of reference of the panel precluded it from examining the motivation for or the validity of the invocation of Article XXI(b)(iii) by the United States. Ultimately, the panel could not provide a legal interpretation of Article XXI(b)(iii) and, in a report which was not adopted, the panel held in this regard that:

> *The Panel first considered the question of whether any benefits accruing to Nicaragua under the General Agreement had been nullified or impaired as the result of a failure of the United States to carry out its obligations under the General Agreement (Article XXIII:1(a)). The Panel noted that, while both parties to the dispute agreed that the United States, by imposing the embargo, had acted contrary to certain trade-facilitating provisions of the General Agreement, they disagreed on the question of whether the non-observance of these provisions was justified by Article XXI(b)(iii)...*
>
> *The Panel further noted that, in the view of Nicaragua, this provision should be interpreted in the light of the basic principles of international law and in harmony with the decisions of the United Nations and of the International Court of Justice and should therefore be regarded as merely providing contracting parties subjected to an aggression with a right to self-defence. The Panel also noted that, in the view of the United States, Article XXI applied to any action which the contracting party taking it considered necessary for the protection of its essential security interests and that the Panel, both by the terms of Article XXI and by its mandate, was precluded from examining the validity of the United States' invocation of Article XXI.*
>
> *The Panel did not consider the question of whether the terms of Article XXI precluded it from examining the validity of the United States' invocation of that Article as this examination was precluded by its mandate. It recalled that its terms of reference put strict limits on its activities because they stipulated that the Panel could not examine or judge the validity of or the motivation for the invocation of Article XXI:(b)(iii) by the United States (cf. paragraph 1.4 above). The Panel concluded that, as it was not authorized to examine the justification for the United States' invocation of a general exception to the obligations under the General Agreement, it could find the United States neither to be complying with its obligations under the General Agreement nor to be failing to carry out its obligations under that Agreement.*[16]

10 The above sums up the approach of a number of states to the security exceptions in the GATT. Essentially, some states took the view that the invocation of Article XXI of GATT was a matter solely within the scope of the discretion available to states under international trade law. Thus, they contended that the motivations for invoking any of the security exceptions could not be reviewed by a dispute settlement panel. As there was no legal interpretation of Article XXI, the uncertainty

11 Ibid.

12 GATT, Council, 'Minutes of Meeting' C/M/157 (22 June 1982).

13 GATT, Council, 'Minutes of Meeting' C/M/157 (22 June 1982) 10.

14 Ibid.

15 Ibid 11.

16 *United States – Trade Measures Affecting Nicaragua*, Report by the Panel, L/6053, (13 October 1986) paras 5.1-5.3.

surrounding the scope of the security exceptions continued until and after the adoption of the WTO Agreement in 1994.

C. The Recent Clarification of the Scope of Article 73(b)(iii) and its Applicability in the Context of Pandemics

11 The uncertainty surrounding the interpretation and scope of the security exceptions continued even after the adoption of GATT 1994 and the TRIPS Agreement until 2019 when Article XXI(b)(iii) of GATT 1994 was interpreted and applied by the WTO dispute settlement panel in *Russia – Measures Concerning Traffic in Transit* (hereinafter, *Russia – Traffic in Transit*). Moreover, in 2020, Article 73(b)(iii) of the TRIPS Agreement which is identical to Article XXI(b)(iii) of GATT 1994 was also interpreted by a panel in *Saudi Arabia – Measures Concerning the Protection of Intellectual Property Rights* (hereinafter, *Saudi Arabia – Intellectual Property Rights*). The decisions of both panels will thus be used to analyse the scope of Article 73(b)(iii) of the TRIPS Agreement.

12 In *Saudi Arabia – Intellectual Property Rights,* Saudi Arabia invoked the security exception in Article 73(b)(iii) of the TRIPS Agreement to justify its measures that prevented a company headquartered in Qatar, beIN, from obtaining Saudi legal counsel to enforce its intellectual property rights through civil enforcement procedures before Saudi courts and tribunals. This violated its obligation under Article 42 of the TRIPS Agreement. Saudi Arabia also invoked this exception to justify its refusal to apply criminal procedures to beoutQ, a company subject to its jurisdiction that was engaged in wilful copyright piracy on a commercial scale through its unauthorised distribution and streaming of media content belonging to beIN (in violation of its obligation under Article 61 of the TRIPS Agreement).

13 In defining the applicable legal standard in this regard, the panel in *Saudi Arabia – Intellectual Property Rights* adopted the analytical framework that was developed by the panel in *Russia – Traffic in Transit* in the context of Article XXI(b)(iii) and it listed the following four factors that need to be considered in this regard:

> *(a) whether the existence of a "war or other emergency in international relations" has been established in the sense of subparagraph (iii) to Article 73(b);*
>
> *(b) whether the relevant actions were "taken in time of" that war or other emergency in international relations;*
>
> *(c) whether the invoking Member has articulated its relevant "essential security interests" sufficiently to enable an assessment of whether there is any link between those actions and the protection of its essential security interests; and*
>
> *(d) whether the relevant actions are so remote from, or unrelated to, the "emergency in international relations" as to make it implausible that the invoking Member considers those actions to be necessary for the protection of its essential security interests arising out of the emergency.*[17]

14 In relation to the first factor, i.e. whether the existence of a "war or other emergency in international relations" has been established, the panel in *Russia – Traffic in Transit* took the view that this should be objectively determined and not decided through the subjective discretionary determination of the state invoking the exception.[18] Thus, the panel rejected the argument that Article XXI(b)(iii) is self-judging and it also rejected Russia's argument that the panel lacks jurisdiction to review Russia's invocation of Article XXI(b)(iii).[19] According

17 *Saudi Arabia – Intellectual Property Rights*, para 7.242. The panel justified its decision to adopt the analytical framework developed by the panel in *Russia – Traffic in Transit* in footnote 752 where it noted that: "Where two sets of exceptions from obligations use similar language and requirements and set out their provisions in the same manner, the Appellate Body has considered prior panel and Appellate Body reports concerning the first set of exceptions to be relevant for its analysis under a second set of exceptions. (See Appellate Body Reports, *US – Gambling*, para. 291 (finding previous decisions under Article XX of the GATT 1994 relevant for its analysis under Article XIV of the General Agreement on Trade in Services (GATS)); and *Argentina – Financial Services*, para. 6.202 (referring to the Appellate Body's interpretation of Article XX(d) of the GATT 1994 in *Korea – Various Measures on Beef* to set out its analytical framework for Article XIV(c) of the GATS).)". Considering the differences between the GATT and the TRIPS Agreement, it has been questioned whether the panel in *Saudi Arabia – Intellectual Property Rights* should have adopted the analytical framework developed in the context of Article XXI of the GATT in its interpretation of Article 73 of the TRIPS Agreement. In this regard, see Caroline Glöckle, 'The Second Chapter on a National Security Exception in WTO Law: The Panel Report in Saudi Arabia – Protection of IPR' *EJIL: Talk!* (22 July 2020) available at < https://www.ejiltalk.org/the-second-chapter-on-a-national-security-exception-in-wto-law-the-panel-report-in-saudi-arabia-protection-of-ipr/>. See further, Susy Frankel, 'The Applicability of GATT Jurisprudence to the Interpretation of the TRIPS Agreement' in Carlos Correa (ed.), *Research Handbook on the Interpretation and Enforcement of Intellectual Property under WTO Rules* (Edward Elgar, 2010) 3-23.

18 *Russia – Traffic in Transit*, paras 7.71, 7.100.

19 Ibid paras 7.102-7.103.

to the panel, the clause "which it considers" in the chapeau of Article XXI(b) "does not extend to the determination of the circumstances in each subparagraph" listed in Article XXI(b).[20] This makes it clear that the determination of the existence of a war or other emergency in international relations is not within the discretion available to states in this regard.

15 The panel in *Russia – Traffic in Transit* arrived at this conclusion for a number of reasons. According to the panel, "the three sets of circumstances under subparagraphs (i) to (iii) of Article XXI(b) operate as limitative qualifying clauses; in other words, they qualify and limit the exercise of the discretion accorded to Members under the chapeau to these circumstances."[21] The panel also examined the negotiating history of Article XXI of GATT 1947 and it concluded in this regard that the drafters considered that:

> *(a) the matters later reflected in Article XX and Article XXI of the GATT 1947 were considered to have a different character, as evident from their separation into two articles;*
>
> *(b) the "balance" that was struck by the security exceptions was that Members would have "some latitude" to determine what their essential security interests are, and the necessity of action to protect those interests, while potential abuse of the exceptions would be curtailed by limiting the circumstances in which the exceptions could be invoked to those specified in the subparagraphs of Article XXI(b); and*
>
> *(c) in the light of this balance, the security exceptions would remain subject to the consultations and dispute settlement provisions set forth elsewhere in the Charter.*[22]

16 The panel thus concluded in this regard that "there is no basis for treating the invocation of Article XXI(b)(iii) of the GATT 1994 as an incantation that shields a challenged measure from all scrutiny."[23]

With regard to the term "emergency in international relations", the panel observed that:

> *the reference to "war" in conjunction with "or other emergency in international relations" in subparagraph (iii), and the interests that generally arise during war, and from the matters addressed in subparagraphs (i) and (ii), suggest that political or economic differences between Members are not sufficient, of themselves, to constitute an emergency in international relations for purposes of subparagraph (iii). Indeed, it is normal to expect that Members will, from time to time, encounter political or economic conflicts with other Members or states. While such conflicts could sometimes be considered urgent or serious in a political sense, they will not be "emergencies in international relations" within the meaning of subparagraph (iii) unless they give rise to defence and military interests, or maintenance of law and public order interests.*
>
> *An emergency in international relations would, therefore, appear to refer generally to a situation of armed conflict, or of latent armed conflict, or of heightened tension or crisis, or of general instability engulfing or surrounding a state. Such situations give rise to particular types of interests for the Member in question, i.e. defence or military interests, or maintenance of law and public order interests.*[24]

17 In *Saudi Arabia – Intellectual Property Rights*, the panel held that there was a situation of heightened tension or crisis which is related to Saudi Arabia's defence or military interests or maintenance of law and public order interests sufficient to establish an emergency in international relations that has persisted since 5 June 2017.[25] The panel arrived at this conclusion for a number of reasons including, inter alia, the fact that Saudi Arabia severed diplomatic and economic ties with Qatar in 5 June 2017.[26] According to the panel, the severance of all diplomatic and economic ties could be considered as "the ultimate State expression of the existence of an emergency in international relations."[27] The panel also supported its conclusion in this regard by referring to Saudi Arabia's accusation against Qatar that the latter is supporting terrorism and extremism. As the panel pointed out, "when a group of States repeatedly accuses anotherof supporting terrorism and extremism … that in and of itself reflects and contributes to a "situation … of heightened tension or crisis" between them that relates to their security interests."[28]

20 Ibid para 7.101. See also, ibid para 7.82 (holding that, "the ordinary meaning of Article XXI(b)(iii), in its context and in light of the object and purpose of the GATT 1994 and the WTO Agreement more generally, is that the adjectival clause "which it considers" in the chapeau of Article XXI(b) does not qualify the determination of the circumstances in subparagraph (iii). Rather, for action to fall within the scope of Article XXI(b), it must objectively be found to meet the requirements in one of the enumerated subparagraphs of that provision.").

21 Ibid para 7.65.

22 Ibid para 7.98.

23 Ibid para 7.100.

24 Ibid paras 7.75-7.76.

25 *Saudi Arabia – Intellectual Property Rights*, para 7.257.

26 Ibid paras 7.258-7.262.

27 Ibid para 7.259.

28 Ibid para 7.263.

18 The analysis of the term "emergency in international relations" in *Russia – Traffic in Transit* clearly excludes political or economic conflicts between states. The panel's approach in this regard seems to situate the term "emergency in international relations" in the context of armed conflict and it is therefore unclear whether it includes a pandemic such as COVID-19.[29] Nevertheless, one could argue that where a pandemic affects the ability of a state to maintain law and public order, then (at least for that state) it could be deemed an "emergency in international relations".[30]

19 Concerning the second factor, i.e. that the relevant actions be "taken in time of" war or other emergency in international relations, the panel in *Russia – Traffic in Transit* took the view that this meant that the relevant actions must be taken during the war or other emergency in international relations.[31] The panel further held that this "chronological occurrence is also an objective fact, amenable to objective determination."[32] In other words, this is also not within the discretion available to states in this regard.

20 In *Saudi Arabia – Intellectual Property Rights*, the panel took the view that the two actions that needed to be examined in this regard (i.e. measures preventing beIN from obtaining Saudi legal counsel to enforce its intellectual property rights through civil enforcement procedures before Saudi courts and tribunals, and the refusal to provide criminal procedures to be applied to beoutQ) were "taken in time of" the emergency in international relations that has persisted since at least 5 June 2017.[33] In relation to COVID-19, measures taken during the pandemic should arguably fall within the scope of this exception.

21 With regard to the third factor, i.e. whether the invoking Member has articulated its relevant "essential security interests" sufficiently to enable an assessment of whether there is any link between those actions and the protection of its essential security interests, the panel in *Russia – Traffic in Transit* began its analysis by drawing a distinction between "security interests" and "essential security interests". According to the panel:

> *"Essential security interests", which is evidently a narrower concept than "security interests", may generally be understood to refer to those interests relating to the quintessential functions of the state, namely, the protection of its territory and its population from external threats, and the maintenance of law and public order internally.*[34]

22 The panel clarified that the articulation of the essential security interests that are directly relevant to the protection of a state from external or internal threats is subjective. According to the panel:

> *The specific interests that are considered directly relevant to the protection of a state from such external or internal threats will depend on the particular situation and perceptions of the state in question, and can be expected to vary with changing circumstances. For these reasons, it is left, in general, to every Member to define what it considers to be its essential security interests.*[35]

23 In other words, the articulation of essential security interests falls within the discretion available to states in this regard. However, the panel stressed that this does not imply that states have the freedom to elevate any concern to that of an essential security interest and it noted that the freedom available to states in this regard is circumscribed by their obligation to interpret and apply Article XXI(b)(iii) in good faith. As the panel notes in this regard:

29 See, *Russia – Traffic in Transit*, para 7.99 (noting that, "The Panel is also mindful that the negotiations on the ITO Charter and the GATT 1947 occurred very shortly after the end of the Second World War. The discussions of "security" issues throughout the negotiating history should therefore be understood in that context.").

30 See also, Henning Grosse Ruse-Khan, 'Access to Covid-19 Treatment and International Intellectual Property Protection – Part II: National Security Exceptions and Test Data Protection' *EJIL:Talk!* (15 April 2020) (contending that: "... the severity of the Covid19 pandemic and its far-reaching consequences across the globe, plus the clarifications under para.5c) of the Doha Declaration that 'public health crises, including (...) epidemics' can represent a 'national emergency', arguably support an application of Article 73(b)(iii) TRIPS ... a WHO declared pandemic should constitute an international emergency, especially if accompanied with general economic, social and political instabilities").

31 *Russia – Traffic in Transit*, para 7.70.

32 Ibid.

33 *Saudi Arabia – Intellectual Property Rights*, para 7.269 (noting that, "The measures at issue are of a continuing nature, as opposed to acts or omissions that occurred or were completed on a particular date, and neither party has suggested that the Panel must assign any dates to them for the purposes of examining the claims and defences before the Panel. In the Panel's view, it suffices to note that beoutQ did not commence operations until August 2017, and hence the actions to be examined under the chapeau were "taken in time of" the "emergency in international relations" that has persisted since at least 5 June 2017.").

34 *Russia – Traffic in Transit*, para 7.130.

35 Ibid para 7.131.

> *...this does not mean that a Member is free to elevate any concern to that of an "essential security interest". Rather, the discretion of a Member to designate particular concerns as "essential security interests" is limited by its obligation to interpret and apply Article XXI(b)(iii) of the GATT 1994 in good faith. The Panel recalls that the obligation of good faith is a general principle of law and a principle of general international law which underlies all treaties, as codified in Article 31(1) ("[a] treaty shall be interpreted in good faith ...") and Article 26 ("[e]very treaty ... must be performed [by the parties] in good faith") of the Vienna Convention.*
>
> *The obligation of good faith requires that Members not use the exceptions in Article XXI as a means to circumvent their obligations under the GATT 1994. A glaring example of this would be where a Member sought to release itself from the structure of "reciprocal and mutually advantageous arrangements" that constitutes the multilateral trading system simply by re-labelling trade interests that it had agreed to protect and promote within the system, as "essential security interests", falling outside the reach of that system.*
>
> *It is therefore incumbent on the invoking Member to articulate the essential security interests said to arise from the emergency in international relations sufficiently enough to demonstrate their veracity.*[36]

24 In *Saudi Arabia – Intellectual Property Rights*, the panel held that Saudi Arabia had expressly articulated its essential security interests in terms of protecting itself from the dangers of terrorism and extremism.[37] The panel further noted that the interests identified by Saudi Arabia clearly relate to the quintessential functions of the state, i.e. "the protection of its territory and its population from external threats, and the maintenance of law and public order internally".[38] The panel equally observed that the standard that is applied to the articulation of essential security interests is whether this articulation is "minimally satisfactory" in the circumstances and it is not necessary to demand greater precision from the invoking state.[39] According to the panel:

> *Although Qatar argued that Saudi Arabia's formulations of its essential security interests are "vague" or "imprecise", the Panel sees no basis in the text of Article 73(b)(iii), or otherwise, for demanding greater precision than that which has been presented by Saudi Arabia. The Panel recalls that, in Russia – Traffic in Transit, the standard applied to the invoking Member was whether its articulation of its essential security interests was "minimally satisfactory" in the circumstances. The requirement that an invoking Member articulate its "essential security interests" sufficiently to enable an assessment of whether the challenged measures are related to those interests is not a particularly onerous one, and is appropriately subject to limited review by a panel. The reason is that this analytical step serves primarily to provide a benchmark against which to examine the "action" under the chapeau of Article 73(b). That is, this analytical step enables an assessment by the Panel of whether either of the challenged measures found to be inconsistent with the TRIPS Agreement is plausibly connected to the protection of those essential security interests.*[40]

25 Indeed, in a footnote, the panel further stated that, "[a]mong other things, it may be noted that an assessment of whether or not certain security interests are "essential" or not is not one that a WTO dispute settlement panel is well positioned to make."[41] Thus, with regard to the pandemic caused by COVID-19, it will be up to any state that wants to invoke Article 73(b)(iii) to articulate in good faith its essential security interests in this regard which may relate to its need to maintain law and order within its territory during the pandemic.

26 In relation to the fourth and final factor, i.e. whether the relevant actions are so remote from, or unrelated to, the "emergency in international relations" as to make it implausible that the invoking Member considers those actions to be necessary for the protection of its essential security interests arising out of the emergency, the panel in *Russia – Traffic in Transit* adopted a standard based on the minimum requirement of plausibility.[42] This requires that the measures in question must not be so remote from, or unrelated to the emergency that it is implausible that the state implemented the measures for the protection of its essential security interests arising out of the emergency.[43]

36 Ibid paras 7.132-7.134.

37 *Saudi Arabia – Intellectual Property Rights*, para 7.280.

38 Ibid.

39 Ibid para 7.281.

40 Ibid citing *Russia – Traffic in Transit*, para 7.137.

41 *Saudi Arabia – Intellectual Property Rights*, para 7.281, footnote 826.

42 *Russia – Traffic in Transit*, para 7.138 (stating that, "The obligation of good faith, referred to in paragraphs 7.132 and 7.133 above, applies not only to the Member's definition of the essential security interests said to arise from the particular emergency in international relations, but also, and most importantly, to their connection with the measures at issue. Thus, as concerns the application of Article XXI(b)(iii), this obligation is crystallized in demanding that the measures at issue meet a minimum requirement of plausibility in relation to the proffered essential security interests, i.e. that they are not implausible as measures protective of these interests.").

43 Ibid para 7.139.

27 In *Saudi Arabia – Intellectual Property Rights*, with regard to the measures preventing beIN from obtaining Saudi legal counsel to enforce its intellectual property rights through civil enforcement procedures, the panel held that these "anti-sympathy" measures meet a minimum requirement of plausibility in relation to the articulated essential security interests.[44] According to the panel in this regard:

> *The measures aimed at denying Qatari nationals access to civil remedies through Saudi courts may be viewed as an aspect of Saudi Arabia's umbrella policy of ending or preventing any form of interaction with Qatari nationals. Given that Saudi Arabia imposed a travel ban on all Qatari nationals from entering the territory of Saudi Arabia and an expulsion order for all Qatari nationals in the territory of Saudi Arabia as part of the comprehensive measures taken on 5 June 2017, it is not implausible that Saudi Arabia might take other measures to prevent Qatari nationals from having access to courts, tribunals and other institutions in Saudi Arabia. Indeed, it is not implausible that, as part of its umbrella policy of ending or preventing any form of interaction with Qatari nationals, as reflected through, inter alia, its 5 June 2017 travel ban intended to "prevent[] Qatari citizens' entry to or transit through the Kingdom of Saudi Arabia", which forms part of Saudi Arabia's "comprehensive measures", Saudi Arabia might take various formal and informal measures to deny Saudi law firms from representing or interacting with Qatari nationals for almost any purpose.*[45]

28 The panel however held that Saudi Arabia's non-application of criminal procedures to beoutQ did not meet the minimum requirement of plausibility. In this regard, the panel observed that:

> *In contrast to the anti-sympathy measures, which might be viewed as an aspect of Saudi Arabia's umbrella policy of ending or preventing any form of interaction with Qatari nationals, the Panel is unable to discern any basis for concluding that the application of criminal procedures or penalties to beoutQ would require any entity in Saudi Arabia to engage in any form of interaction with beIN or any other Qatari national.*[46]

29 Importantly, the panel noted that the non-application of criminal procedures to beoutQ was affecting not only Qatar or Qatari nationals, "but also a range of third-party right holders" from other countries.[47] The panel therefore concluded in this regard that there is "no rational or logical connection between the comprehensive measures aimed at ending interaction with Qatar and Qatari nationals, and the non-application of Saudi criminal procedures and penalties to beoutQ."[48]

30 Concerning the COVID-19 pandemic, a state invoking Article 73(b)(iii) in defence of its decision to suspend the protection and enforcement of intellectual property rights would have to demonstrate that the measures it is implementing are not remote from or unrelated to the emergency. Thus, where a state suspends the protection and enforcement of patent rights to facilitate the local production of vaccines or medicines for treating COVID-19, this could arguably be held to be related to the COVID-19 pandemic and therefore related to the emergency. Therefore, in theory, the invocation of the security exception in response to the COVID-19 pandemic can satisfy all the four factors identified by the panels in both *Russia – Traffic in Transit* and *Saudi Arabia – Intellectual Property Rights*.

D. Article 73(b)(iii) of the TRIPS Agreement and Pandemics: A Realistic Assessment

31 While it may be possible, at least in theory, for states to invoke Article 73(b)(iii) of the TRIPS Agreement in response to pandemics such as COVID-19, it is contended here that this is not a realistic option for a number of states. In this regard, there are at least two reasons why Article 73(b)(iii) of the TRIPS Agreement is not a realistic option for some states. These reasons are further explored below.

32 First, regarding the production of patented medicines or vaccines, only states that possess the capacity to manufacture pharmaceutical products domestically can arguably invoke Article 73(b)(iii) to justify the suspension of the protection and enforcement of patent rights to protect their essential security interests during a pandemic such as COVID-19. Invoking Article 73(b)(iii) may thus be unhelpful to countries that cannot produce the needed vaccines or medicines domestically. Besides the fact that only some developed and developing countries can actually produce vaccines, several developing and least-developed countries do not even possess the capacity to produce medicines.[49]

44 *Saudi Arabia – Intellectual Property Rights*, paras 7.286-7.288.

45 Ibid para 7.286.

46 Ibid para 7.289.

47 Ibid para 7.291.

48 Ibid para 7.292.

49 See, Zoheir Ezziane, 'Essential Drugs Production in Brazil, Russia, India, China and South Africa (BRICS): Opportunities and Challenges' (2014) 3(7) *International Journal of Health Policy and Management* 365; UNCTAD, 'COVID-19 Heightens Need for Pharmaceutical Production in Poor Countries' (27 May 2020) available at < https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2375> In relation to COVID-19,

33 Second, in relation to the importation of patented medicines or vaccines, the security exception in Article 73(b)(iii) cannot be used to circumvent the problems associated with the waiver system contained in Article 31*bis* of the TRIPS Agreement.[50] Article 31*bis* waives the obligation contained in Article 31(f) of the TRIPS Agreement[51] where a state grants a compulsory licence for the production of a pharmaceutical product and its export to an eligible importing country. The usefulness of the waiver mechanism in Article 31*bis,* however, remains doubtful as it contains a number of complex and cumbersome requirements and this has meant that it has been used only once to export anti-retroviral drugs from Canada to Rwanda.[52] In this regard, the key point is that, Article 73(b)(iii) is specifically designed to enable the state invoking the exception to take measures to protect *its* own essential security interests during an emergency and therefore, it cannot be used to address the essential security interests of another state and thereby avoid the strict and cumbersome requirements associated with Article 31*bis* of the TRIPS Agreement. This is not to suggest that Article 73 is subject to either Article 31 or Article 31*bis* but rather to emphasise the limited scope of Article 73(b)(iii) of the TRIPS Agreement. This further complicates the situation for countries that do not possess domestic manufacturing capacity to produce medicines and vaccines.

34 Thus, to provide an illustration, State A cannot invoke the security exception in Article 73(b)(iii) to justify a decision to suspend the protection and enforcement of patent rights in its territory to produce and export patented medicines or vaccines into the territory of State B. As interpreted by the panel in *Russia – Traffic in Transit* and in *Saudi Arabia – Intellectual Property Rights*, the measures implemented by State A pursuant to Article 73(b)(iii) must not be remote from or unrelated to the emergency that it is implausible that State A implemented the measures for the protection of *its* own essential security interests arising out of the emergency. In other words, it is doubtful whether State A can invoke Article 73(b)(iii) to justify the suspension of the protection and enforcement of patent rights in its own territory in order to protect the essential

it is worth noting that China, India, and Russia have been able to produce some vaccines. See, BBC, 'COVID: What do we know about China's Coronavirus Vaccines?' (14 January 2021) available at <https://www.bbc.co.uk/news/world-asia-china-55212787>; Kamala Thiagarajan, 'COVID-19: India is at Centre of Global Vaccine Manufacturing, But Opacity Threatens Public Trust' *The BMJ* (28 January 2021) available at <https://www.bmj.com/content/bmj/372/bmj.n196.full.pdf>; Rachel Schraer, 'Russia's Sputnik V Vaccine has 92% Efficacy in Trial' *BBC News* (2 February 2021) available at https://www.bbc.co.uk/news/health-55900622; Ian Jones and Polly Roy, 'Sputnik V COVID-19 Vaccine Candidate Appears Safe and Effective' (2021) 397 *The Lancet* 642-643.

50 *Cf.* Henning Grosse Ruse-Khan, 'Access to Covid-19 Treatment and International Intellectual Property Protection – Part II: National Security Exceptions and Test Data Protection' *EJIL:Talk!* (15 April 2020) (querying whether "a WTO Member that (for whatever reason) cannot use the Article 31bis system [can] alternatively rely on Article 73 [by] arguing that importing Covid19 treatment to address its own insufficient manufacturing capacity is 'necessary' for protecting its 'essential security interests'").

51 Article 31(f) of the TRIPS Agreement provides that compulsory licences and government use must be authorised "predominantly for the supply of the domestic market".

52 See, UN Secretary General's High-Level Panel on Access to Medicines, 'Report of the United Nations Secretary-General's High Level Panel on Access to Medicines: Promoting Innovation and Access to Health Technologies' (September 2016) 23 (noting that, "There are differing opinions as to why the "Paragraph 6 decision" has only been used once in 13 years. Some note that multilateral health financing has removed the need for resource-constrained countries to use it. Others argue that it is too complex to be used. The only time the mechanism was used, it proved to be complex and cumbersome and serious questions remain as to its effectiveness."). See also, Muhammad Zaheer Abbas and Shamreeza Riaz, 'Compulsory Licensing and Access to Medicines: TRIPS Amendment Allows Export to Least-Developed Countries' (2017) 12(6) *Journal of Intellectual Property Law and Practice* 451, 452 (observing that, "the effectiveness of Article 31bis is likely to be hindered by the tedious and unnecessarily cumbersome authorization processes. Procedural details and formalities may discourage the generic drug manufacturers from exploiting this provision ... As of February 2017, the waiver flexibility has been used only once. This demonstrates that it did not provide a workable solution to the problem highlighted in Paragraph 6 of the Doha Declaration. Making this flexibility a permanent solution, without making changes to address the above-mentioned concerns, is unlikely to have any substantial practical significance."); Carlos Correa, 'Will the Amendment to the TRIPS Agreement Enhance Access to Medicines?' Policy Brief No. 57, South Centre (January 2019) 3 (noting that, "The required notifications and the nature of the information required – plus the obligation to adopt measures to avoid the 'diversion' of the products to other countries – would seem more suitable for the export of weapons or dangerous materials than for products to address public health needs."); Nicholas Vincent, 'TRIP-ing Up: The Failure of TRIPS Article 31*bis*' (2020) 24(1) *Gonzaga Journal of International Law* 1. It should be noted that Bolivia recently notified the WTO that it needs to import COVID-19 vaccines via Article 31*bis* of the TRIPS Agreement. If Bolivia is successful, then this would be the second instance where Article 31*bis* has been used by a WTO member. See, WTO, 'Bolivia Outlines Vaccine Import Needs in use of WTO Flexibilities to tackle Pandemic' (12 May 2021) available at <https://www.wto.org/english/news_e/news21_e/dgno_10may21_e.htm>

security interests of State B by exporting patented medicines or vaccines from State A into State B.

35 Therefore, even if one can successfully argue that the COVID-19 pandemic should be classified as "an emergency in international relations", invoking Article 73(b)(iii) may be unhelpful to a number of developing and least-developed countries that do not possess domestic manufacturing capacity to produce pharmaceutical products. Besides, least-developed countries are currently exempted from providing patent protection for pharmaceutical products until 2033.[53] Thus, it is unnecessary for least-developed countries to invoke Article 73(b)(iii) in order to implement measures to suspend the protection and enforcement of patent protection for pharmaceutical products.

E. Conclusion

36 It is now clear that the invocation of the security exceptions in Article 73 of the TRIPS Agreement is not self-judging and non-justiciable. Importantly, the determination of whether there is an emergency in international relations pursuant to Article 73(b)(iii) of the TRIPS Agreement is an objective fact that is amenable to objective determination. Nevertheless, the articulation of the essential security interests for which protection is being sought falls within the discretion available to the invoking state in this regard although this has to be done in good faith.

37 Crucially, the panels in both *Russia – Traffic in Transit* and *Saudi Arabia – Intellectual Property Rights* arguably struck the right balance between respecting the principle of territoriality and the sovereignty of states in terms of protecting their essential security interests on the one hand and ensuring that states do not abuse and misuse the security exception as a means for avoiding their obligations under international trade law and international intellectual property law on the other hand.[54]

38 Moreover, even if a pandemic such as COVID-19 can be regarded as an emergency in international relations, it is doubtful if suspending the protection and enforcement of patent rights would really be helpful to countries with no capacity to domestically produce pharmaceutical products. Thus, Article 73(b)(iii) of the TRIPS Agreement may not be helpful in addressing the needs of the poorest countries even during a pandemic.[55] Crucially, this shows that, in the absence of domestic manufacturing capacity, most of the flexibilities in the TRIPS Agreement (including the most extreme one, i.e. the national security exception) may not be useful to some countries. Importantly, it also demonstrates the point that facilitating access to medicines in some situations may require measures that (include but also) transcend intellectual property rights.[56]

53 See, WTO Council for TRIPS, 'Extension of the Transition Period under Article 66.1 of the TRIPS Agreement for Least Developed Country Members for Certain Obligations with Respect to Pharmaceutical Products', Decision of the Council for TRIPS of 6 November 2015, IP/C/73 (6 November 2015).

54 The approach of the panels also reflects the intention of the drafters of Article XXI of GATT 1947. See, UN Economic and Social Council, 'Second Session of the Preparatory Committee of the United Nations Conference on Trade and Employment' Verbatim Report, Thirty-Third Meeting of Commission A, E/PC/T/A/PV/33, (24 July 1947) 20-21. See also, GATT, *Analytical Index: Guide to GATT Law and Practice* (1995) 600.

55 See also, UNCTAD-ICTSD, *Resource Book on TRIPS and Development* (CUP, 2005) 809 (noting that, "The rare recourse to security exceptions in the context of international economic relations illustrates the limited importance of such exception for developing countries. The problems these countries will face in the intellectual property area are usually of an economic and a social nature, rather than security-related."); Carlos Correa, 'Lessons from COVID-19: Pharmaceutical Production as a Strategic Goal' SouthViews No. 202 (17 July 2020) 1 available at <https://www.southcentre.int/wp-content/uploads/2020/07/SouthViews-Correa.pdf> (observing that: "The strategic importance of a local pharmaceutical industry has been growingly recognized as a result of the COVID-19 crisis. Developing countries should take advantage of this opportunity to strengthen their pharmaceutical industry, including biological medicines. Industrial policies would need to be reformulated under an integrated approach so as to expand value added & create jobs while addressing public health needs. South-South cooperation may also play an important role in increasing the contribution of developing countries to the global production of pharmaceuticals.").

56 As Correa notes, "Taking advantage of these opportunities to strengthen a pharmaceutical/ biotechnology industry may require the reformulation of industrial policies, so as to promote with an integrated approach this sector as a generator of value added, employment and foreign exchange, as well as an instrument for achieving health autonomy to address public health needs. Such an integrated approach implies the deployment of a series of well articulated instruments ... These instruments include, among others, fiscal measures, access to financing, support to research and development (R&D) including of an experimental nature, a regulatory framework that does not create undue obstacles to registration (especially for biosimilars), an intellectual property regime that uses the flexibilities of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) such as compulsory licensing, and a policy of government procurement that provides predictability to local demand." See, Carlos Correa, 'Lessons from COVID-19: Pharmaceutical Production as a Strategic Goal' SouthViews No. 202 (17 July 2020) 3.

Creativity in crisis: are the creations of artificial intelligence worth protecting?

by **Anthoula Papadopoulou***

Abstract: Up until recently, intellectual creation and inventiveness were purely human activities, and their protection systems, that is, copyright law and patent law, have been built on the basis of motivating and enhancing human creativity. This ancient and self-evident assumption is being challenged due to AI technology today. This article explores the concept of creativity in the field of law from a legal point of view, as well as the impending serious moral and social consequences. In the field of copyright law, intellectual creation is inextricably linked with humans and cannot be replaced by any advanced AI system. This results from the legal definition of work, and in particular from the element of "originality". The Court of Justice of the European Union (CJEU) in its rich case law validates this position. In the field of patent law, ingenuity is also associated with a natural person through the moral right of inventorship. Here, however, the inventor's intellectual endeavor derives from the field of cognition, while fields of human intellect concerning personality in general are not involved in the inventive activity nor are crucial for obtaining a patent. However, it is doubtful whether AI-generated inventions can be protected under patent law for other reasons. Furthermore, decoupling the question of creativity stresses the need for specific legal protection of AI-generated works and inventions. Legislating a sui generis right in order to boost innovation, protect competition and maintain a healthy market for intellectual creations is suggested as the best option.

Keywords: creativity; copyright law; patent law; AI output, legal protection

Recommended citation: Anthoula Papadopoulou, Creativity in crisis: are the creations of artificial intelligence worth protecting?, 12 (2021) JIPITEC 408 para 1

A. Introduction

1 Instead of an introduction, we will mention two typical examples that reveal the problem of our study.

> *1st Example:* E-David observes the painting he created and intervenes autonomously by correcting the intensity of the colours or the errors created by the colour dripping. E-David selects the type of brush that will produce the best result and works in an unexpected and creative way. E-David was born about 10 years ago by a research team at the University of Konstanz in Germany.[1]

> *2nd Example:* A research team from the University of Surrey in England submitted applications to the Intellectual Property Office (UKIPO) requesting a patent on two inventions. The first was a new form of beverage container based on fractal geometry, and the second was a device for attracting increased attention during search and rescue operations. Applications for the above inventions were submitted also to the European Patent Office (EPO). The common feature of all applications was that DABUS, an artificial intelligence system, was named as the inventor.[2]

* Associate Professor of Commercial & Economic Law at the School of Law of Aristotle University of Thessaloniki (AUTH).

1 E-David competed with 25 others robots designed by students across the US <www.theguardian.com/artanddesign/2016/apr/19/robot-art-competition-e-david-cloudpainter-bitpaintr> accessed 22 October 2020.

2 The patent applicant and owner of the AI DABUS, Stephen Thaler (USA), has been working with AI for decades. The name

2 These indicative examples reveal the core problems of this article and call into question fundamental assumptions of copyright and patent law. In particular, artificial intelligence systems challenge the concept of creativity on a legal, moral, as well as philosophical level. Creativity—either defined as intellectual creation or as inventiveness—is exclusively connected with the human intellect. Up until recently, intellectual creation and inventiveness were exclusively human activities, and protection systems have been built on motivating and enhancing human creativity. This self-evident and century old assumption is being challenged because of the features modern artificial intelligence systems have. Features that allow some to argue that there is an analogy between human and artificial intelligence and, therefore, the creative output could be protected as an intellectual work or as a patent.

B. Artificial intelligence and creative output

3 Artificial intelligence, as a general targeting technology, covers many scientific and social fields and is difficult to define. Based on a general approach, it could be seen as an attempt to imitate natural or human intelligence that can learn, perceive, process, compose, decide, and provide an output;[3] which, if mediated by the human intellect, we would characterise as a work or an invention. A sub-concept of artificial intelligence, which is essentially the technological key, is machine learning.[4] Machine learning is achieved through adaptive algorithms that can autonomously recognise patterns, interfaces, and technical rules while making them usable. Through machine learning, an artificial intelligence system develops an output/solution on its own, using the trained artificial neural network. Neural networks are not simple algorithms, which are clear rules for solving a problem; rather, algorithms are used as elements of the neural network, which includes synapses and whose function mimics that of the human brain. Neural networks exhibit an intrinsically probabilistic undefined behaviour. They do not solve problems strictly following the rules that have been set; instead, they formulate the solution to a problem based on variable links and the correction factors themselves. In other words, at their current stage, AI systems can learn and improve on their own through trial and error.

4 The result is that the *how* and the *why* of an artificial intelligence output cannot be easily understood from the outside. Nevertheless, the output of an incomprehensible—not only for legal scholars—cognitive computational process based on an external approach, focusing only on the output, could easily be characterised as creative. It is very likely, for example, that a consumer could not distinguish whether a musical composition is the result of human creation or artificial intelligence[5]. In the field of copyright, this is proven by the so-called Alan Turing test for artworks where a behavioural criterion is adopted.[6] To the extent that the creative

"DABUS" stands for "Device Autonomously Bootstrapping Uniform Sensibility <https://legal-patent.com/patent-law/ai-dabus-autonomous-inventor-but-not-official/> accessed 20 October 2020).

3 See, EU 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*, COM(2018) 237 final, at 1: "Artificial Intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g., voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g., advanced robots, autonomous cars, drones or Internet of Things applications)." See, among others, Shomit Yanisky-Ravid (2017), "Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – The human-like authors are already here- A new model", Mich. St. L. Rev 659, 672; Daniel Schönberger (2018), "Deep Copyright: up – and downstream questions related to artificial intelligence (AI) and machine learning (ML)", in: *Droit d'auteur 4.0/Copyright 4.0*, De Werra, Jacques (ed.), Geneva/Zurich: Schulthess Editions Romandes, pp. 145-173, available at SSRN: <https://ssrn.com/abstract=3098315>, accessed 14 March 2020; Lilian Mitrou (2019), "Data Protection, Artificial Intelligence and Cognitive Services - Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?", available at SSRN: <https://ssrn.com/abstract=3386914>, accessed 15 April 2020; Steven Finley (2018), Artificial Intelligence and Machine Learning for Business A No- Nonsense Guide to Data Driven Technologies, Relativistic, 3rd edition, 2018, 6, 31. Cf. EU Commission: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Building Trust in Human-Centric Artificial Intelligence, Brussels 8.4.2019 COM(2019) 168 final.

4 Ana Ramalho (2018), "Patentability of AI-Generated Inventions: Is a Reform of the Patent System Needed?" < https://ssrn.com/abstract=3168703>, accessed 10 March 2021; Theodoros Chiou (2019), "Copyright lessons on Machine Learning: what impact on algorithmic art?" 10(3) *JIPITEC* 398 para 2 <www.jipitec.eu/issues/jipitec-10-3-2019/5025> accessed 29 May 2020.

5 Shomit Yanisky-Ravid, (n 3) 703.

6 This test asks people which work of art is man-made and which is computer-generated. Once an AI-generated work of art cannot be perceived as such and people cannot tell whether

output can surprise as pleasantly and cause the same enjoyment as if it had been generated by a human being, it does not matter whether the AI is really creative, but whether it appears to be so judging by the outcome.

5 The perception of the output as a creative one by society has its own value for financial scrutiny and integration of these outputs into the market. Nevertheless, the *external approach* to the creative output *does not prejudge the internal approach to creativity.*

C. Artificial intelligence and human creativity

6 The relationship between artificial intelligence and human creativity poses a strong challenge to intellectual property law with strong moral and philosophical attributes.

I. Creativity and intellectual creation in the field of copyright: an exclusive privilege of humans?

7 It is a common assumption, both in the human-centric system of continental law and in the Anglo-Saxon copyright system—which is not obviously human-centric—that creativity goes hand in hand with the spirituality of man.[7] The author of a work can only be a human being as a work can only derive from the human mind. This assumption moreover is the basis of the whole system of protection of moral rights.

8 As an *intellectual creation*, the work can only derive from the human mind. This self-evident assumption on human-centric protection systems[8] has been contested and confirmed by the United States district court in the Monkey Selfie case [9] The case was not about an AI system but instead about the creativity of animals. The question arose as to whether the monkey who used the photographer's camera could be assigned copyright on the photographs. The court ruled that under applicable law copyright cannot be assigned to the monkey and a monkey could not be an author.[10]

9 Further, the *originality* of the work is also linked to human creativity. The legal concept of originality, although it is a very important prerequisite for the definition of work, is not specified by the law. The conceptual framework comes from theory but is mainly provided by jurisprudence.[11] Without further expanding on this topic, let us just note that the dynamic concept of originality moves between a human-centric approach, which puts the individuality of the author at the core, and a work-centric approach, which focuses on the individuality of the work. Today, the position of the Court of Justice of the European Union is of prime importance. By defining the concept of originality as an autonomous

is man-made, it passes the test. *See* Mark Coeckelbergh (2017), "Can Machine Create Art?" 30(3) Philosophy Technology 285, 288 <www.researchgate.net/publication/308535691_Can_Machines_Create_Art> accessed 16 January 2020.

7 In Greek law, human creativity is inherent in the concept of work as a legal term; in particular, a work shall be an *intellectual creation* and have *originality* (Art. 2 Law 2121/1993). For US law, *see* Section 17 U.S.C §102 (1990). *See also*, *U.S Copyright Compendium (third)* §306: 'The U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being' <www.copyright.gov/comp3/>. accessed 3 October 2020; for English law, CDPA 1988, s 9 (1), Lionel Bently/Brad Sherman, *Intellectual Property Law* (4th ed Oxford University Press 2014) 124; *see also* Ralph Clifford, 'Creativity Revisited' (2018) 59 IDEA - The Law Review of the Franklin Pierce Center for Intellectual Property 25, 26*ff*; Pratap Devarapalli, 'Machine learning to machine owning: redefining the copyright ownership from perspective of Australian, US and EU law' (2018) 40 *EIPR* 722; Shomit Yanisky-Ravid, (n 3) 718; Julia Dickenson, 'Creative machines: ownership of copyright in content created by artificial intelligence applications' (2017) 38 EIPR 457.

8 For French law, *see* André Lucas/Henri-Jacques Lucas, *Traité de la Propriété Littéraire et Artistique* (3rd edn, Lexis-Nexis /Litec 2006), para 143.

9 CA *Naruto v. Slater*, No 16-15469 (9th Cir. 2018) <https://law.justia.com/cases/federal/appellate-courts/ca9/16-15469/16-15469-2018-04-23.html>.

10 CA *Naruto v. Slater*, (n 9); *See also, U.S. Copyright Compendium of U.S* (third) § 306 'The copyright law only protects the fruits of intellectual labor that are founded in the creative powers of the mind. Because copyright law is limited to original intellectual conceptions of the author, the Office will refuse to register a claim if it determines that a human being did not create the work'.

11 Case C-145/10 *Eva-Maria Painer* [2011] EU:C:2011:798, paras 89-93; Case C-5/08 *Infopaq* [2009] EU:C:2009:465, paras 37-45; Cases C-403/08 *Football Association Premier League Ltd and Others v QC Leisure and Others* and C- 429/08 *Karen Murphy v Media Protection Services Ltd* [2011] EU:C:2011:631, paras 97-98; Case C-393/09 *Bezpečnostní softwarová asociace (BSA)- Svaz softwarové ochrany v. Ministerstvo kultury* [2010] EU:C:2010:816, paras 46-49; Case C-161/17 *Land Nordrhein-Westfalen κατά Dirk Renckhoff* [2018] EU:C:2018:634, para 14; Case C- 30/14 *Ryanair Ltd v PR Aviation BV* [2015] EU:C:2015:10, para 34. *See also* André Lucas/Henri-Jacques Lucas, (n 8) para 80, Lionel Bently/Brad Sherman, (n 7) 93 -108.

concept of EU law, the CLJEU has taken a human-centric approach through a series of decisions. In particular, the CJEU identifies originality as the result of the *author's personal intellectual creation*. Basically, the CJEU with its established case law extended the above concept of originality, which had already been legally recognised for three categories of works[12], to all works indiscriminately.[13] Further specifying the concept, it clarified that the intellectual creation of the author occurs when the author is able to make free and creative choices that express their personality.[14]

10 The personal touch with which the author can stamp their work is the result of a complex intellectual process; a process that incorporates mostly the deconstruction of all the elements they receive, the conscious processing of ideas, images, sounds, emotions and senses and finally the composition of the above with a conscious choice, or with a conscious randomness.

11 Questions about the impact of technology on human creativity were raised three to four decades ago because of the so-called computer-generated works. First, the UK incorporated in its copyright law (Copyright, Designs and Patents Act 1988/CDPA) a provision for computer-generated works, i.e., works generated by computer in circumstances such that there is no human author of the work. As provided for by the UK law, an author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken.[15] Classifying a computer programme into the category of the *author's tool* became more widely accepted.[16] Simply put, a music software used to create new content represents an asset for the composer as does a camera for a photographer or a brush for a painter. It was a compromise option for integrating computer-generated works into the current legal system ascribing authorship to the individual who coordinates, controls, and possibly intervenes with the result generated by a computer programme.[17]

12 This approach could in principle be applied to works generated with the assistance of artificial intelligence insofar as there is involvement of a natural person (AI-assisted works). The crucial question, however, is the degree of the person's involvement and whether that is enough to ascribe authorship to them. It is claimed that it is not enough if the person simply causes or initiates the process without having control over the output.[18]

13 The essential dilemma then arises with works produced entirely by artificial intelligence (AI-generated works). In the near future, an advanced super-intelligence (ASI) system will have the ability to generate output autonomously, independent of any human involvement. At a legal level, artificial super-intelligence cannot be granted the same status as human creativity and the output it achieves

12 Council Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs, OJ L 111/16, article 1 par. 3, where reference is made to 'the author's own intellectual creation'; Council Directive 96/9/EC of 11 March 1996 on the legal protection of databases, OJ L 77/20, article 3, where reference is made to, 'by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation'; Council Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights, article 6 of Directive 2006/116, where reference is made to 'the author's own intellectual creation'.

13 See above (n 11).

14 *See* extensively on the concept of originality and creativity through the jurisprudence of the CJEU Thomas Margoni, 'The harmonisation of EU copyright law: The originality standard' in Perry (ed), *Global Governance of Intellectual Property in the 21st Century* (Springer International Publishing 2016), 85-105; Henrik Bengtsson, 'EU Harmonisation of the copyright originality criterion' in Rosén (ed), *European Intellectual Property Law* (Elgar Research Collection 2016), 486-493; Jonathan Griffiths, 'The role of the Court of Justice in the development of European Union Copyright Law' in Stamatoudi/Torremans (eds), *EU Copyright Law- A Commentary* (Edward Elgar 2014), 1102-1104; Mira Sundara Rajan, 'The attribution right: authorship and beyond', in Brison/Dusollier/Janssens/Vanhees (eds), *Moral Rights in the 21st Century*, ALAI Congress Brussels 17-20 September 2014 (Group Larcier 2015), 246-248; Lionel Bently/Brad Sherman, (n 7) 100-102; Irini Stamadoudi, 'The originality in the European Union's copyright law' (2016) 13 *DIMEE*, 49 (in Greek); Stef van Gompel, 'Creativity, autonomy and personal touch: A critical appraisal of the CJEU's originality test for copyright' in M. van Eechoud (ed), *The work of authorship* (Amsterdam University Press 2014).

15 CDPA 1988, s 9(3): 'In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken'.

16 Ana Ramalho, 'Will robots rule the (artistic) world? A proposed model for the legal status of creations by artificial intelligence systems' (2017) Journal of Internet Law 2 <doi:10.2139/ssrn.2987757> , accessed 8 April 2020, Mark Perry and Thomas Margoni, 'From music tracks to Google Maps: Who owns computer-generated works?' (2010) 26 CLSR 621.

17 The question of originality, however, which goes hand in hand with that of human creativity, had not been convincingly answered, Toby Bond/Sarah Blair, 'Artificial Intelligence &copyright: Section 9(3) or authorship without an author' (2019) 14 JIPLP 423.

18 Anne Lauber-Rönsberg/ Sven Hetmank, 'The concept of authorship and inventorship under pressure: Does artificial intelligence shift paradigms?' (2019) 14 JIPLP 570.

cannot be equated with artworks worthy of copyright.[19] There is no doubt that artificial intelligence can successfully mimic or prove to be superior to a part of the human brain: specifically, the part that deals with the analysis and synthesis of knowledge, rules and principles, complex calculations, as well as drawing conclusions or results. However, other brain functions that are less understood have not yet become part of machine learning, such as inspiration, imagination, consciousness, expression of emotions like love, fear, etc.[20] The free and creative choices that leave the author's personal touch, as established by the CJEU, cannot be equated with random outputs by neural networks despite the superiority of their cognitive ability in relation to humans. Even if we accept that a machine can create an artwork, this does not express anything; it does not have the interiority that originates in a human artwork. Therefore, based on an internal approach, which has moral and philosophical foundations but is also fully reflected in the legal meaning of the work, artificial intelligence's outputs cannot be granted the same status as the works of authorship created by human beings. Further, such a change in their status in the current copyright system would completely undermine the whole foundation of moral rights.

14 The consequences of granting AI-generated outputs the status of copyright-protected works on a moral and social level are deeper and more substantial. Imagine a world where a robot of advanced intelligence recites its own poems after having devoured all of Elytis's poems[21] as data or posts news on the internet by selecting headlines based on the criteria of an algorithm.[22] At the same time, imagine a society that has easy and cheap access to mass-produced culture.[23] In such an inflationary context where works of human creation cannot be distinguished from AI-generated works, it is very likely—based on supply and demand—that the human creator's remuneration may be minimal and thus humans may lack the economic incentive to create. In this very same context, the influence of a creator's ideas, views, aesthetics and feelings on the public will fade. Undermining the communication between the creator and the public also minimises the moral motivation of creation. Taking into account that literature, art, science and culture in general have the power to shape consciences and societies, it is not difficult to imagine that if the multitude of AI outputs outlive the creations of the human intellect, there will be societies that will bear the imprint of the outputs of neural networks and perhaps of the users who control those networks.

15 It is clear that AI-generated outputs should not be granted the same status as copyright works. However, as we will see, AI-generated outputs deserve some protection by establishing sui generis right.

II. Creativity and ingenuity in the field of patent law: an exclusive privilege for humans?

16 In the field of technical creations, creativity takes the specific form of ingenuity and inventiveness.[24] Similar concerns arise in the case of an AI system's inventive activity that produces an output worthy of a patent.[25] As in the field of copyright, the dilemma concerns the AI-generated inventions and not the

19 For proponents that artificial intelligence can be equated with the concept of creativity, *see* Shomit Yanisky-Ravid, (n 3) 78 *ff.*, who mentions ten features that an AI system may have with the current level of development which justify the element of "creativity"; among them, she mentions autonomous and independent operation, unpredictable and new outputs, the ability to learn and self-improve/self-develop, the rational system of receiving and processing information, and selecting the best result in relation to its orientation (e.g. creating drafts, writing stories, composing music, etc.).

20 On the philosophical critique of whether machines can create art, *see* David Gunkel, 'Special Section: Rethinking Art and Aesthetics in the Age of Creative Machines' (2017) 30 Philosophy &Technology 263.

21 Odysseus Elytis (1911-1996) was one of the greatest Greek poets of modern Greece. He was awarded the Nobel Prize in Literature in 1979. He was a major exponent of romantic modernism in Greece.

22 Extensively on the issue of automated journalism based on algorithms, Seth Lewis, et al. 'Libel by Algorithm? Automated Journalism and the Threat of Legal Liability' (2019) 96 Journalism and Mass Communication Quarterly, 60.

23 Using the words of Konstantinos Daskalakis, Professor at MIT: 'No, a computer cannot yet write Shakespeare, however, a modern algorithm can learn superb English and imitate the style of the British author' *H Kathimerini* (Athens 22.1.2020) <www.kathimerini.gr/1057253/article/epikairothta/ellada/k_daskalakis-> accessed 5 February 2020

24 The law of technical inventions encompasses, in addition to patents, utility models, plant creation certificates, etc.

25 Oliver Baldus, 'A practical guide on how to patent artificial intelligence (AI) inventions and computer programs within the German and European Patent System: much ado about little' (2019) 41 EIPR 750; Peter Blok 'The inventor's new tool: artificial intelligence – how does it fit in the European Patent System?' (2017) 39 EIPR 69; Erica Fraser, 'Computers as Inventors - Legal and Policy Implications of Artificial Intelligence on Patent Law' (2016) 13(3) SCRIPTed 305.

AI-assisted inventions. Can an artificial intelligence system be an inventor? In the aforementioned example of works created by an AI system, the patent applications were rejected by both the Intellectual Property Office (UKIPO)[26] and the European Patent Office (EPO)[27] because DABUS was named as the inventor. The argument was the same: under English law and the European Patent Convention (EPC), the term *inventor* refers only to a natural person.[28] Subsequently, UK's Intellectual Property Office (UKIPO) updated its Formalities Manual to state that 'an AI inventor is not acceptable as this does not identify "a person" which is required by law'.

17 Patenting dilemmas are less intense because in the technological field of inventions, the inventor's intellectual processes to achieve an innovation are derived from the field of cognition: i.e., the ability to synthesise and analyse data, process and solve problems. In contrast, imagination, emotions or choices that suggest the inventor´s personality are neither required for an inventive activity nor are crucial for obtaining a patent. In other words, the invention is evaluated by objective criteria which do not consider who and how the innovation occured, nor if it expresses the personality of the inventor. In this sense alone, *the ability to invent* could be replaced by the cognitive ability of an artificial intelligence system.

18 However, there is also the parameter of the moral right of inventorship. Under generally applicable law, both nationally and internationally, it is necessary that the natural person who made the invention be named in the application, to ascribe inventorship. If attribution of inventorship is treated as a formal requirement, it can be surpassed by the fictional naming of a natural person, e.g., the system user. Besides, based on the principle of the *first declarant* (art. 63 par. 3 Munich Convention), the one who submits the application is presumed to be the inventor without any further examination.[29] This choice, however, would be morally reprehensible because the strict application of this legal principle which requires a person as an inventor will simply lead companies to formally or fictitiously provide a person's name in order to obtain the patent. This would be unfair: not, of course, for the artificial intelligence system that has no acknowledgement interest but because it would allow people to get credit for inventions they have not made and would devalue human creativity. It would put on an equal footing the person who just poses a question to a robot—and the robot solves the problem—with the person who is really striving to devise an invention.[30]

19 The problem, therefore, is mainly moral and social. The gradual replacement of the inventor by artificial intelligence could lead to the decay of human inventiveness and ingenuity with everything that this may imply in the evolution of the human spirit.

D. Is legal protection for an output generated by an artificial intelligence system justified?

20 This issue needs to be explored primarily in economic terms and in terms of protecting competition, detached from the above thoughts on human creativity. The impact of AI technology on competition law, although of particular importance, has not yet been included in the World Intellectual Property Organization (WIPO) questionnaire.[31]

I. Creative outputs in the field of art, literature and science

21 In the field of intellectual creation and copyright, the question first arises as to whether AI generated creative outputs deserve legal protection. The answer is positive. Refusal to protect could encourage

26 UKIPO patent decision BL O/741/19 of 4 December 2019 <www.ipo.gov.uk/p-challenge-decision-results/p-challenge-decision-results-bl?BL_Number=O/741/19> accessed 26 August 2020.

27 EPO publishes grounds for its decision to refuse two patent applications naming a machine as an inventor <www.epo.org/news-issues/news/2020/20200128.html> accessed 20 September 2020.

28 There was a further problem as to DABUS' ability to own legal rights. In these patent applications, DABUS was designated as the inventor, while Dr. Stephen Thaler (the DABUS developer) was named as the applicant. The Office challenged how the applicant could derive any rights to the invention from the inventor when "an artificial intelligence machine [the inventor] cannot own property rights". Without being entitled to own such legal rights, artificial intelligence machines cannot be considered to transfer any legal rights to the owner or applicant of a patent filing, even if it is acknowledged that the AI created the invention.

29 Moreover, as reported, the European Patent Office does not verify the name of the natural person who is declared as the inventor, Anne Lauber-Rönsberg/ Sven Hetmank, (n 15) 572.

30 Ryan Abbot, 'The Artificial Inventor Project' (2019) WIPO Magazine 1, 3 <www.wipo.int/wipo_magazine/en/2019/06/article_0002.html>.

31 WIPO, 'WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence' (2020) WIPO/IP/AI/2/GE/20/1 Rev. 3 <www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf> accessed 29 May 2020.

parasitic competition which is not justified. Imagine a market where intellectual property and artificial intelligence coexist and only human creations are protected. Based on the above hypothesis, a scenario could be that artificial intelligence outputs imitate with absolute fidelity the style of well-known artists without, however, copying works, which results in consumer confusion and encourages parasitic competition. Once a work or an AI-generated output is exploited, it is on a market, which would thus justify applying competition law. In any case, the perception of the AI output as a creative one by the average consumer combined with the expectedly low price compared to human creations of art could possibly create conditions of unfair competition and consumer deception. For the above reasons, there is a need for a *specific legal protection* of creations generated by artificial intelligence. Recognition of specific legal protection will contribute to the proper functioning of competition rules while preserving the value of human creativity.

22 The question raised then concerns the type of protection provided. Can the protection of AI-generated creative outputs be integrated into the copyright or related rights protection system? Based on a relevant questionnaire set by WIPO[32] and other international forum, such as International Association for the Protection of Intellectual Property (AIPPI) to national delegations, opinions vary.[33] Although no one denies the need for protection, the majority accept the aforementioned possibility of copyright protection only under the condition of the involvement of the human factor (AI-assisted works), referring to the tool's theory.[34] On the contrary, if the creative output is autonomous, unpredictable and there is no human intervention, protection is not admitted under copyright law.[35] Regarding AI-generated works, the absence of any human intervention completely excludes the CJEU requirement for the author's personality expression through voluntary choices. The establishment of a new sui generis economic right could ensure the necessary specific legal protection for these works, as well as reinforce investment without pressuring and deconstructing concepts such as originality and creativity.[36] Moreover, the scenario of granting AI outputs the same status as works of authorship raises the risk that we will be led to a normality of creating works by algorithms, resulting in confusion of the "originality" of human-made works with the endless diversity of AI outputs. In theory, all possible uses of a work (reproduction, distribution, communication to the public, etc.) are also ways of using and exploiting AI-generated outputs. Therefore, a number of relevant property rights are possible, but for a shorter period of protection. It is also important to point out the non-obvious difference in the consumers' perception of the origin of a work.

II. Creative outputs in the field of inventions

23 The need to protect AI-generated inventions is rooted in the European Union's policy of strengthening and promoting technology and innovation. Europe must compete with the United States and China in the development of innovative technologies. In February 2020, the European Commission issued the *White Paper on Artificial Intelligence: (A European approach to excellence and trust)*[37], while in September 2020 the Committee of Legal Affairs issued the *Report on Intellectual Property Rights for the development of artificial intelligence technologies*.[38] Clearly, the EU's strategy for AI is much broader than the perspective on the issues we are addressing. It reaches many areas of our lives which it aspires to change, such as health care (e.g., allowing for more diagnostic accuracy that facilitates better disease prevention), increasing the efficiency of agriculture, mitigating climate change, enhancing the efficiency of

32 WIPO, (n 28) 7-8.

33 Jonathan Osha et al., '2019-Study Question- Copyright/Data Copyright in artificially generated works' (2019) Summary Report AIPPI <www.aippi.dk/wp-content/uploads/2019/05/Study-Guidelines_Copyright_Copyright-in-artificially-generated-works_22January2019.pdf> accessed 20 December 2019.

34 AIPPI, 'Resolution 2019 - Study Question, Copyright in Artificially generated works' (2019) <www.aippicanada.org/wp-content/uploads/2019/12/Resolution_Copyright_in_artificially_generated_works_English.pdf> accessed 11 May 2020.

35 In the context of US law, the view has been expressed that the element of creativity could be recognised to artificially generated works and their protection should remain in the field of copyright through the model of works created by an employee or contractor as an object of work or project, Shomit Yanisky-Ravid, (n 3) 707.

36 Anne Lauber-Rönsberg/ Sven Hetmank, (n 15) 576-577, where the options for legal treatment of artificial intelligence creative outputs are presented extensively.

37 European Commission, *White Paper on Artificial Intelligence: A European approach to excellence and trust* COM (2020) 65 final <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 29 June 2020.

38 European Parliament, Committee on Legal Affairs, *Report on Intellectual Property Rights for the Development of Artificial Intelligence Technologies/Opinion of the Committee on Culture and Education 2020/2015* (INI) <www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html> accessed 11 October 2020.

production systems, etc. Self-evidently, the political interest is great, as is the financial support that will be allocated.[39]

24 The correct legal framework for protecting AI-generated inventions is still in question. Protection within the current legislative system of patent law is problematic, although as stated before, ingenuity is evaluated objectively and, therefore, the involvement of the human inventor may not be of interest in a future legislation.[40] In the context of the ongoing WIPO conference, the possibility of having patent or some other certification without having a paternity attribution to a person is under consideration.[41]

25 However, other crucial issues arise in connection with obtaining a patent. It is well known that a key element in a patent application is the description of the invention in a way that the average expert in the art can understand and apply it.[42] As mentioned above, the *how* and *why* in the operation of an artificial intelligence system is opaque. An artificial intelligence system incorporates special features of many technologies and, by working in combination, they become complex, unpredictable and behaviourally autonomous. As a result, the operation of artificial intelligence leading to the output or invention becomes unclear (black box effect).[43] Given this, it is difficult to describe the invention in the patent application in such a way that it is possible for the average expert in the art to put the invention into practice.[44] Might it be enough to disclose the original algorithm? The clear disclosure of the steps taken for the final result is an essential precondition for obtaining a patent; it restablishes the social legitimacy of patents to the extent that the disclosure contributes to the sharing of knowledge and technological development.[45]

26 Concern is also raised by the required element of *inventive step,* meaning that the invention must not not be obvious *to* for an average expert given the current state of the art.[46] This condition is subject to reconsideration, if we place it within the field of artificial intelligence. Who becomes the average expert? What is obvious? Is it evaluated based on cognitive power of the artificial intelligence rather than humans? Or could the person, training artificial intelligence with data, be taken as a reference measure? Moreover, the *level of technique* is reversed at much shorter intervals because the human speeds of evolution will be overturned. Unprecedented velocity will be imposed, and the issue of short-term devaluation of an invention will arise as the cycles of innovation become shorter. In much less than 20 years, the increasingly well-trained artificial intelligence will make the next technological leap in every field. This leads to an inflation of technological advances which is doubtful whether it also justifies patent inflation.[47]

27 Based on the above, AI-generated output protection under the applicable patent law is difficult and problematic. On the contrary, the need to protect AI-generated inventions is achieved by the recognition of a specific *sui generis right.* A sui generis property right, of shorter duration, adapted to the characteristics of artificial intelligence would be the best option.[48] The suggested sui generis right should provide the power

39 *White Paper* (n 37), 25: 'AI is a strategic technology that offers many benefits for citizens, companies and society as a whole, provided it is human-centric, ethical, sustainable and respects fundamental rights and values'.

40 According to Ana Ramalho, (n 4) 14: '...there is nothing in the EPC definition of invention that would preclude AI-generated innovations from being considered as "inventions" for purposes of patentability, especially since exceptions to patentability are to be interpreted narrowly'. Regarding whether an AI invention can be patent, the U.S Court in the case *New Idea Farm Equipment Corp. v. Sperry Corp.* 916 F.2d 1561 (Fed. Cir. 1990,) 16 U.S.P.Q.2d 1424 stated that only people conceive ideas and not machines.

41 WIPO (n 28) 4-5.

42 The obligation to describe the invention on which the claims are based is provided for in article 7 par. 4 of Greek Law 1733/87, Michalis-Theodoros Marinos, *Patent Law*, (Law & Economy P.N. Sakkoulas 2013) paras 5.28-5.30 (in Greek).

43 Corinne Cath, 'Governing artificial intelligence: ethical. Legal and technical opportunities and challenges' (2018) Philosophical Transactions of the Royal Society <https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0080> accessed 5 May 2020.

44 Lionel Bently/Brad Sherman, (n 7) 574-576; Ebrahim Tabrez, 'Artificial Intelligence Inventions & Patent Disclosure' (October 31, 2020), Penn State Law Review, 125 (1), 2020 <https://ssrn.com/abstract=3722720> accessed 5 March 2021.

45 This obligation is provided for in Article 83 of the Munich International Convention, in Article 29 par. 1 of the TRIPS Agreement, in Article 5 of the PCT (Patent Cooperation Treaty) and is included in all national legislation.

46 *See,* for example, Art. 5 par. 4 L. 1733/1987 (Greek Patent Law). For Greek law, *see* Michalis -Theodoros Marinos, (n 38) paras 3.65 -3.66. See also Ralph Clifford, (n 7) 36

47 Anne Lauber-Rönsberg/ Sven Hetmank, (n 15) 578.

48 Ana Ramalho, (n 4) 22 -25 accepts protection under applicable law, as far as in all current constructions inventions a human is still, to a greater or lesser extent, involved. She proposes to develop common guidelines between Patent Offices taking account the characteristics of AI-generated output.

and right (e.g., exclusive use, placing on the market, economic exploitation licenses) as well as provide protection against illegal appropriation. Moreover, the non-recognition of adequate legal protection in an AI-generated invention carries the risk of extending their retention as trade secrets resulting in the non-disclosure of information to the public at the expense of knowledge sharing and technological progress.[49] The possibility to maintain a certain artificial intelligence technology as confidential (trade secret) is obviously much greater if it cannot be protected by an exclusive property right.[50] And this is a possibility that does not help the goal of the developing innovation and the dissemination of knowledge.

E. Allocation of rights on creative outputs and liability: a challenging puzzle for legal scholars

28 The allocation of rights on a creative AI-generated output is a matter of particular significance both for determining the person who will enjoy the economic benefits and because this person will be associated with the liability that may arise from illegal acts. The allocation of rights is a challenging puzzle for the legislator.

29 Three categories of persons make significant contributions to the process of operating an artificial intelligence system.[51] First, the *owner* of the artificial intelligence system who is the natural or legal person who has borne the burden of the financial investment. Second, the *developer* or the natural person who creates the artificial intelligence system Usually, there is more than one developer working on a team to create a series of software that are integrated into a neural network with the ability to work in combination. Third, the *user* of the system, that is, the person who enters the data/inputs and trains the system for a reliable output. It is possible that the *user* is the same person as the developer or the owner, but this is not necessary. The user is the last person to intervene in the chain of final and autonomous operation of an AI system.

30 The above three categories of persons involved are common whether the output is a work or an invention. Which category of persons can claim authorship or inventorship? The owner of the system is the person who has invested in the creation of the system. Although this person does not have any involvement in the operation of the system, they must be financially secure in order to recuperate the costs of their investment and to be motivated to invest further in the field of artificial intelligence. Proponents of computational creativity have argued that an artificial intelligence system can be understood as a creator with analogous (or legal) acknowledgement of legal personality in this system.[52] In our view, a sui generis right analogous to that of a database maker could possibly be established in order to secure the investment and avoid a 'market failure' in the absence of legal exclusivity.[53]

31 The developer or—more commonly—the team of developers who work together to develop the software acquire the copyright as authors or co-authors of the computer programme. In particular, the developers are co-authors and initial co-holders of the copyright on the programmes they develop. The property rights assigned to these persons by law or on contractual terms if they work as contractors are granted to the company. They are usually employees of tech companies. Persons, as authors, retain moral rights on software. Developers, however, do not seem to have a reason to be considered authors of the creative output of the system they developed, as the camera manufacturer has no copyright to the photos taken by the photographer.[54] Other ideas have been also suggested, such as to name as co-inventors those who developed the artificial intelligence system along with those who entered the data of the technological problem, that is, the user of the system.[55]

49 WIPO (n 28) 5.

50 Ana Ramalho, (n 4) 23; Ebrahim Tabrez, (n 43) 207.

51 As an option, it is also advocated to classify these creative outputs as free works belonging to public space; *see* Konstantinos Christodoulou, 'Legal Issues from artificial Intelligence' [2019] Chronika idiotikou Dikaiou 330 (in Greek); Anne Lauber-Rönsberg/ Sven Hetmank, (n 15) 577.

52 Anne Lauber-Rönsberg/ Sven Hetmank, (n 15) 577; Konstantinos Christodoulou (n 45) 331, who point out the risks of opacity in relation to natural persons who will have control over the legal entity.

53 Article 45 A par. 1 of Greek Law 2121/1993 which is a transposition of art. 7 par. 1 of Directive 96/9/EC.

54 It has been argued that the creative output can be considered a derivative work of the creator of the program. This view is not consistent with mine to the extent that it does not answer the question of originality/creativity that should also characterise a derivative work. Also, as rightly observed by Konstantinos Christodoulou (n 45) 330 'The technical output achieved with the use of specific software is not a derivative work, even if this output would be a work e.g., a piece of music or a painting generated by creative software'.

55 Anne Lauber-Rönsberg/Sven Hetmank, (n 15) 572.

32 The role of the user of the system seems to be crucial and is the closest to the creative output. It is the person who introduces training data—which may be previous works—and sets the goal. It is the person who controls the result more, in the case of an AI-assisted work, and less (up to a minimum) in the case of an AI-generated output. In the first case we may accept that there is a copyrighted work and the initial copyright holder is the user considering that the artificial intelligence system assumes the role of a *tool*. The choice of training data may be paralleled with the requirement of creative choices set by the CJEU. In the second case, the *user* is the person who theoretically deserves to acquire the sui generis right as the person who entered into the system all the data on the basis of which the system came to the AI-generated creation or work. In fact, what usually happens is that the user is an employee of the company that owns the artificial intelligence system. Therefore, based on the proportional application of the national rules governing works made by hired employment, the sui generis right will be acquired upon assignment by the legal entity that owns the AI system.[56] The same person, the employer's company, should be liable for possible infringements of previous works used as data for system training. Also, it has been expressed that all AI-generated creations potentially fall under the public domain with possibilities to make national rules 'outside' the copyright sphere, e.g., competition law applicable.[57]

33 Regarding an AI-generated invention, the user's role is just as critical. The selection and the quality of data used to train the AI system is of the utmost importance for achieving a good result. The more data, the better the training of the system and the more the chances of achieving a reliable inventive output. Thus, the user's role is the one entailing the necessary ingenuity for the output and, therefore, the user is the person who can theoretically be deemed to be the rightholder of the sui generis right. Often, the user is not a self-employed natural person but an employee of a company and it is very likely that the company owns the AI system. Therefore, the following situation may arise regarding the allocation of a sui generis right: either there will be a proportional application of the national provisions for employees' inventions[58] or the company will acquire the rights following a contractual assignment. An important issue may arise in relation to the allocation of liability for defective new products or methods derived from artificial intelligence. Who is responsible for the safety of new products or methods or, even if there is no question of safety, who is responsible if these products infringe other rights such as, e.g., personal data.[59]

34 It is clear that some legislative initiative will be taken at the EU level so that, in the future, there is a harmonised legal protection of creative outputs in the member states.

F. Concluding thoughts

35 Artificial intelligence has vigorously permeated all areas of social and economic life.[60] An issue such as the impact of artificial intelligence on human creativity cannot be closed nor can conclusions be drawn. Questions and dilemmas remain open.[61] The

56 Under Anglo-Saxon law, it has been argued that the provisions on employees' work could apply proportionally (work for hire), Shomit Yanisky-Ravid, (n 3).

57 Ole-Andreas Rognstad, 'Artificial Intelligence and Copyright-Ownership', in *"EU copyright, quo vadis? From the EU copyright package to the challenges of Artificial Intelligence." ECS International Conference* Brussels, 25 May 2018, as reported by B.G Otero/J.P. Quintais, 'Before the Singularity: Copyright and the Challenges of Artificial Intelligence' <http://copyrightblog.kluweriplaw.com/2018/09/25/singularity-copyright-challenges-artificial-intelligence/> accessed 11 March 2021.

58 Regarding the significant differences in the ways in which the EU member states handle the legal issue of employees' inventions, *see* Marie-Christine Janssens, 'EU Perspectives on Employees' Inventions' (2013), in: M. Pittard, A. Monotti and J. Duns (eds), *Business Innovation and the Law: Perspectives from Intellectual Property, Labour, Competition & Corporate Law*, (Edwards Elgar Publ., Cheltenham, UK, 2013), 113-116, <https://ssrn.com/abstract=2287765> accessed 10 March 2021.

59 White Paper, COM (2020) 65 final, 12: 'Market surveillance and enforcement authorities may find themselves in a situation where they are unclear as to whether they can intervene, because they may not be empowered to act and/or don't have the appropriate technical capabilities for inspecting systems. Legal uncertainty may therefore reduce overall levels of safety and undermine the competitiveness of European companies....' In footnote 36, the White Paper provides the example of the smart watch for children: 'This product may cause no direct harm to the child wearing it, but lacking a minimum level of security, it can be easily used as a tool to have access to the child. Market surveillance authorities may find it difficult to intervene in cases where the risk is not linked to the product as such'.

60 WIPO, 'Artificial Intelligence' 2019 Technology Trends 37 <www.wipo.int/publications/en/details.jsp?id=4386> accessed 11 May 2020, where it is stated that deep learning showed an impressive average annual growth rate of 175 percent from 2013 to 2016 in patent filings.

61 In the summer of 2019, a painting exhibition was held at the University of Oxford by AI-DA, a robot that was awarded female identity, female image and emerged as a creator or artist.

reservations I have expressed have mainly moral and social bases while I pointed out the important legal incompatibilities which differ to some extent between the two scientific fields. There is no doubt that legislative initiatives should be taken at the EU level both for copyright and patent law. Introduction of sui generis solutions are more suitable for European countries' individual legal systems. On the one hand, the interest and value of humans and human creativity must be preserved in every way. On the other hand, regarding AI-generated outputs classified into works or inventions, legal exclusivity must be ensured through sui generis rights. The above option is a clear solution and does not force the existing legal framework to incorporate AI-generated outputs that have different structural characteristics from a work or from an invention arising from the human intellect.

JIPITEC

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

www.jipitec.eu