

jipitec

1 | 2024

Volume 15(2024)
Issue 1 ISSN 2190-3387

Editorial

by Séverine Dusollier

Articles

Different Digital Exhaustion: Enhancing Legitimacy of Content Moderation
by Jelizaveta Juříčková

To what extent can online service providers adopt voluntary content moderation measures without losing their immunity shields? A comparative analysis of online service providers' liabilities in the European Union and the United States
by Adriana Berbec

How the AI Act Applies to E-Commerce
by Elif Cansu Yaşar

Online Intermediaries and Trademark Owners: The Legal Position and Obligations of Online Intermediaries to Trademark Owners Prior and post-Louboutin v Amazon
by Dania van Leeuwen, Mark Leiser and Lotte Anemaet

Devaluing SEPs: Hold-up bias and side effects of the European Draft Regulation
by Oscar Borgogno and Giuseppe Colangelo

Trademark protection for faces? A comprehensive analysis on the benefits and drawbacks of trademarks and the right to facial image
by Barna Arnold Keserű

Editors:

Thomas Dreier
Séverine Dusollier
Lucie Guibault
Orla Lynskey
Axel Metzger
Miquel Peguera Poch
Karin Sein
Gerald Spindler (†)

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

www.jipitec.eu

2024



Editors:

Thomas Dreier
Séverine Dusollier
Lucie Guibault
Orla Lynskey
Axel Metzger
Miquel Peguera Poch
Karin Sein
Gerald Spindler (†)

Board of Correspondents:

Graeme Dinwoodie
Christophe Geiger
Ejan Mackaay
Rita Matulionyte
Giovanni M. Riccio
Cyrill P. Rigamonti
Olav Torvund
Mikko Välimäki
Rolf H. Weber
Andreas Wiebe
Raquel Xalabarder

Editor-in-charge for this issue:

Séverine Dusollier

Technical Editor:

Lars Flamme

ISSN 2190-3387

Funded by

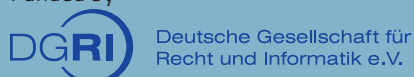


Table Of Contents

Editorial

by **Séverine Dusollier**

1

Articles

Different Digital Exhaustion: Enhancing Legitimacy of Content Moderation

by **Jelizaveta Juříčková**

2

To what extent can online service providers adopt voluntary content moderation measures without losing their immunity shields? A comparative analysis of online service providers' liabilities in the European Union and the United States

by **Adriana Berbec**

13

How the AI Act Applies to E-Commerce

by **Elif Cansu Yaşar**

38

Online Intermediaries and Trademark Owners: The Legal Position and Obligations of Online Intermediaries to Trademark Owners Prior and post-Louboutin v Amazon

by **Dania van Leeuwen, Mark Leiser and Lotte Anemaet**

56

Devaluing SEPs: Hold-up bias and side effects of the European Draft Regulation

by **Oscar Borgogno and Giuseppe Colangelo**

74

Trademark protection for faces? A comprehensive analysis on the benefits and drawbacks of trademarks and the right to facial image

by **Barna Arnold Keserű**

88

Editorial

by **Séverine Dusollier**

© 2024 Séverine Dusollier

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Séverine Dusollier, Editorial, 15 (2024) JIPITEC 1 para 1.

- 1 The AI Act has just been enacted by the EU Council when this new JIPITEC issue is finalized, adding another major piece to the construction of a comprehensive EU regulatory framework of digital technologies, actors and practices. The EU has been extremely active and a forerunner in addressing the effects of big online platforms and of AI development, as well as of the transition to a data-based economy and society. Articles on the many legislative acts have increasingly appeared in JIPITEC pages. This issue is no exception with three papers on recently adopted EU regulations. A first article by Jelizaveta Juříčková scrutinises the question of copyright content moderation, mandated by both the 2019 Copyright directive and the DSA, in the light of procedural justice that, based on users' perceptions of fairness, could provide an interesting approach to content moderation. The platforms liability, as enacted in the DSA, is also the topic of Adriana Berbec's paper that compares the EU regulatory framework with the US long standing section 230 of the Communication Decency Act, as well as case law in both jurisdictions. The AI Act then is examined, by Elif Cansu Yaşar, in the form of a rarely raised interrogation: can it apply to e-commerce practices such as data analytics, personalisation of shopping experiences and custom-made advertisements?
- 2 The other articles composing this issue relate to 'classical' IP questions, though certainly revisited by the rapid evolution of technology. The new standard of 'commercial communication' proposed by the CJEU in the *Louboutin v. Amazon* case to identify an active role of the online intermediary in trade mark infringements and its connection to the perspective of the internet user is analysed by Dania van Leeuwen, Mark Leiser and Lotte Anemaet under the light of the DSA liability regime. In another article, Oscar Borgogno and Giuseppe Colangelo tackle the complex and fascinating issue of standard-essential patents with a critical analysis of the recent EU proposal for a regulation, arguing that it creates a potential risk for investments in innovation. Finally the intriguing question of the registrability of human faces as trade marks and how trade mark law can complement personality rights in protecting use of such images is studied by Barna Keserű.
- 3 Once again this JIPITEC issue demonstrates the vitality of digital law and IP scholarship in a rapidly ever-changing legal environment.

Enhancing Legitimacy of Content Moderation

by Jelízaveta Juříčková *

Abstract: Platforms are actively developing strategies to enhance the legitimacy of their content moderation and gain acceptance and trust across diverse user groups. This paper explores one such strategy, endorsed by the EU regulator, which involves proceduralizing content moderation, with a focus on copyright enforcement as a case study. However, the paper raises concerns regarding the efficacy of proceduralization in legitimizing content moderation, citing historical limitations in the adoption of dispute resolution mechanisms by ordinary

users. In response, the paper suggests a complementary approach: integrating elements of procedural justice, based on users' perceptions of fairness, into the implementation of content moderation requirements mandated by regulators. By elucidating how procedural justice enhances legitimacy and drawing from user experiences with content moderation, the paper proposes a preliminary index of procedural justice values to be used as a metric and guidance for putting regulatory requirements into practice.

Keywords: Online Platforms; Content Moderation; Procedural Justice

© 2024 Jelízaveta Juříčková

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Jelízaveta Juříčková, Enhancing Legitimacy of Content Moderation, 15 (2024) JIPITEC 2 para 1.

A. Introduction

1 Initially, rightsholders struggled to enforce copyright against individual internet users, only to later pivot their approach by enlisting the assistance of online intermediaries, including online platforms, as “innocent bystanders”.¹ Now, we find ourselves

in a time where the dynamics have changed once more, as platforms are mandated to take a proactive role in enforcing copyright, as evident in CDSM² and DSA.³ However, this newfound responsibility has left

* Ph.D. candidate at the Institute of Law and Technology, Masaryk University. This article was written at Masaryk University as part of the project n. MUNI/A/1529/2023 - Právo a technologie XII.

1 Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (Cambridge University Press 2017) <<https://www.cambridge.org/>

core/books/injunctions-against-intermediaries-in-the-european-union/A42D5F859EF35FAF33C2FC4EB65A6AAA>.

2 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

3 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).

platforms ill at ease, as they face increased scrutiny from various stakeholders: the public, including the platform users, creative industries, and academia.⁴ In response, platforms are devising strategies to legitimize their content moderation efforts, seeking acceptance and trust from these diverse groups.

- 2 One such strategy involves proceduralization of content moderation. This approach has also been embraced by EU regulator as a means to bring structure and accountability to the process. While this is a positive step, we must ask ourselves, is it enough to win over the general public? My argument suggests that it might not be sufficient, particularly considering that the dispute resolution mechanisms, the very vehicles of proceduralization approach, have historically seen limited adoption by ordinary users.⁵
- 3 Considering this, a complementary approach is proposed: focusing on procedural justice in the psychological sense when implementing content moderation requirements imposed by the regulator. This approach goes hand in hand with proceduralization, complementing it while emphasizing a different aspect. By prioritizing procedural justice, platforms can foster a notion of fair content moderation among users, thereby favourably changing their perception of its legitimacy. This emphasis on procedural justice could bridge the gap between platforms' efforts to enforce copyright and the acceptance and understanding of these measures by the broader public.
- 4 Section 2 introduces the proceduralization trend in content moderation and its role as a platform governance legitimation strategy. Section 3 provides examples of proceduralization within platform initiatives, focusing on copyright content

moderation as a case study. Section 4 analyzes the EU-level regulatory framework governing copyright content moderation and sheds light on the limits of the proceduralization approach embedded in the regulatory framework. The paper posits that proceduralization primarily promotes legality-based legitimacy while neglecting sociological legitimacy. Furthermore, it is maintained that dispute resolution mechanisms as pivotal components of proceduralization, rely on adoption by users, which historically tends to be low. To address the limitations discussed in Section 4, Section 5 proposes a complementary legitimation strategy. This approach involves integrating elements of procedural justice, as derived empirically from psychological research, into the practical implementation of the regulatory framework by both platforms and dispute resolution bodies. These elements have been shown to influence sociological legitimacy and complement formal legality. The paper further discusses how EU regulator can incentivize platforms and dispute resolution bodies to adhere to this strategy. Section 6 we summarizes key findings and insights from the preceding sections.

B. Proceduralization Approach in Content Moderation

- 5 Proceduralization of content moderation refers to the process of establishing explicit rules, procedures, and standards for content moderation on online platforms. It involves making the content moderation process more structured and systematic, akin to legal or judicial systems.⁶ Proceduralization comprises the following aspects — due process, quality of decisions and transparency.
- 6 Incorporation of safeguards of due process ensures that users whose content is being moderated have certain rights and protections.⁷ This might include the right to report a piece of content that breaches the user's rights, the right to be notified about the action undertaken towards the content and be provided with justification and the right to appeal the decision. Internal mechanisms for reviewing the appeal by the platform present a particularly fruitful ground for implementation of due process features. A meaningful pendant to review by platforms are external mechanisms for settlement of disputes,

4 Taddeo and Floridi bring a comprehensive overview of the discourse regarding responsibilities of intermediaries, empirically demonstrating its evolution by evaluating relevance of the topics based on the volume of literature dedicated to each topic. Mariarosaria ed. Taddeo and Luciano ed. Floridi, *The Responsibilities of Online Service Providers* (1., Springer International Publishing AG). Chapter 2.

5 Lenka Fiala and Martin Husovec, 'Using Experimental Evidence to Improve Delegated Enforcement' (3 March 2022) <<https://papers.ssrn.com/abstract=3218286>> accessed 9 May 2023; Jennifer M Urban, Joe Karaganis and Brianna L Schofield, 'Notice and Takedown: Online Service Provider and Rightsholder Accounts of Everyday Practice' (2017) 64 *Journal of the Copyright Society of the USA* 317; Jennifer M Urban and Laura Quilter, 'Symposium Review Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act' (2000) 512 621.

6 Evelyn Douek, 'The Siren Call of Content Moderation Formalism' (10 January 2022) <<https://papers.ssrn.com/abstract=4005314>> accessed 21 June 2023.

7 Catalina Goanta and Pietro Ortolani, 'Unpacking Content Moderation: The Rise of Social Media Platforms as Online Civil Courts' (22 November 2021) <<https://papers.ssrn.com/abstract=3969360>> accessed 19 June 2023 p. 18.

promoted by the regulator.

- 7 The second aspect of proceduralization is raising standards for quality of decisions in content moderation. By drawing on the principles and logic used in judicial systems, consistent and coherent reasoning is applied to content decisions.⁸ It involves following past decisions as precedents for current and future rulings, creating a sense of predictability.⁹
- 8 The third aspect, transparency, involves explaining the steps of content moderation, i.e. laying out the specific actions and procedures that content moderators follow when evaluating and handling content. It presents a *conditio sine qua non* for control of content moderation by public, academia and the regulator by offering the insight into the actual content moderation practices.
- 9 Formalizing content moderation has a significant potential to improve its legitimacy. The main legitimacy concepts are normative, focusing on the justification of power, sociological, which examines how the subordinate perceive legitimacy of the ruling power,¹⁰ or hybrid.¹¹ An example of latter type and a point of reference for this paper is Beetham's conception, that acknowledges legality, i.e. the necessity of exercising power according to established rules, as an essential but insufficient aspect of legitimacy, contending that the power needs to be justified in terms of peoples' beliefs.¹²
- 10 Proceduralization impacts legitimacy in the following ways. Firstly, it advances the value of legality. Secondly, proceduralization legitimizes content moderation by promoting due process, an integral part of rule of law ideal,¹³ that serves

as a benchmark of political legitimacy¹⁴ and an adequate framework for discussions about legitimate exercise of governance power.¹⁵ Thus, imbuing the procedure with guarantees of due process enhances its legitimacy by aligning content moderation with rule of law.

C. Proceduralization by Platforms

- 11 In the area of copyright, proceduralization efforts of platforms appear to be most prominent in policymaking and oversight. Platforms devise increasingly detailed substantive and procedural rules on content moderation in terms of service, policies and help pages, approaching "the prolixity of a legal code".¹⁶ While this approach might enhance legitimacy by offering users greater certainty, empirical evidence indicates that the proliferation of regulations has led to heightened complexity.¹⁷ This is evident in the significant surge in the variety of documents, the gradual diversification in normative types and subjects of regulations.¹⁸ Consequently, platforms achieve the opposite of the intended effect by making it challenging for users to navigate the waters of content moderation.
- 12 As to oversight, platforms have made efforts to facilitate external scrutiny of their content moderation practices through transparency reports. As an illustration, since December 2021, YouTube has been issuing a semi-annual Copyright Transparency Report.¹⁹ These reports play a crucial role in promoting accountability and transparency by showcasing how content moderation decisions are made and enforced. Nevertheless, it's important to recognize that as platforms have the discretion

8 Douek (n 6), p. 3.

9 *ibid.*

10 Reinhard Bendix, *Max Weber: An Intellectual Portrait* (Routledge 1998).

11 Fabienne Peter, 'Political Legitimacy' (*Stanford Encyclopedia of Philosophy*, rev 2017 2010) <<https://plato.stanford.edu/entries/legitimacy/#LegJusPolAut>>.

12 David Beetham, *The Legitimation of Power* (Issues in Political Theory, Palgrave MacMillan 1991). p. 65-80. Beetham's framework includes the concept of subordinate consent as a component of legitimacy. However, it's important to note that this paper only partially employs his legitimacy framework as a reference point, and thus, the notion of subordinate consent is not a central focus within the scope of this paper.

13 Jeremy Waldron, 'The Concept and the Rule of Law' (2008) 43 *Georgia Law Review* <<https://digitalcommons.law.uga>.

edu/cgi/viewcontent.cgi?article=1028&context=lectures_pre_arch_lectures_sibley>. p. 7, 62.

14 *ibid.* p. 3.

15 Nicolas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 *Berkeley Technology Law Journal* 1817. p. 1836.

16 Douek (n 6), p. 6.

17 João Pedro Quintais and others, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (reCreating Europe 2022) <<http://dx.doi.org/10.2139/ssrn.4210278>>.

18 *ibid.*

19 'Copyright Transparency Report H1 2021' (YouTube 2021) <<https://blog.youtube/news-and-events/access-all-balanced-ecosystem-and-powerful-tools/>>.

to determine which information is included and how it is presented, transparency reports can also be strategically leveraged to shape a specific narrative.²⁰ For example, platforms might use these reports to craft a more favourable image of their content moderation efforts.

- 13 Before the enactment of the pertinent EU legislation, namely the CDSM Directive, a significant proceduralization endeavour involved platforms voluntarily adhering to codes of conduct, which influenced creation and application of content moderation rules.²¹ One specific aspect of codes of conduct that contributed to proceduralization were rules about notice and takedown mechanisms.²² These processes were notably absent from the EU safe harbour framework at that time.²³ Furthermore, codes of conduct encompassed obligations such as issuing warnings to subscribers engaged in infringing activities, retaining crucial traffic data, disclosing the identities of implicated subscribers and terminating accounts of the infringers.²⁴
- 14 Another example of voluntary proceduralization initiative are Santa Clara Principles, are a set of guidelines developed to safeguard freedom of expression and privacy rights in content moderation practices and endorsed by major platform providers such as Meta, Google, Reddit, X, and GitHub.²⁵ The

principles emphasize transparency, accountability, and user empowerment in online platforms' content removal policies and advocate for clear explanations of content moderation decisions, opportunities for appeal, and limitations on the use of automated tools in content removal.

- 15 Providing a possibility to appeal platform's content moderation actions may also be counted among the proceduralization measures. The problem is that platforms partially do so to comply with their legal obligations, in particular DMCA.²⁶ However, it's worth noting that many platforms proactively take the initiative to establish complaint and redress mechanisms that go beyond what is strictly required by law.²⁷ To that extent, provision of such mechanisms may be considered platforms' own proceduralization initiative.
- 16 The crown jewel of platforms' proceduralization efforts is Meta's Oversight Board, that gives impression of being created for the sole purpose of legitimization. Its design borrows attributes of supreme or constitutional courts,²⁸ creating "an institutional aesthetic of governance."²⁹ Oversight

accessed 6 March 2024.

- 20 Aleksandra Urman and Mykola Makhortykh, 'How Transparent Are Transparency Reports? Comparative Analysis of Transparency Reporting across Online Platforms' (2023) 47 Telecommunications Policy 102477.
- 21 For instance, in 2007, several UGC platforms, such as MySpace, Veoh, DailyMotion, and Soapbox, joined forces with major players of creative industry such as Disney, CBS, NBC Universal, and Viacom to put forth a set of guidelines known as the 'Principles for User Generated Content Services' See 'User Generated Content Principles' <<http://ugcprinciples.com/>> accessed 7 June 2023; discussed in Michael S Sawyer, 'Filters, Fair Use & Feedback: User Generated Content Principles and the DMCA' (2009) 24 Berkeley Technology Law Journal 363.
- 22 P Bernt Hugenholtz, 'Codes of Conduct and Copyright Enforcement in Cyberspace' (7 March 2012) <<https://papers.ssrn.com/abstract=2017581>> accessed 7 June 2023.
- 23 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').
- 24 Hugenholtz (n 22).
- 25 'Santa Clara Principles on Transparency and Accountability in Content Moderation' (*Santa Clara Principles*) <<https://santaclaraprinciples.org/images/santa-clara-OG.png>>

- 26 Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 1201 et seq. (1998).
- 27 Péter Mezei and István Harkai, 'End-User Flexibilities in Digital Copyright Law – An Empirical Analysis of End-User License Agreements' (3 July 2021) <<https://papers.ssrn.com/abstract=3879740>> accessed 14 September 2023.
- 28 For example, the case selection mechanism bears resemblance to the certiorari process employed by the US Supreme Court. This process involves the careful selection of a limited number of cases, with a particular emphasis on disputes that present significant legal questions. Inspiration from European constitutional courts is on the contrary visible in "a prevalence of written over oral submission, a limited role for the disputing parties, and an emphasis on the development of the law for the future. See Goanta and Ortolani (n 7).but fail to ensure adequate access to justice through content moderation when harms arise. This chapter focuses on a gap in current scholarship on platform governance, by addressing content moderation from the procedural perspective of dispute resolution. We trace the emergence of content moderation as a form of digital dispute resolution, proposing a theoretical framework for the understanding of social media platforms as private adjudicators, and illustrating how platforms have progressively embraced this role. This framework is further complemented by an empirical overview of the content reporting mechanisms of four social media platforms (Facebook, TikTok, Twitch and Twitter p. 17.
- 29 Monroe E Price and Joshua M Price, 'Building Legitimacy

Board serves as policy advisor, an appeal board and a source of information about Meta's content moderation structures and processes. It remedies ad hoc content moderation shortcomings by reviewing a small number of "highly emblematic" cases selected by it from appeals by users,³⁰ assessing the compliance of content with Facebook's policies³¹ in the light of international human rights standards.³² Oversight Board has yet to make a decision on any copyright-related matter. However, the possibility remains that it may do so in the future, for instance in a case involving the balancing of copyright and freedom of expression.

D. Proceduralization in Regulatory Framework

I. Article 17 CDSM Directive

17 The first major regulatory intervention of the EU legislator concerning copyright content moderation is Article 17 of the CDSM Directive.³³ Procedural elements in Article 17 give the impression of being somewhat perfunctory. Article 17 enhances due process for rightsholders by providing them with an additional avenue of asserting their rights by means of providing "relevant and necessary" information regarding their works.

18 However, Article 17 does not improve the position of the users from the procedural perspective. An interesting safeguard is the obligation of platforms to inform their users in their terms and conditions of the possibility to use the defence of copyright

in the Absence of the State: Reflections on the Facebook Oversight Board' [2023] *International Journal of Communication*; Vol 17 (2023) 3 p. 6.

30 'Oversight Board | Independent Judgment. Transparency. Legitimacy.' <<https://www.oversightboard.com/>> accessed 8 May 2023.

31 *ibid.*

32 Those norms include the International Covenant on Civil and Political Rights (ICCPR)'s Article 19, which states that while "everyone shall have the right to freedom of expression...the exercise of [that] right may...be subject to certain restrictions, but only...as provided by law and are necessary. 'Oversight Board Annual Report 2021' (Oversight Board 2022). p. 9.

33 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

exceptions or limitations. Unfortunately, it seems to be dysfunctional, as explained in Section 5.1.2.

19 Mechanisms for appealing content moderation decisions — a single procedural safeguard of relevance for users — are lacking. Firstly, the range of content moderation decisions which may be appealed is limited to removal or access restriction, not taking into account that the preferred action in the majority of copyright infringement claims is demonetization.³⁴ Secondly, Article 17 (9) does not provide foundations for adversarial proceedings.³⁵ For example, it merely requires that decisions to disable access to or remove uploaded content shall be subject to human review, without specifying who performs the review. Consequently, complaint and redress mechanisms offered by Meta (for Facebook and Instagram) and by YouTube,³⁶ in which the platform acts as a messenger rather than an arbiter and the decision about content is made by the rightsholder,³⁷ would be compliant with this provision. Another remedy available to the user, out-of-court redress mechanisms, should enable impartial settlement of disputes arising from content moderation. Article 17 places no requirements on the dispute resolution bodies and does not incentivize either platforms or rightsholders to participate in the scheme.

20 Additionally, Article 17 does not promote the quality of content moderation decisions. It does not attempt to influence the accuracy of content moderation decisions³⁸ by placing requirements on the setting

34 Henning Grosse Ruse-Khan, 'Automated Copyright Enforcement Online: From Blocking to Monetization of User-Generated Content', *Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur* (Cambridge University Press 2021) <10.1017/9781108688529>. p. 2.

35 A cornerstone to the right to a fair trial, a corollary to the right to an effective remedy according to Article 47 of the Charter of Fundamental Rights. Manuel Kellerbauer, Marcus Klamert and Jonathan Tomkin (eds), *The EU Treaties and the Charter of Fundamental Rights: A Commentary* (Oxford University Press 2019) <<https://doi.org/10.1093/oso/9780198794561.001.0001>> accessed 16 April 2023. p. 2222.

36 'Dispute a Content ID Claim - YouTube Help' <<https://support.google.com/youtube/answer/2797454?hl=en-GB>> accessed 14 April 2023.

37 'Resolve Usage Disputes in Rights Manager' (*Meta Business Help Centre*) <<https://en-gb.facebook.com/business/help/2523148971045474>> accessed 14 September 2023.

38 Niva Elkin-Koren, 'Fair Use by Design' (2017) <<https://papers.ssrn.com/abstract=3217839>> accessed 6 January 2023.

of parameters of automated content filtering tools, nor does it require the original content moderation decision or the result of dispute to be accompanied by justification. Transparency is also neglected by Article 17. The only transparency obligation in Article 17 does not extend to dispute resolution. It is limited to information regarding platforms actions towards content and the use of licensed works in content. Additionally, it is curiously one-sided, applying only to the rightsholder. Therefore, the regulator is unable to supervise the quality of content moderation due to the lack of data.

II. Digital Services Act

- 21 On the contrary, the DSA, which marks a “procedural turn” in EU lawmaking, considerably proceduralizes content moderation by introducing a set of obligations spanning the whole content moderation process.³⁹ Article 16 DSA establishes clear rules for reporting content. Article 17 DSA, a provision that is also applicable to the Article 17 CDSM regime, requires every content moderation decision to be accompanied by a statement of reasons. It should explain what actions are being taken and their scope, as well as where and for how long they apply, the reasons for the decision, use of automated processes and legal basis for determining that the piece of content in question is illegal. Importantly, it should also contain information about how the recipient of the decision may seek redress.
- 22 Article 20 DSA broadens access to justice by encompassing a significantly wider array of content moderation decisions that extend beyond the mere blocking and removal of content.⁴⁰ It emphasizes accessibility and fairness: submission of complaints should occur electronically and free of charge, the mechanism should be user-friendly and complaints should be handled in a non-discriminatory, diligent and non-arbitrary manner. Also, according to Article 14 DSA, the platform should provide rules of the complaint-handling procedure in Terms and Conditions.
- 23 The out-of-court dispute settlement mechanism in DSA is also fully compliant with the proceduralization approach. To fall within the purview of Article 21,

a dispute resolution body must obtain certification, contingent on criteria such as impartiality and independence, the establishment of clear and fair procedural rules, and the capacity to efficiently resolve disputes⁴¹ – all of which align with the due process requisites specified in Article 47 of the EU Charter of Fundamental Rights. Furthermore, the designated body must possess the requisite expertise, and the dispute should take place online.⁴² The platform is mandated to engage in the dispute resolution process presented by an entity chosen by the service recipient, unless a dispute has already been resolved concerning the same information and the same grounds.⁴³ Moreover, the DSA imposes a time constraint of 90 days for the resolution process⁴⁴ and establishes a mechanism for attributing procedural costs, which tilts the balance in favour of users over platforms,⁴⁵ contributing to equality of arms.

- 24 The same holds for transparency provisions regarding use of automated content recognition tools,⁴⁶ complaint and redress mechanisms,⁴⁷ cases submitted to out-of-court dispute resolution bodies⁴⁸ and database of content moderation decisions.⁴⁹ They provide the public with exhaustive information

41 Article 21(3) DSA.

42 *ibid.*

43 Article 21(2) DSA.

44 Article 21(2) DSA.

45 According to Article 21(5) DSA, if the out-of-court dispute settlement body decides in favor of the user, the online platform provider must bear all fees and reimburse the user for reasonable expenses related to the dispute. If the decision favors the provider, the user is not required to reimburse any fees or expenses of the provider of the online platform paid, unless they are found to have acted in bad faith.

46 These include the following obligations of providers of online platforms: include information about the use of algorithmic decision-making in content moderation in their Terms and Conditions (Article 14(1) DSA); provide detailed information about use of automated tools in content moderation in the annual transparency report (Article 15(1) (c) and (e) DSA); and inform a user in the particular instance of content moderation about the use of the use made of automated means in taking the decision regarding content (Article 17(3) c) DSA).

47 Article 20 DSA.

48 Article 21 DSA.

49 Article 24(5) DSA.

39 Pietro Ortolani, ‘If You Build It, They Will Come: The DSA “Procedure Before Substance” Approach’, *Putting the Digital Services Act into Practice: Enforcement, Access to Justice, and Global Implications* (Verfassungsblog 2023).

40 According to Article 20(1) DSA, users can appeal decisions regarding the removal or restriction of access to content, the suspension or termination of services or user accounts, and the restriction of monetization of user content.

regarding both types of mechanisms, enabling the exercise of control and promoting consistency of decision-making.

III. Limits of Proceduralization Approach

- 25 As previously discussed, proceduralization significantly enhances the legitimacy of content moderation practices. Additionally, it establishes legal certainty by defining expectations for all involved parties. The implementation of formalized procedures also simplifies the task of holding platforms accountable for their content moderation decisions, as these procedures are documented and subject to review and assessment. Nonetheless, it's important to acknowledge that proceduralization does have its limits.
- 26 As was said in Section 2, proceduralization promotes legitimacy of content moderation by advancing the legality principle. It is also important to bear in mind that legality is only one aspect of the legitimacy concept — necessary, but insufficient.⁵⁰ Relying solely on a formalistic approach cannot inherently legitimize content moderation. The reason is that “[a]uthority also needs to be sociologically and morally legitimate to be accepted, and legalistic legitimacy alone is not enough to garner social and moral respect”.⁵¹ Content moderation should also be justifiable in terms of beliefs of the relevant constituency,⁵² who in this case arguably are the users as the addressees of platform governance.
- 27 The second problem is that the impact of mechanisms of redress, which constitute an essential vehicle of proceduralization approach, is dependent on the uptake by the stakeholders – civic rights organisations, external dispute settlement bodies, but most importantly ordinary users. For both of those mechanisms, the uptake by individuals is crucial, that happens to be notoriously low in copyright content moderation cases.⁵³ Possible reasons for under-assertion include intimidation and a weak prospect of successful redress.⁵⁴ A causality

circle emerges here: the mechanisms will serve as an instrument of legitimation when taken up by the people, and the people, in turn, will adopt these mechanisms if they perceive them as a legitimate means of resolving their problems.

E. Procedural Justice Approach as a Successor of Proceduralization

- 28 To address the concerns with lukewarm adoption of dispute resolution mechanisms and enhance the legitimacy of content moderation in the sociological sense, this section proposes a complementary legitimization strategy that aligns with the proceduralization approach. The strategy entails the incorporation of the psychological concept of procedural justice into the practical implementation of the legal framework, specifically focusing on the establishment of dispute resolution mechanisms.

I. Procedural Justice, Due Process and Legitimacy

- 29 Procedural justice in the psychological sense refers to how individuals subjectively perceive the fairness of the process. While distinct from distributive justice that centres on outcome fairness, procedural justice nonetheless is empirically proven to have a positive impact on distributive justice judgments, even in cases when outcomes are negative.⁵⁵ The scope of procedural justice concept is very broad – in fact, it is applicable to any social processes where outcomes are allocated,⁵⁶ which distinguishes it from formal due process principles and makes it suitable for application to content moderation. At the same time, procedural justice is a natural pendant to due process principles. The popular notion of fair procedure provided the original impetus for the creation of due process principles, while due process principles in turn equip people with “a helpful template for what fair process looks like” in forming the perception of what is fair.⁵⁷

50 Beetham (n 12). p. 69.

51 Douek (n 6). p. 15.

52 Beetham (n 12). p. 17.

53 Annemarie Bridy and Daphne Keller, ‘U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry’ (2017) 7 SSRN Electronic Journal; Urban, Karaganis and Schofield (n 5).

54 Fiala and Husovec (n 5).

55 Edgar Allan Lind and Tom Tyler, *The Social Psychology of Procedural Justice*, vol 18 (Springer Science + Business Media LLC 1988). p. 67.

56 Rebecca Hollander-Blumoff and Tom Tyler, ‘Procedural Justice and the Rule of Law: Fostering Legitimacy in Alternative Dispute Resolution’ (2011) 2011 Journal of Dispute Resolution <<https://scholarship.law.missouri.edu/jdr/vol2011/iss1/2/>>.

57 *ibid.* p. 9.

- 30 Various criteria influence procedural justice judgments. For instance, it has been found that people value control over the process and outcome, ethical behaviour of the authority, and impartiality.⁵⁸ Ethicality encompasses politeness and respect for disputants' rights, while process control involves being heard and presenting information that the individual considers important. Other sources cite the authority's consideration of arguments,⁵⁹ ability to gather sufficient information for a high-quality decision, consistency in decisions, and credibility of the decision-making authority in the sense that it made best efforts to do the disputants justice.⁶⁰ Additional criteria which matter to the disputants include airing the problem, speed of resolution, personal control, animosity reduction, cost, minimizing disruption of everyday affairs, and reducing the possibility of future conflict.⁶¹
- 31 The connection between legitimacy and procedural justice is supported by empirical evidence showing that people base their judgments about the overall legitimacy of authorities on their personal experiences with their representatives.⁶² While various factors impact people's attitudes towards authorities,⁶³ assessments of procedural fairness have been identified as the major influence,⁶⁴ surpassing distributive fairness.⁶⁵ Notably, even in cases of negative outcomes, fair procedures act as a cushion, maintaining high levels of support for the

authority.⁶⁶

II. Procedural Justice Values in Content Moderation

As regards empirical evidence of which elements of procedural justice are relevant for content moderation, it is possible to draw from a rich body of knowledge has emerged in recent years through empirical studies examining user accounts of their interactions with platforms.⁶⁷ Since the literature focuses on shortcomings of content moderation, these accounts serve to define the procedural justice values in content moderation negatively, i.e. by their absence.

Value	Content Moderation Stage
"Legal aid" – explanation of substantive and procedural platform policies, ideally with examples	Stage 1
Individualized explanation of the decision	Stage 1
Accessibility of redress mechanisms	Between Stage 1 and 2
Quality of human interactions	Stages 1 and 2
Opportunity to present user's case	Stage 2
Impartiality of content moderators	Stage 2
Qualification of content moderators	Stage 2

This chart summarizes procedural justice values derived from the studies, explained in more detail in the following sections.

58 Tom R Tyler, 'What Is Procedural Justice?: Criteria Used by Citizens to Assess the Fairness of Legal Procedures' (1988) 22 Law & Society Review 103.

59 Donald E Conlon, E Allan Lind and Robin I Lissak, 'Nonlinear and Nonmonotonic Effects of Outcome on Procedural and Distributive Fairness Judgments.' (1989) 19 Journal of Applied Social Psychology 1085.using a classic procedural justice paradigm (e.g., L. Walker et al; see record 1975-23047-001

60 Hollander-Blumoff and Tyler (n 56). p. 5.

61 Robin I Lissak and Blair H Sheppard, 'Beyond Fairness: The Criterion Problem in Research on Dispute Intervention.' (1983) 13 Journal of Applied Social Psychology 45.

62 Tom R Tyler, *Why People Obey the Law* (Princeton University Press 2006) <<http://www.jstor.org/stable/j.ctvj66769>> accessed 5 October 2022. p. 88, 91.

63 For example, previous experience, social background, moral convictions of the individual and instrumental considerations, such as personal gain from the outcome.

64 Lind and Tyler (n 55). p. 78.

65 *ibid.* p. 65.

1. The First Stage – Content Detection

- 32 The bulk of academic literature focuses on the first content moderation stage – (automated) detection of content that infringes copyright or platform

66 *ibid.* p. 71.

67 Sophie Bishop, 'Managing Visibility on YouTube through Algorithmic Gossip' (2019) 21 New Media & Society 2589; Sophie Bishop, 'Influencer Creep: How Artists Strategically Navigate the Platformisation of Art Worlds' [2023] New Media & Society 14614448231206090; Laura Savolainen and Minna Ruckenstein, 'Dimensions of Autonomy in Human-Algorithm Relations' [2022] New Media & Society 14614448221100802; Sarah Myers West, 'Censored, Suspended, Shadowbanned: User Interpretations of Content Moderation on Social Media Platforms' (2018) 20 New Media & Society 4366; Kelley Cotter, 'Playing the Visibility Game: How Digital Influencers and Algorithms Negotiate Influence on Instagram' (2019) 21 New Media & Society 895; Brooke Erin Duffy and Colten Meisner, 'Platform Governance at the Margins: Social Media Creators' Experiences with Algorithmic (in)Visibility' (2023) 45 Media, Culture & Society 285.

policies and application of a wide range of content moderation measures, including restriction of visibility or demotion, which forms the primary object of interest in the studies. Many of them describe how users, in particular content creators, attempt to decode and adapt to the principles of functioning of algorithms and avoid having the visibility of their content reduced,⁶⁸ while some of them examine how algorithms shape the creative process and the presentation of users on the internet.⁶⁹

responses.⁷⁵

- 33 The first element that emerges from the user accounts is the need for clear and detailed rules of application of platform “substantive law”. Users perceive rules contained in terms and conditions or community guidelines as vague and unhelpful and miss specific examples.⁷⁰ Therefore, they develop heuristics, such as which hashtags to use or how much skin to show to avoid being flagged for nudity, and share this information in support groups.⁷¹ In the field of copyright, users have proven themselves woefully ignorant of the legal basics and platform policies, expressing a desire to learn more.⁷² Consistency in platform decisions, unsurprisingly, emerges as another trait valued by users, who frequently expressed frustration at the erratic nature of platform decisions.⁷³
- 34 Another important factor is an individualized explanation of reasons behind the decision. Users lamented the lack of detailed explanation of how user violated community guidelines, reporting that instead, they receive generic repetitive references to general platform policies.⁷⁴ Unfortunately, the obligation to provide statement of reasons for the decision introduced by Article 17 DSA is unlikely to change the users’ dissatisfaction in that regard, since the provision merely lists the mandatory elements without requesting an individualized response. As the examples from DSA Transparency Database demonstrate, platforms continue to use formulaic

68 Cotter (n 67); Duffy and Meisner (n 67).

69 Cotter (n 67).

70 Duffy and Meisner (n 67). p. 295.

71 *ibid.* p. 297.

72 Daria Dergacheva and Christian Katzenbach, “‘We Learn Through Mistakes’: Perspectives of Social Media Creators on Copyright Moderation in the European Union’ (2023) 9 *Social Media + Society* 20563051231220329. p. 5.

73 Duffy and Meisner (n 67).

74 *ibid.*

75 <https://transparency.dsa.ec.europa.eu/statement>

2. Stage One-and-a-Half: Transition from the First to the Second Stage

- 35 For the success of next content moderation stage, the internal and external redress mechanisms, the decisive moment is whether users will engage with them. Therefore, accessibility emerges as a prerequisite value for these mechanisms. This is corroborated by the evidence from content moderation, citing that a relatively high number of users express desire to appeal the mechanism and yet encounter problems such as unclear instructions,⁷⁶ and an example from a different field – the soon-to-be repealed ODR platform for resolution of consumer disputes, which, while exhibiting a 8.5 million visits, only enables on average 200 cases per year to be treated by ADR entities,⁷⁷ since its design is confusing to users.⁷⁸ While DSA attempts to address this problem by requiring that the user accesses the procedure simply by clicking on a link that leads to internal mechanism or a page where dispute settlement bodies present themselves for an easy selection.⁷⁹

3. The Second Stage – Appeal Mechanisms

- 36 The second stage becomes relevant when the content is blocked and the user appeals the decision. Both Article 17 of the DSM Directive and Article 20 of the Digital Services Act provide and obligation

of platforms to establish an internal complaint-handling mechanism, where the platform acts as an arbiter and, when platform's own-initiative content moderation measure is disputed, platform plays the party to the dispute. The use of external mechanism is not pre-conditioned on the internal process.

- 37 An overarching and essential factor for the second content moderation stage is human interaction. This factor related to both the desire to be heard, i.e. to present information the individual considers important, and to receive a satisfactory explanation of their case. Some users went to considerable lengths to exercise their “right to be heard” – finding other means of communication not designed for such cases, such as via company accounts on other social media platforms or technical support channels.⁸⁰ Nevertheless, the users were not willing to accept just any human interaction; it had to meet specific quality standards. Some users who interacted with human personnel complained that their responses were formulaic and repetitive, not offering any relief in comparison with responses from a bot.⁸¹ Another concern was over the qualification and impartiality of content moderators. The users expressed doubts about content moderators' expertise and impartiality, asserting that they are biased towards marginalized groups.⁸²

III. The Role of the Regulator

- 38 It remains to be examined how can the regulator contribute to introducing procedural justice in the design of redress mechanisms, using the above-described procedural justice index. In case of out-of-court dispute resolution bodies, Digital Services Coordinators (“DSC”)⁸³ have a considerable leverage over them, since they are the authority which provides them with time-limited and revocable certification, assessing inter alia whether their rules of procedure are fair or whether the body's expertise allows them to settle the dispute effectively.⁸⁴ Further, the bodies report to DSC annually as regards their operation and DSC may offer them recommendations as to how improve their functioning.⁸⁵ In both of these

⁷⁶ Myers West (n 67), p. 4378.

⁷⁷ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL repealing Regulation (EU) No 524/2013 and amending Regulations (EU) 2017/2394 and (EU) 2018/1724 with regards to the discontinuation of the European ODR Platform 2023.

⁷⁸ Emma van Gelder, *Consumer Online Dispute Resolution Pathways in Europe: An Analysis into Standards for Access and Procedural Justice in Online Dispute Resolution Procedures* (2022) p. 158-161.

⁷⁹ This is required by the DSA in several provisions. Firstly, article 17(3)f requires statement of reasons to contain “clear and user-friendly information on the possibilities for redress available to the recipient of the service in respect of the decision, in particular, where applicable through internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress”. Secondly, article 20(3) demands that the internal complaint-handling mechanism is easy to access and user-friendly. Also, article 21(1) requires providers of online platforms to ensure that “information about the possibility for recipients of the service to have access to an out-of-court dispute settlement, [...], is easily accessible on their online interface, clear and user-friendly”.

⁸⁰ Myers West (n 67), p. 4376.

⁸¹ *ibid.* p. 4377.

⁸² Duffy and Meisner (n 67), p. 238.

⁸³ The authorities responsible for enforcement of DSA, together with the Commission. See Articles 49-51 DSA.

⁸⁴ Article 21(3) DSA.

⁸⁵ Article 21(4) DSA.

functions, DSC may use the procedural justice index as a point of reference.

- 39 The key question is how to encourage platforms to prioritize procedural justice when shaping their dispute resolution mechanisms. While platforms are showing engagement with proceduralization trend, it remains uncertain whether their commitment is sincere or a form of virtue signalling. Given their profit-oriented nature, platforms might concentrate on improving content moderation in less controversial areas than copyright, where the discourse is dominated by two antagonist groups of rightsholders and free speech advocates.
- 40 In case of very large online platforms, Commission and the European Board for Digital Services⁸⁶ may impact their implementation of relevant DSA provisions by influencing the standards for adequate risk mitigation measures based on the above index. As was mentioned above, very large online platforms are under obligation to mitigate systemic risks stemming from the design or functioning of their service and its related systems.⁸⁷ Such risks include “any actual or foreseeable negative effects for the exercise of fundamental rights,”⁸⁸ which covers the right to an effective remedy and to a fair trial. Content moderation features both as a factor to be taken into consideration in risk assessment⁸⁹ and as the object of risk mitigation measures.⁹⁰
- 41 Commission may provide guidelines on measures relating to specific risks⁹¹ and adopt delegated acts laying down the necessary rules for the performance of the annual audits by independent organisations, which assess among other things compliance with due diligence obligations, including operation of the internal redress mechanism.⁹² The Board is expected

to identify best practices for risk mitigation in its yearly reports.⁹³ Ideally, the concerted efforts of Commission, DSC and the Board should be directed toward creating an index of parameters that will be used to assess the adequacy of the mechanisms.

F. Conclusion

- 42 To summarize the above findings, although proceduralization as a legitimizing strategy in platform governance has its merits, it addresses only one facet of legitimacy — legality, neglecting legitimacy in the sociological sense. This deficit can be mitigated by a complementary legitimation strategy, namely through incorporating empirically derived values of procedural justice into the mechanisms mandated by the CDSM and DSA. To facilitate this integration, an index outlining procedural justice values pertinent to users should be developed. While this paper has provided a preliminary framework of such values within the context of content moderation, further research is warranted, as these values were derived from studies with slightly different objectives.
- 43 In conclusion, the paper has provided an analysis of content moderation proceduralization and outlined potential future directions. The hope is that this exploration contributes to the ongoing discourse on the regulation of online platforms and the advancement of effective governance strategies.

⁸⁶ An independent advisory group of Digital Services Coordinators on the supervision of providers of intermediary services. Its tasks are contributing to the consistent application of DSA, coordinating and contributing to guidelines and analysis of the Commission and Digital Services Coordinators and other competent authorities and assisting the Digital Services Coordinators and the Commission in the supervision of very large online platforms. See Article 61 DSA.

⁸⁷ Articles 34 and 35 DSA.

⁸⁸ Article 34(1)(b) DSA.

⁸⁹ Article 34(2)(b) DSA.

⁹⁰ Article 35(1)(c) DSA.

⁹¹ Article 35(3) DSA.

⁹² Article 37(7) DSA.

⁹³ Article 35(2)(b) DSA.

To what extent can online service providers adopt voluntary content moderation measures without losing their immunity shields?

A comparative analysis of online service providers' liabilities in the European Union and the United States

by **Adriana Berbec** *

Abstract: Immunity for engaging in voluntary content moderation measures is a new addition to the European Union legal framework for intermediaries' liabilities. Article 7 of the Digital Services Act guarantees eligibility for immunity to online service providers undertaking good faith voluntary own-initiative investigations similar to the Good Samaritan provision originating in Section 230 of the US Communication Decency Act. The latter has been in place for more than two decades and the breadth of US case law sheds some insights into the strengths and weakness of this provision. This research paper aims to identify similarities and differences between the rules that protect online Good Samaritans in both jurisdictions and determine whether the rules effectively

fight illegal content online without undermining the immunity of online service providers. It does so by looking at the relevant jurisprudence and the existing legal provisions on liability exemptions for voluntary content moderation in both jurisdictions. It further examines the proposals to amend Section 230 in the US which are a symptom of the dissatisfaction surrounding the broad immunity granted to online service providers and the perceived, occasionally misconstrued, shortcomings of the provision. Additionally, they provide indications as to whether limiting the immunity shields to online service providers engaging in voluntary content moderation measures aligns with the standards of good faith and diligence set forth in the Digital Services Act.

Keywords: Content Moderation, Digital Services Act, Section 230, Liability, Online Platforms

© 2024 Adriana Berbec

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Adriana Berbec, To what extent can online service providers adopt voluntary content moderation measures without losing their immunity shields? A comparative analysis of online service providers' liabilities in the European Union and the United States, 15 (2024) JIPITEC 13 para 1.

A. Introduction

1 In both the European Union ("EU") and the United States ("US"), the rules on liability exemptions are meant to protect online service providers undertaking voluntary content moderation measures to remove or disable access to illegal or objectionable content. In the EU, Article 7 of the Digital Services Act (DSA)¹ guarantees that online service providers

do not lose their eligibility for liability exemptions when they carry out, in good faith and in a diligent manner, voluntary own-initiative investigations to

article are those of the author and do not necessarily reflect the official opinion of the author's employer.

1 Regulation of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (the "Digital Services Act") (DSA).

* Adriana Berbec holds an LL.M. in IP and ICT Law from KU Leuven, Belgium. The information and views set out in this

remove or disable access to illegal content. Their exemption from liability is however conditioned by the requirement that the service provider expeditiously removes illegal content once they acquire knowledge or awareness of it. In the US, Section 230(c)(2) of the US Communications Decency Act (CDA)², also known as the Good Samaritan provision, is meant to promote good faith voluntary content moderation measures by protecting online service providers for any action undertaken to remove content that the provider or user of an interactive computer service deems objectionable. Their exemption from liability is not conditioned by promptly removing objectionable content once they acquire knowledge about it. The provisions in both jurisdictions nevertheless share the common element of acting in good faith when undertaking voluntary content moderation measures. The DSA is more detailed and explicit about what constitutes good faith. Section 230 does not provide a statutory definition of what constitutes good faith, but US Courts have generally interpreted the term based on what it does not constitute acting in good faith. The ambiguity of what constitutes objectionable content has also led to interpreting the term either as being an objective standard or a subjective one. In addition, the removal decisions of online service providers have been afforded immunity also under Section 230(c)(1) of the CDA which is meant to protect online service providers from publishing third-party content. This broad interpretation has raised criticism since Section 230(c)(1) does not provide for a good faith covenant, nor does it apply to a certain type of content, such as content similar to pornography, violence, obscenity or harassment outlined in Section 230(c)(2). Several proposals and legislative developments to amend Section 230(c)(2) in the US have therefore emerged that would make the immunity of service providers contingent upon specific safeguards or conditions when they engage in content moderation. One proposal aims that immunity for removal decisions should be available only under Section 230(c)(2), while others suggest a more precise definition of what constitutes good faith and objectionable content.

- 2 The aim of this paper is to undertake a comparative analysis between the voluntary content moderation measures outlined in Article 7 of the EU DSA and Section 230(c)(2) of the US CDA. There are several reasons for choosing to compare these two jurisdictions. First, they have both contributed to the existing legal framework on service provider liabilities either through statutory laws or jurisprudence. Second, the EU service provider

liability exemptions have been influenced by the US system of knowledge-based liability doctrine of the US Digital Millennium Copyright Act (DMCA).³ Third, the voluntary content moderation measures, known as the Good Samaritan principle, originate from Section 230(c)(2). Finally, the DSA addresses all major online service providers, the majority of which are US-based companies that offer their services to EU users. The ultimate goal is to assess whether the legal provisions in both jurisdictions manage to achieve their desired objective of fighting illegal content online while preserving the immunity status of online service providers. It does so by examining the legislative framework governing the online service provider liabilities in the EU and the US, in particular the rules on voluntary content moderation measures in the DSA and Section 230.

- 3 This research paper is structured as follows. Chapter A serves as an introduction. Chapter B provides the regulatory framework for online service providers liability in both the EU and the US. Chapter C examines the jurisprudence from the EU Court of Justice ("CJEU") and of the US Courts with regards to liability exemptions and voluntary content moderation measures. Chapter D analyses the recent proposals to modify the Good Samaritan provision in the US, the objective being to determine the perceived weaknesses of Section 230(c) and the solutions to tackle them. Chapter E concludes the findings of the research and provides some general reflections in relation to the interplay between voluntary content moderation measures and liability shields.

B. Regulatory framework for online service providers liability

- 4 This chapter describes the framework directive governing electronic commerce in the EU which, *inter alia*, regulates intermediary liability. It will touch upon the transition of intermediary liability regime from a directive to a regulation, by analysing the similarities and differences between the relevant legal provisions in the directive and the regulation. Similarly, the chapter explores the main legislation that governs intermediary liability in the US, along with the sequential steps that have led to the creation of Section 230. Subsequently, the chapter will examine the voluntary content moderation measures outlined in the DSA and in Section 230(c)(2), known as the Good Samaritan provision.

² Communications Decency Act (CDA), also called Title V of the Telecommunications Act of 1996, enacted by the US Congress primarily in response to concerns about minors' access to pornography via the Internet.

³ Digital Millennium Copyright Act of 1998 (DMCA), < <https://www.copyright.gov/dmca/> >, accessed 16 March 2024.

I. European Union

5 At the EU level, Directive 2000/31/EC on electronic commerce (hereby ‘the Directive’), is the legislation that regulates central legal aspects of electronic commerce, including online communications, online contracts, and intermediary liability.⁴ Its objective is to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between Member States.

6 Section 4 of the Directive lays down intermediaries’ liabilities exemptions for all the unlawful activities carried out by third parties, subject to conditions as laid down in Article 12 (*mere conduit*)⁵, Article 13 (*caching*)⁶ and Article 14 (*hosting*).^{7,8} Among these three provisions, Article 14 is the most important one as it basically reflects the knowledge-based liability principle, and it applies to providers that host third-party content on their servers. The Directive clarifies that the liability exemptions in the Directive

apply to intermediary service providers when their activity “is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored”.⁹ According to the Directive, the passive nature of the provider is commensurate with a lack of knowledge or control over the content. This passive nature of the service provider guarantees its liability exemptions.

7 More than two decades after the adoption of the Directive, the European Commission (the ‘Commission’), in light of the “new and innovative business models ...[that] have allowed business users and consumers to impart and access information and engage in transactions in novel ways”¹⁰, proposed a new Regulation on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act), shortly known as the DSA. The DSA entered into force on 16 November 2022. The DSA maintains the liability regime in the Directive, but it introduces transparency requirements and due diligence obligations proportionate to the size of the intermediary service provider. The DSA also includes online search engines and online platforms which were left out in the Directive. Online platforms are defined as a sub-category of internet intermediaries that provide a digital hosting service at the request of a recipient of the service.¹¹ The hosting service includes the storing, but also the dissemination of information to the public, unless that activity is a minor and purely ancillary feature of another service or a minor functionality of the principal service.

8 The liability exemptions contained in Articles 12 to 14 of the Directive are now construed as references to Articles 4, 5, and 6 of the DSA. Likewise, the DSA also maintains the provision on the prohibition for general monitoring in Article 15 of the Directive, now construed as reference to Article 8 DSA.

9 Pursuant to Article 6 of the DSA (former Article 14 of the Directive), a (hosting) service provider is exempt from liability of third-party illegal content if it “does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent” (Article 6(1)a), or “upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content” (Article 6(1)b).¹² Illegal content is defined as information relating to illegal content, products,

4 Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Recital 7.

5 *Ibid.*, Article 12, according to which a service provider is not liable for the information transmitted or accessed if it “does not initiate the transmission; does not select the receiver of the transmission; and does not select or modify the information contained in the transmission”.

6 *Ibid.*, Article 13, according to which a service provider is not liable for the automatic, intermediate and temporary storage of information if it “does not modify the information; complies with conditions on access to the information; complies with rules regarding the updating of the information [...]; does not interfere with the lawful use of technology [...] to obtain data on the use of the information; and acts expeditiously to remove or to disable access to the information upon obtaining actual knowledge of the fact that the information at the initial source of the transmission’ has been removed or disabled”.

7 *Ibid.*, Article 14, according to which a service provider is not liable for the information transmitted or accessed on the condition that “(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information”.

8 For each of Articles 12, 13, and 14, even if no liability is established, national courts and administrative authorities can require the service provider to terminate or prevent an infringement or to remove or disable access to illegal information respectively, in accordance with the law of the Member State.

9 Directive 2000/31/EC, Recital 42.

10 DSA, Recital 1.

11 *Ibid.*, Article 3(i).

12 *Ibid.*, Article 6(1).

services, and activities¹³ that are not in compliance with the law of the Union or of any Member State.¹⁴

- 10 According to Article 6(2) of the DSA, Article 6(1) does not “*apply when the recipient of the service is acting under the authority or control of the provider*”.¹⁵ The DSA goes a bit further than the Directive and introduces Article 6(3) to indicate that Article 6(1) does not apply with respect to liability under consumer protection law of online platforms that allow customers to conclude distance contracts with traders, if the online platform leads an average consumer to believe that the product or service is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.

1. Voluntary content moderation measures under the DSA

- 11 Article 7 of the DSA, entitled “Voluntary own-initiative investigations and legal compliance” fills in a gap in the Directive¹⁶ by introducing a provision relating to liability exemptions for intermediary service providers engaging in voluntary own-initiative investigations. An ‘intermediary service’ is defined as an information society service that provides either a ‘mere conduit’, ‘caching’, or ‘hosting’ service.¹⁷ For ease of comparison with the immunity of interactive computer service providers in Section 230, ‘intermediary service providers’ will be referred to as ‘online service providers’.
- 12 The concept of extending protections to online service providers engaging in voluntary pro-active measures dates back to 2017, when the Commission considered the option of introducing a Good Samaritan provision aimed at encouraging service providers to tackle illegal content (“*proactive steps to detect, remove or disable access to illegal content (the so-called “Good Samaritan” actions)*”).¹⁸ This is now

reflected in Article 7 of the DSA which holds that online service providers shall not lose the liability shields referred to in Articles 4, 5 and 6 of the DSA *solely* because they “*in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content*”.¹⁹ Article 7 further aims at reassuring online service providers that any measures undertaken to comply with the requirements in the DSA (such as the due diligence obligations) do not lead to unavailability of the exemptions²⁰ due to categorizing such actions as ‘active’ involvement.²¹ Unlike own-initiative investigations which are voluntarily initiated by online service providers and are meant to promote self-regulation, the measures undertaken for legal compliance pertain to mandatory (due diligence) obligations that online service providers must fulfill. To maintain the focus of the comparative analysis with the liability regime applicable under US Section 230(c)(2) concerning Good Samaritan voluntary content moderation measures, this research paper will center on the liability exemptions available for voluntary own-initiative investigations to remove or disable access to illegal content (from now on ‘voluntary content moderation measures’).

2. Knowledge and take-down

- 13 According to the DSA, liability exemptions for voluntary content moderation measures are subject to several conditions. First, pursuant to Article 6 of the DSA, liability exemptions are conditional upon online service providers (i) lacking actual knowledge of the illegal content or awareness of facts or circumstances from which the illegal activity or illegal content is apparent (Article 6(1)(a)), or (ii) acting expeditiously to remove illegal content once they obtain actual knowledge or awareness of the illegal content (Article 6(1)(b)). Since knowledge and awareness can be acquired not only through notices submitted by third parties, but also through own-initiative investigations,²² online service providers can avoid liability if they act expeditiously to remove

13 *Ibid.*, Recital 12.

14 *Ibid.*, Article 3(h).

15 *Ibid.*, Article 6(2).

16 Directive 2000/31/EC only specifies in Recital 48 that the Directive does not prevent Member States to request hosting providers to apply a duty of care to detect illegal activities.

17 *Ibid.*, Article 3(g).

18 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Tackling

Illegal Content Online, Towards an enhanced responsibility of online service providers COM(2017) 555.

19 DSA, Article 7.

20 *Ibid.*, Article 7 (“to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation”).

21 Communication from the Commission COM(2017) 555, *supra* note 18.

22 *Ibid.*, Recital 22.

or disable access to the illegal content²³ in line with Article 6(1)(b) also when engaging in voluntary content moderation. This has been acknowledged by the Commission in its Communication and later on, its Recommendation on tackling illegal content online.²⁴ More specifically, the Commission explained that taking such voluntary proactive measures “does not automatically lead to the online service provider losing the benefit of the liability exemption provided for in Article 14 of Directive”.²⁵ This is due to the fact that acting expeditiously to remove or disable access to illegal content the online service providers continue to “benefit from the liability exemption pursuant to point (b) of Article 14(1) [of the Directive]”.²⁶ Accordingly, when online service providers undertake voluntary content moderation measures to remove content whose illegality is apparent²⁷ their acquired knowledge and awareness of that specific illegal content does not automatically render them liable. Online service providers lose their liability exemptions only if they fail to expeditiously remove the specific content whose illegality is obvious.²⁸ Similarly, the mere fact that online service providers undertake such voluntary measures does not make them active providers in respect of the illegal content posted on their servers²⁹ as interpreted in Recital 18 of the

DSA. This is also the view expressed by the Advocate General in *YouTube and Cyando*.³⁰

- 14 To better understand the rules on liability exemptions, a reading of the Recitals of the DSA is necessary. Although the Recitals are not legally binding, they play an important role in the decisions of the CJEU as they help with the interpretation of the operative provisions of the Regulation.
- 15 Thus, Recital 18 clarifies that liability exemptions are available as long as the service providers confine themselves to “providing the services neutrally by a merely technical and automatic processing of the information” and do not play “an active role of such a kind as to give it knowledge of, or control over, that information”.³¹ This Recital rephrases the liability exemptions in the Directive, by focusing on the active nature of the service provider that removes the liability exemptions as opposed to the passive nature of the service provider that guarantees the liability exemptions in the Directive. Neutrality, as the Recital reads, is correlated with knowledge and an online service provider which acquires knowledge of illegal content can still benefit from liability exemptions provided it expeditiously removes that specific content in line with Article 6 of the DSA.
- 16 Recital 22 provides further insights into the interplay between liability exemptions and knowledge of illegal content. Therefore, the fact that an online service provider automatically indexes information, has a search function, or recommends information based on profiles or preferences is not sufficient to conclude it has a ‘specific’ knowledge of the illegal content. Nor would an online service provider become knowledgeable solely by being aware, in a general sense, that its service is also used to store illegal content.³² In other words, being aware that online service providers, although designed to be used for legal purposes, are inevitably used by third parties also for illegal purposes, does not lead to

23 Joan Barata, ‘Positive Intent Protections: Incorporating a Good Samaritan principle in the EU Digital Services Act’ (2020), Centre for Technology and Democracy, <<https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf>>, accessed 16 March 2024.

24 Communication from the Commission COM(2017) 555, *supra* note 18, section 3.3. See also Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, C(2018)1177.

25 *Ibid.*

26 *Ibid.*

27 DSA, Article 6 (“does not have knowledge [...] or is not aware of facts or circumstances from which the illegal activity or the illegal content is apparent”).

28 See also Domingos Fahrino, ‘The Digital Services Act: A European Digital Republic, If We Can Keep It Or The Long And Winding Road’ (*The Digital Constitutionalist*, 7 December 2022) (“by having content moderation, service providers, especially hosting ones, do not waiver the exemptions of liability they are given, but, if in the course of moderating content, illegal one is found or made apparent (see article 6(1)(a) and (b)) than the service provider is liable for such content if it does not act to counter it.”), <<https://digi-con.org/the-digital-services-act-a-european-digital-republic-if-we-can-keep-it-or-the-long-and-winding-road/>>, accessed 16 March 2024.

29 Communication from the Commission, COM(2017) 555,

supra note 18.

30 Opinion of Advocate General Saugmandsgaard Øe delivered on 16 July 2020 in *Frank Peterson v Google LLC and Elsevier Inc. v Cyando AG*, Joined Cases C682/18 and C683/18 (*‘YouTube and Cyando’*), para. 166 (“it is necessary to avoid an interpretation of the concept of ‘active role’ that could produce the paradoxical result whereby a service provider conducting research on its own initiative into the information which it stores[...], would lose the benefit of the exemption from liability laid down in Article 14(1) of that directive and would, therefore be treated more severely than a provider which does not”).

31 DSA, Recital 18.

32 *Ibid.*, Recital 22.

knowledge-based liability.³³

- 17 Recital 26 further confirms that such measures “should not be taken into account when determining whether the provider can rely on an exemption from liability, in particular as regards whether the provider offers its service neutrally [...] without this rule implying that the provider can necessarily rely thereon”.³⁴ In other words, undertaking voluntary content moderation measures should not be taken into account to determine whether the online service provider can claim or invoke an exemption from liability,³⁵ in particular for determining that the online service provider offers its services neutrally. The rule does not mean that the online service providers can necessarily invoke an exemption from liability.³⁶ The only thing that these voluntary measures guarantee is that the online service providers can invoke eligibility for liability exemptions (“shall not be deemed ineligible”³⁷). Whether the online service provider is exempted from liability depends on whether the service provider satisfies the conditions for liability exemptions in Article 6 of the DSA. Kuczerawy explained that “taking voluntary actions in good faith neither guarantees nor precludes neutrality” and that the online platforms may still lose immunity.³⁸

3. Good faith and diligence

- 18 Second, pursuant to Article 7 of the DSA, online service providers do not lose their eligibility for liability exemptions referred to in Articles 4, 5

and 6 of the Regulation, “solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content”.³⁹ Recital 26 provides more clarity by indicating that the mere undertaking of voluntary measures does not render the liability exemptions unavailable on the condition that these measures are taken in good faith and in a diligent manner. These conditions include “acting in an objective, non-discriminatory and proportionate manner, with due regards to the rights and legitimate interest of all parties involved, and providing the necessary safeguards against unjustified removal of legal content”.⁴⁰ To that aim, where automated tools are used, the technology used must be sufficiently reliable “to limit to the maximum extent possible the rate of errors”.⁴¹

- 19 It can be inferred from this Recital that acting in good faith means acting in an objective, non-discriminatory and proportionate manner, while duly considering the rights and legitimate interests of all the parties involved.⁴² This interpretation is reinforced by the Directive on Unfair Terms in Consumer Contracts (‘UCTD’) which provides that the seller or the supplier can meet the good faith requirement by dealing “fairly and equitably with the other party whose legitimate interests he has to take into account”.⁴³ It is worth noting that ‘fairly’ and ‘equitably’ are synonyms of ‘objective’, ‘non-discriminatory’ and ‘proportionate’ and that the UCTD, just like the Recital 26 of the DSA, specifically requires that the legitimate interests (of the other party) must be taken into account when acting in good faith. The Commission Notice on the interpretation of UCTD also confirms that “good faith is an objective concept linked to the question of whether [...] the contract term in question is compatible with fair and equitable market practices that take the consumer’s

33 By analogy with the safe harbours in DMCA, see for instance Emerald Smith, ‘Lord of the Files: International Secondary Liability for Internet Service Providers’ (2011) in 68(3) Wash. & L.L. Rev. (“The court interpreted the DMCA placing the burden of policing content on copyright owners as logical given that the service platforms in question contain both infringing and non-infringing works and submission methods can make it difficult to determine which is which”), <<https://scholarlycommons.law.wlu.edu/wlulr/vol68/iss3/24>>, accessed 16 March 2024.

34 DSA, Recital 26.

35 In French: « si ledit fournisseur peut se prévaloir d’une exemption de responsabilité », DSA, Recital 26.

36 In French: « [...]cette règle n’impliquant cependant pas que ledit fournisseur peut nécessairement se prévaloir d’une exemption de responsabilité », DSA, Recital 26.

37 DSA, Article 7.

38 Aleksandra Kuczerawy, ‘The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act’ (Verfassungsblog, 12 January 2021), <<https://verfassungsblog.de/good-samaritan-dsa/>>, accessed 16 March 2024.

39 DSA, Article 7.

40 Ibid., Recital 26.

41 Ibid.

42 See also Jacob van de Kerkhof, ‘Good Faith in Article 6 Digital Services Act (Good Samaritan Exemption)’ (The Digital Constitutionalist, 15 February 2023) (“the components of good faith in Recital 26 are objectivity, non-discrimination, proportionality, due regard of rights and interests of users and necessary safeguards in place to ensure automated technologies are sufficiently reliable”), <<https://digi-con.org/good-faith-in-article-6-digital-services-act-good-samaritan-exemption/>>, accessed 16 March 2024.

43 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, No L 95/30, Recital 16.

legitimate interests sufficiently into account".⁴⁴

- 20 Recital 26 does not distinctly separate acting in good faith from acting diligently, and while the two standards may overlap,⁴⁵ a diligent operator must also remove content when its illegal character is manifestly evident.⁴⁶ The statement of the Advocate General Saugmandsgaard Øe in the *YouTube and Cyando* judgment accurately conveys this concept by explaining that "a provider must remove such information only where its illegal nature is 'apparent', that is to say manifest".⁴⁷ This judgment aligns with the principles outlined in Recital 53 of the DSA pursuant to which the illegal character of the content can be considered apparent, when a third-party notice contains sufficient information to enable a diligent operator to establish that character "without a detailed legal examination".⁴⁸ The service provider is required to diligently assess the facts brought to its attention concerning specific illegal information⁴⁹ and to address it.⁵⁰ The requirement for a diligent online service provider to remove the content which, based on a notice from third-party, appears sufficiently illegal is likely to be applicable in relation to own-initiative investigations also.⁵¹

- 21 Exercising diligence in the context of voluntary content moderation measures does not come

44 Commission notice-Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, (2019/C 323/04), sub-paragraph 3.4.1.

45 See Guidance on the Implementation/Application of the Directive 2005/29/EC on Unfair Commercial Practices, COM(2016) 320 final ("The notion of 'professional diligence' encompasses principles which were already well-established in the laws of the Member States before the adoption of the UCPD, such as 'honest market practice', 'good faith' and 'good market practice'. These principles emphasise normative values that apply in the specific field of business activity"), pages 50-51.

46 DSA, Recitals 22 and Recital 53.

47 AG Opinion in *YouTube and Cyando*, *supra* note 30, para. 187.

48 DSA, Recital 53. See also Judgment of 22 June 2021, *YouTube and Cyando*, para.116.

49 AG Opinion in *YouTube and Cyando*, *supra* note 30, para.185.

50 *Ibid.*, para.194 ("Removing information requires the service provider to react (diligently) to a notification").

51 Folkert Wilman, 'Between preservation and clarification, the evolution of the DSA's liability rules in light of the CJEU's case law' (citing *YouTube* judgment), (*Verfassungsblog*, 2 November 2022) <<https://verfassungsblog.de/dsa-preservation-clarification/>>, accessed 16 March 2023.

without challenges. In particular, questions have been raised about how to measure whether an online service provider acted diligently when failing to remove some but not all illegal content.⁵² For instance, consider a scenario where the same illegal content is shared on two different platforms. If one platform identifies it and removes it, while the other overlooks it and fails to remove it,⁵³ such instances of unsuccessful content moderation could be considered as not undertaken in a diligent manner.⁵⁴ There can be two consequences. Either the number of online service providers that will remove illegal content will diminish⁵⁵ fearing potential liability for incomplete removal, or the online service providers will exercise excessive removal (including unjustified removal of legal content)⁵⁶ to avoid liability. The DSA strives to achieve a balance between encouraging the removal of content whose illegality is apparent⁵⁷ (without losing the liability exemptions)⁵⁸ and applying safeguards to prevent the arbitrary removal of legal content.⁵⁹

- 22 On the other hand, raising the bar too high for

52 See also Kuczerawy, *supra* note 38 ("Could unsuccessful voluntary actions be considered as not undertaken in a "diligent manner"? Could it actually discourage hosts from taking one-time voluntary decisions in particular cases if no coherent framework for 'diligence' is in place?").

53 This example is based on a similar example provided by Aleksandra Kuczerawy, *supra* note 38 ("if a moderator trained to review for one type illegality (e.g. incitement to violence) looked at a video, but failed to recognize that it contained another type (e.g. defamation)").

54 *Ibid.*

55 Jan M. Smits, discussing good Samaritan's liability for non-rescue, 'The good Samaritan in European private law: on the perils of principles without a programme and a programme for the future' (2000), <<https://doi.org/10.26481/spe.20000519js>>, accessed 16 March 2024.

56 See also Wilman, *supra* note 51. ("Even when sincerely meant to tackle illegal content, they [the measures] can cause considerable damage if not enacted diligently. For instance, the large-scale removal of content that is wrongly considered illegal comes to mind").

57 See also *infra* note 64 and the accompanying text.

58 See DSA, Recital 22. A diligent operator who becomes aware (through own-initiative investigations or third-party notices) of content whose character is clearly illegal can continue to benefit from the exemptions from liability if it takes immediate action to address it.

59 See *supra* notes 40 and 41 and *infra* notes 66 and 67 and the accompanying text.

Article 7 of the DSA would (i) defeat its own purpose⁶⁰ and (ii) would be contrary to Article 8 of the DSA which prohibits a general monitoring obligation. First, the objective of introducing Article 7 is to encourage online service providers to moderate content without fear of losing the liability exemptions. Requiring absolute accuracy in moderating content would discourage them from doing so and would be contrary to the objective of introducing such provision. Second, as explained in Recital 30 of the DSA, “*nothing in this Regulation should be construed [...] as a general obligation for providers to take proactive measures in relation to illegal content*”.⁶¹ More importantly, it confirms that online service providers should not be, neither *de jure* or *de facto*, subject to a monitoring obligation except in a specific case or when faced with an injunction, as interpreted by the CJEU.⁶² In that respect, it addresses the concerns raised on how to reconcile the prohibition on general monitoring with proactive measures and how to distinguish between general and specific monitoring obligations.⁶³

- 23 Notwithstanding these opposing approaches, it is worth noting that failing to remove content equates to leaving content up or continuing to host third-party illegal content. Article 6 of the DSA exempts online service providers from liability for hosting or leaving up illegal third-party content provided that they do not have knowledge of the content whose illegality is apparent⁶⁴ or upon obtaining knowledge, they expeditiously remove or disable access to that content. The natural train of thought would lead us to conclude that the apparent illegality makes the online service provider knowledgeable which in return allows it to remove that content, thereby acting diligently. Knowledge, which stems from apparent illegality, is necessary to allow good faith

and diligent content moderation. In fact, Article 7 applies to online service providers that remove in good faith third-party content they *know* it is illegal, while Article 6(a) applies to online service providers that *unknowingly* host third-party illegal content.

4. Fundamental rights

- 24 Third, pursuant to Recital 22 of the DSA, liability exemptions for voluntary content moderation measures are conditional upon online service providers acting “*in the observance of the fundamental rights of the recipients of the service, including the right to freedom of expression and of information*”⁶⁵ when they expeditiously remove illegal content upon obtaining actual knowledge. The intention here is that online service providers “*avoid that removal and disabling measures affect legal and protected speech*”⁶⁶ and a balance is achieved between fighting illegal content and users’ rights to freedom of expression and information.⁶⁷ The protection of freedom of expression and of information is further reinforced by the transparency requirements in Article 15 of the DSA according to which online service providers should make publicly available reports which include meaningful and comprehensible information about the content moderation engaged in at their own initiative.⁶⁸

II. United States

- 25 In the US, Section 230 of the CDA provides limited federal immunity⁶⁹ to providers and users of interactive computer service,⁷⁰ protecting them from

⁶⁰ Wilman, *supra* note 51.

⁶¹ See also Cases C70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* (2011) and C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (2012), where an injunction would require the service provider to carry out a general monitoring obligation contrary to Article 15 of the Directive.

⁶² DSA, Recital 30.

⁶³ See for instance Thomas Riis and Sebastian Felix Schwemer, ‘Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation’, University of Copenhagen Faculty of Law Legal Studies Research Paper Series, paper no. 2019-64.

⁶⁴ DSA, Article 6 (“*does not have knowledge [...] or is not aware of facts or circumstances from which the illegal activity or the illegal content is apparent*”).

⁶⁵ *Ibid.*, Recital 22.

⁶⁶ Joan Barata, ‘Digital Services Act and the Protection of Fundamental Freedoms-Recommendations for the dialogue process’, (*Digital Services Act Observatory*, 11 April 2022), <<https://dsa-observatory.eu/2022/04/11/digital-services-act-and-the-protection-of-fundamental-freedoms-recommendations-for-the-trilogue-process/>>, accessed 16 March 2024.

⁶⁷ See also *You Tube and Cyando*, para. 116.

⁶⁸ DSA, Article 15(c) and Recital 66.

⁶⁹ It does not apply to federal criminal law, intellectual property law, any state law “consistent” with Section 230, certain privacy laws applicable to electronic communications, or certain federal and state laws relating to sex trafficking.

⁷⁰ Interactive computer service means “any information service, system, or access software provider that provides or enables

liability for content provided by third parties. The CDA, part of the Telecommunications Act of 1996, originally endeavoured to protect children from indecency and obscene material online.⁷¹ However, the Supreme Court of the US (SCOTUS)⁷² struck down the CDA almost entirely for being unconstitutional and violating the First Amendment⁷³ on freedom of speech.⁷⁴ Section 230, which was introduced as a free-standing bill⁷⁵ that promoted speech online while encouraging moderation and removal of obscene content,⁷⁶ was allowed to stand. Section 230 contains two different immunities listed under Section 230(c) under the title ‘Protection of “Good Samaritan” blocking and screening of offensive material’. The first one is Section 230(c)(1) on ‘treatment of publisher or speaker’ and the second one is Section 230(c)(2) on ‘civil liability’.

- 26 To understand how Section 230 emerged and was eventually enacted, it is useful to look at the influence of the two court cases, *Cubby, Inc. v. CompuServe, Inc.*⁷⁷ (‘Cubby’) and *Stratton Oakmont, Inc. v. Prodigy Services Co.*⁷⁸ (‘Stratton Oakmont’). These cases dealt with the

computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions” (47 U.S.C. Section 230 (f)(2)).

- 71 Emine Ozge Yildirim, ‘CDA §230: The Section Behind the Internet Boom’, Georgetown University Law Center, (2017).
- 72 SCOTUS is the highest court in the federal judiciary of the United States. It has ultimate appellate jurisdiction over all federal court cases, and over state court cases that involve a point of U.S. Constitutional or federal law. Source: Wikipedia.
- 73 The First Amendment protects freedom of speech, the press, assembly, and the right to petition the Government for a redress of grievances, < <https://www.whitehouse.gov/about-the-white-house/our-government/the-constitution/>>, accessed 16 March 2024.
- 74 *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
- 75 Christopher Cox (Former United States Representative and co-author of Section 230), ‘Section 230: A Retrospective’ (*The Center for Growth and Opportunity at Utah State University*, 10 November 2022), <<https://www.thecgo.org/research/section-230-a-retrospective/>>, accessed 16 March 2024.
- 76 Jason Kelley, ‘Section 230 is Good, Actually’, (*Electronic Frontier Foundation*, 3 December 2020) <<https://www.eff.org/deeplinks/2020/12/section-230-good-actually>>, accessed 16 March 2024.
- 77 *Cubby, Inc. v. CompuServe Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).
- 78 *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710

issue of whether interactive computer service providers (from now on ‘online service providers’) could be held liable for defamatory third-party content hosted on their servers.⁷⁹

- 27 In *Cubby*, the online service provider was considered merely a distributor, rather than a publisher of that information and therefore was not held liable for content hosted on its server. The defendant, CompuServe was the owner of an electronic library consisting of different interest forums, one of which was Rumorville, a daily newsletter that was reporting on broadcast journalism.⁸⁰ Rumorville was sued for defamation by Cubby who asserted that CompuServe should be held liable as a publisher of the content posted by Rumorville. The Southern District Court of New York disagreed and held that CompuServe would only be liable if it had knowledge of such defamatory content, therefore creating a notice and take down standard for defamation cases.⁸¹
- 28 In *Stratton Oakmont*, the online service provider was considered a publisher because it exercised editorial control, including by removing offensive content from its bulletin boards. It was therefore held liable for content hosted on its server. In reaching that conclusion, the SCOTUS held that Prodigy maintained control over the content by means of an automatic screening program in accordance with company guidelines that ‘board leaders’ were required to enforce.⁸² Prodigy explained that it did not screen material on the bulletin boards, but rather screened and blocked postings containing ‘the seven dirty words’ and their equivalents in major languages (the so-called ‘George Carlin screener’).⁸³ Consequently, some postings, such as calling “someone a piece of a

(N.Y. Sup. Ct. 1995).

- 79 Electronic Frontier Foundation, Section 230 Legislative History <[1 jipitec](https://www.eff.org/issues/cda230/legislative-history#:~:text=Cubby%20and%20Stratton%20Oakmont&text=v.,be%20held%20responsible%20for%20it.>”, accessed 16 March 2024.</p>
<p>80 Josh Slovin, ‘Section 230 of the Communications Decency Act: The “Good Samaritan” Law which Grants Immunity to “Bad Samaritans”’ (2022) in 73(2) Mercer Law Review.</p>
<p>81 Eric Goldman, ‘An Overview of the United States’ Section 230 Internet Immunity’, in Giancarlo Frosio (ed) <i>Oxford Handbook of Online Intermediary Liability</i> (OUP 2020).</p>
<p>82 Marc Jacobson, (Vice President, General Counsel for Prodigy), ‘Prodigy: It May Be Many Things To Many People, But It Is Not A Publisher For Purposes Of Libel, And Other Opinions’ (1996), 3(11) Journal of Civil Rights and Economic Development.</p>
<p>83 <i>Ibid.</i></p>
</div>
<div data-bbox=)

Shitake mushroom” were not screened due to being separate words.⁸⁴ The Court eventually held that by actively deleting notes from its bulletin boards on the basis of ‘offensiveness’ and ‘bad taste’, Prodigy exercised editorial control over the content and was therefore considered a publisher.⁸⁵ The Court drew a distinction between *Stratton Oakmont* and *Cubby* emphasising that CompuServe, unlike Prodigy, lacked the opportunity to monitor information on its website.

29 The *Stratton Oakmont* decision led to what is now known as ‘the moderator’s dilemma’, pushing online service providers to choose between removing content (and potentially being treated as publishers and held liable for third-party content) and not removing content and thereby avoiding liability.⁸⁶ To address this issue, Section 230(c) was introduced as an amendment to the CDA and overruled *Stratton Oakmont* by establishing two key rules.⁸⁷

30 The first one, Section 230(c)(1), specifies that a provider or user of an interactive computer service may not be treated as publisher or speaker of any content provided by another information content provider.⁸⁸ Section 230 defines the information content provider as “any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service”.⁸⁹ When interpreting Section 230(c)(1), Courts employ either (i) a presumption standard, or (ii) a three-part test.⁹⁰ Under the presumption standard, a service provider incurs no liability for third-party content unless it actively contributes to the development of the content.⁹¹ The test for determining whether

an online service provider benefits from liability protection under Section 230(c)(1) “is whether the service provider developed the content that is the basis for liability”.⁹² If it is found not to be a publisher, it can lead to online service providers being offered protection in situations where they negligently fail^{93,94} or chose not to remove content from their websites even upon notification.⁹⁵ Under the three-step test (i) the defendant must be a provider or user of an interactive computer service, (ii) the defendant must not be an information content provider, and (iii) the plaintiff’s claims must seek to treat the defendant as a publisher or speaker of the content.⁹⁶

31 The second one, Section 230(c)(2) concerns civil liability, and it consists of two sub-paragraphs. The first sub-paragraph (A) deals with voluntarily removing or restricting access in good faith to objectionable material,⁹⁷ and the second sub-paragraph (B) deals with action taken by online service providers to provide users (or content

84 *Ibid.*

85 Yildirim, o.c.

86 Goldman, o.c. *supra* note 81.

87 Statement of Justice Thomas, Supreme Court of the United States, *Malwarebytes, Inc. v. Enigma Software Group USA, LLC*, On Petition For Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit, 13 October 2020.

88 47 U.S.C., Section 230(c)(1): “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider”.

89 47 U.S.C., Section 230(f)(3).

90 Yaffa A. Meeran, ‘As Justice So Requires: Making the Case for a Limited Reading of § 230 of the Communications Decency Act’ (2018), 86 Geo. Wash. L. Rev. 257, 267.

91 *Ibid.*

92 Congressional Research Service (‘CRS’), ‘Section 230: An Overview,’ (2021).

93 For instance, in *Zeran v. America Online, Inc.*, 129 F.3d 327 (4th Cir. 1997), Zeran brought negligence claims against America Online (AOL) as AOL “had a duty to remove the defamatory posting promptly, to notify its subscribers of the message’s false nature, and to effectively screen future defamatory material”. In *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008), Doe brought negligence claims against MySpace from failing to implement “basic safety measures to prevent sexual predators from communicating with minors on its Web site”.

94 Negligence has been interpreted by US Courts as failure to investigate and remove a defamatory statement. See *Zeran v. AOL o.c.* (“Publication does not only describe the choice by an author to include certain information. In addition, both the negligent communication of a defamatory statement and the failure to remove such a statement when first communicated by another party— each alleged by Zeran here under a negligence label—constitute publication.”). See also Amicus Brief in *Reynaldo Gonzalez, et al., Petitioners v. Google LLC*, No. 21-1333 (“publication is an element of the tort of defamation that encompasses all “communication intentionally or by a negligent act to one other than the person defamed.”).

95 *Zeran v. AOL.*, o.c. (“Liability upon notice would defeat the dual purposes advanced by § 230 of the CDA”).

96 CRS, *supra* note 92, Johnson and Castro, o.c., Meeran, o.c.

97 47 U.S.C., Section 230(c)(2)(A) (“no provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected”).

providers) with technical tools to restrict access to content, described in first sub-paragraph (A).⁹⁸ These tools refer to “*blocking and filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material*”.⁹⁹

- 32 Compared to Section 230(c)(1), Section 230(c)(2)(A) immunity is narrower as it applies only to good-faith content moderation of *certain type* of third-party objectionable content.¹⁰⁰ In contrast, Section 230(c)(1) is broader as it applies to liability for publishing *any* third-party content and the test employed by most Courts¹⁰¹ is whether it has materially contributed to the development of the content. The general rule is that when it comes to litigation, if the service provider shows that it did not act as a speaker or publisher of the content, the Courts will not investigate whether it is immune under Section 230(c)(2)(A). If it is established that the service provider acted as publisher or speaker of the content, it can still enjoy immunity under Section 230(c)(2)(A) if it shows that it took down in good faith third-party content that the provider or the user considered objectionable.¹⁰²
- 33 Even though both sections come under the heading of Good Samaritan principle, only Section 230(c)(2) sub-paragraph (A) (hereafter “Section 230(c)(2)(A)”) would qualify for a Good Samaritan provision.¹⁰³ This is because Section 230(c)(2)(A) requires a voluntary action to restrict access to objectionable material in good faith¹⁰⁴ and therefore a duty of care, whereas Section 230(c)(1) requires *no action*. Additionally, some scholars and Court of Appeals claim that only Section 230(c)(2) confers immunity, being the only

section under the heading “civil liability”.¹⁰⁵

- 34 The primary objective of this research paper is to conduct a comparative analysis between the liability shields afforded to online service providers that engage in voluntary good faith content moderation measures under Section 230(c)(2)(A) and Article 7 of DSA. Nonetheless, since US Courts have read Section 230(c)(1) to apply to removal and content moderation decisions,¹⁰⁶ an analysis of Section 230(c)(1) is necessary.

1. Voluntary content moderation measures under US Section 230

- 35 The Good Samaritan principle reflected in Section 230(c)(2)(A) immunizes interactive computer service providers and users in situations where they voluntarily take any action to remove illegal or objectionable content subject to the good faith safeguard. The provision reads as follows: “no provider or user of an interactive computer service shall be held liable on account of (a) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected;”¹⁰⁷
- 36 A reading of the provision suggest that Section 230(c)(2)(A) has two limitations. Particularly, it requires the finding that the voluntary actions were taken in good faith and that the content removed is objectionable. Neither the term ‘good faith’ nor the term ‘objectionable’ have a statutory definition.
- 37 The US Courts have generally defined good faith in terms of what it is not considered good faith.¹⁰⁸ Other definitions refer to acting in good faith belief that the content requires moderation or making a good faith effort to moderate objectionable content.¹⁰⁹
- 38 While Section 230(c)(2)(A) enumerates a specific type of content that is obscene, lewd, lascivious,

98 47 U.S.C., Section 230(c)(2)(B) (“no provider or user of an interactive computer service shall be held liable on account of any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)”).

99 47 U.S.C., Section 230(b)(4).

100 CRS, *supra* note 92.

101 According to Meeran, *o.c.*, these concern the Fourth, Sixth, and Ninth Circuits. The three-steps test has been employed by the Tenth Circuit in *FTC v. Accusearch*.

102 Ian C. Ballon, ‘The Good Samaritan Exemption-Section 230 of the CDA’, Excerpted from Chapter 37 (Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)) from *E-Commerce and Internet Law: Legal Treatise with Forms*, 2d Edition (2021).

103 Mary Anne Franks, ‘Reforming Section 230 and Platform Liability’, *Stanford Cyber Policy Center* (2021).

104 Ballon, *o.c.*

105 See Shlomo Klapper, ‘Reading Section 230’, *Buffalo Law review*, Volume 70, No.4, (2022), page 1304; See also Meeran, *o.c.*

106 Adam Candeub, ‘Reading Section 230 as Written’, *Journal of Free Speech Law*, <<https://www.journaloffreespeechlaw.org/candeub.pdf>>, accessed 16 March 2024.

107 47 U.S.C., Section 230(c)(2)(A).

108 See *infra* notes 200-202.

109 Klapper, *o.c.*, page 1304.

filthy, excessively violent, and/or harassing, it also mentions content that the provider or user finds ‘otherwise objectionable’. The term ‘otherwise objectionable’ has been interpreted by some Courts either as content similar to the content enumerated before under the principle of *ejusdem generis*¹¹⁰ or as a broad concept¹¹¹ encompassing any content the user or provider finds objectionable.¹¹² Under the *ejusdem generis* principle, otherwise objectionable material should relate to content similar to pornography, violence, or harassment.¹¹³ If the *ejusdem generis* principle is applied, *objectionable* content becomes an objective standard and therefore excludes political viewpoints.¹¹⁴

III. Analysis

- 39 Both Article 7 of the DSA and Section 230(c)(2)(A) provide (eligibility) for liability exemptions for online service providers engaging in voluntarily good faith measures to remove or restrict access to third-party illegal or objectionable content.
- 40 Under Article 7 of the DSA, online service providers that engage in voluntary content moderation measures are eligible for liability exemptions. To be eligible for liability exemptions, voluntary content moderations measures must be undertaken: i) in good faith, meaning in an objective, non-discriminatory and proportionate manner, with due regards to the rights and legitimate interests of all parties involved¹¹⁵, ii) in a diligent manner, ensuring the removal of content whose illegal

character is apparent,¹¹⁶ and iii) in the observance of fundamental rights, such as the freedom of expression and of information.¹¹⁷ Provided that these conditions are met, online service providers become eligible for liability exemptions. To be exempted from liability, online service providers, upon obtaining actual knowledge or awareness of illegal content, must act expeditiously to remove or disable access to it.¹¹⁸ Under Section 230(c)(2)(A), online service providers that engage in voluntary content moderation measures are exempted from liability under the safeguard of good faith and provided that the content removed is objectionable.

- 41 A couple of similarities on liability exemptions in the two jurisdictions can be observed from the text of the provisions. First, both Article 7 of the DSA and Section 230(c)(2)(A) require good faith voluntary *action*. Section 230(c)(2)(A) guarantees the liability exemptions when proactively taking *action* to remove objectionable content. Article 7 of the DSA guarantees that the liability exemptions are not lost and that online service providers can still benefit from immunity for their *actions* to remove content subject to the conditions in Article 6 of the DSA. This creates a nexus between the action of moderating content and the liability exemptions.¹¹⁹
- 42 Second, liability exemptions in both jurisdictions constitute rules,¹²⁰ whereas the good faith requirements for content moderation constitute standards.¹²¹ The distinction between rules and standards is that the rules constrain the discretion of judges, whereas the standards leave a lot of discretion to judges when interpreting those provisions.¹²² The standard of good faith, being an open term, is or can

110 *National Numismatic Certification, LLC. v. eBay, Inc.*, No. 6:08-CV-42-ORL-19GJK, 2008 WL 2704404, (M.D. Fla. July 8, 2008), *Song Fi, Inc. v. Google, Inc.*, 2015 WL 3624335 (N.D. Cal. June 10, 2015). The principle was also acknowledged in *Holomaxx Techs. v. Microsoft Corp.*, 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011), *Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169 (9th Cir. 2009) (Judge Fisher concurring opinion).

111 *Burns v. United States*, 501 U.S. 129, 138 (1991), *Gollust v. Mendell*, 501 U.S. 115, 126 (1991).

112 Candeub, o.c.

113 Eric Goldman, ‘Online User Account Termination and 47 U.S.C. § 230(c)(2)’, 2 U.C. Irvine L. Rev. 659 (2012).

114 See also Klapper, o.c., page 1296 (quoting Rep. Christopher Cox: “Nor is Section 230 immunity automatically provided on account of moderation or curation policies that restrict access to or availability of content on the basis of political viewpoint”).

115 DSA, Article 7 and Recital 26.

116 *Ibid.* See also *supra* notes 46 and 47.

117 *Ibid.*, Recitals 22 and 26.

118 *Ibid.*, Article 6.

119 See Klapper, o.c. (“Section 230(c)(2) immunity applies only to cases where the entity would have otherwise been held liable because of the moderation decisions. The moderation must be essential to the alleged liability; it cannot be incidental”).

120 See also Eric Goldman, ‘Why Section 230 Is Better Than the First Amendment’ (2019) in 95(1) *Notre Dame Law Review Reflection* (“Section 230 is like a rule; First Amendment defenses are like standards”).

121 Martijn W. Hesselink, ‘The Concept of Good Faith’, in A.S. Hartkamp, E.H. Hondius, M.W. Hesselink, C.E. du Perron & M. Veldman (eds.) *Towards a European Civil Code*, 4th rev. and exp. ed. (pp. 619-649) (KLI, 2011).

122 William Fisher, CopyrightX Lecture Transcripts, <<https://copyx.org/lectures/>>, accessed 16 March 2024.

be subject to the interpretation of judges in both jurisdictions. As the rules on liability exemptions and content moderation measures will have time to mature, the interpretation by the judges of the good faith requirement will convert into guidelines.¹²³

- 43 As to differences, it can be noted that first, both rules on liability exemptions have a test, but the test differs quite significantly. In the EU, the test is whether the online service provider has actual knowledge or awareness of illegal content. If the test is positive, the online service provider can continue to benefit from liability exemptions provided that it acts expeditiously to remove the specific illegal content. In the US, the test is whether the online service provider has materially contributed to the development of content (i.e. whether it is a publisher of the content) ((Section 230(c)(1)). If the test is positive, the online service provider can continue to benefit from the liability exemptions provided that it voluntarily removes in good faith objectionable material (Section 230(c)(2)(A)).
- 44 Second, liability exemptions for voluntary good faith content moderation in Article 7 of the DSA are specifically related to illegal content,¹²⁴ whereas immunity for voluntary good faith content moderation in Section 230(c)(2)(A) pertains to a specific type of content that the provider or user finds objectionable. Based on the interpretation of objectionable content, it may refer to either content similar to pornography, violence, obscenity or harassment under the *ejusdem generis* canon, or to anything that service or provider finds objectionable under a broad interpretation. The latter means that objectionable content may include both illegal and legal but harmful content.
- 45 Third, the rules for liability exemptions under the DSA are subject to other safeguards which are not explicitly mentioned in Section 230. These relate to the principles of proportionality and non-discrimination attached to the good faith standard, the protection of fundamental rights and the

diligence requirement. Nonetheless, as discussed in Chapter C II of this research paper, the US Courts interpretation of Section 230(c) suggests that some of these principles, although not explicitly mentioned in the provision, are embedded in the objectives of enacting Section 230, as well as in the definition pertaining to good faith and objectionable content.

C. Relevant jurisprudence

- 46 This chapter provides an overview of the applicable legal precedents concerning the establishment of liability exemptions for online service providers in relation to voluntary content moderation actions in both jurisdictions. Since the Directive on electronic commerce does not foresee voluntary content moderation measures and the DSA has only been recently adopted, there is a scarcity of legal cases addressing specifically liability exemptions and voluntary content moderation measures. In contrast, Section 230 has been in existence for over twenty years, leading to a substantial body of case law that aids in interpreting the relevant provisions. Nevertheless, the Good Samaritan principle under Section 230(c)(2) has been litigated less than Section 230(c)(1) following the Court's decision in *Zeran v. AOL* to treat removal decisions under Section 230(c)(1) instead of under Section 230(c)(2).¹²⁵

I. European Union

- 47 The DSA confirms the case law of the CJEU on liability exemptions under the Directive and brings clarity to certain elements regarding liability exemptions for online service providers. The cases mostly deal with knowledge and awareness of illegal content, as well as the nature of the service provider (active or passive) that would determine whether the online service provider is exempted from liability.

1. Knowledge and take-down

- 48 The situations in which the online service providers become knowledgeable or aware of the illegal content as a result of both own-initiative investigations and notices by third parties have been examined by the CJEU in *L'Oréal v eBay*¹²⁶ and are reflected in

123 *Ibid.* On the standard of fair use in US copyright law: “over time the courts have tacitly subdivided the universe of cases implicating colorable fair use defenses into subfields and have converged on guidelines concerning how the four factors will be interpreted in each subfield”.

124 DSA, Recital 17 (“the exemptions from liability established in this Regulation should apply in respect of any type of liability as regards any type of illegal content, irrespective of the precise subject matter or nature of those laws.”). See also ‘Questions and answers on the Digital Services Act’ (“The new rules only impose measures to remove or encourage removal of illegal content, in full respect of the freedom of expression”), <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348>, accessed 15 March 2024.

125 *Klapper, o.c.*, fn 142 and citing *Domen v. Vimeo, Inc.*, 433 F. Supp. 3d 592, 601 (S.D.N.Y. 2020), *Riggs v. MySpace, Inc.*, 444 F. App'x 986, 987 (9th Cir. 2011), *Ebeid v. Facebook, Inc.*, No. 18-cv-07030, 2019 WL 2059662, at *5 (N.D. Cal. May 9, 2019).

126 C324/09 *L'Oréal SA v eBay International AG* [2011], para. 122.

Recital 22 of the DSA. In the same case, the CJEU defined the notion of knowledge as knowledge that results from information which is sufficiently and adequately substantiated.¹²⁷ Recital 53 parallels this notion by stating that a notice should contain sufficient information to enable a diligent provider of hosting services to identify, without a detailed legal examination, that it is clear that the content is illegal. *L'Oréal v eBay* judgment also brings clarity of what it means to play an active role of such a kind to give it knowledge, such as providing assistance which entails, in particular, optimizing the presentation of the offers for sale in question or promoting them.¹²⁸ Furthermore, the role played by the active nature of online service providers in determining liability exemptions, which were confirmed by the CJEU in *Google France and Google*¹²⁹ and *L'Oréal v eBay*¹³⁰, are reproduced in Recital 18 of the DSA.

- 49 The most recent case, *YouTube and Cyando*¹³¹ which was adopted after the DSA proposal and related to liability of online service providers for hosting copyright infringing material, provides elements in relation to voluntary content moderation measures and liability exemptions which are also found in the DSA. Thus, the CJEU conclusion that automatic indexing, search function and recommending information does not lead to liability is reproduced in Recital 22 of the DSA. Furthermore, the fact that the online service provider “*is aware, in a general sense of the fact that its service provider is also used to share content which may infringe intellectual property rights*”¹³² does not constitute actual knowledge or awareness, as well as the fact that actual knowledge refers to specific content,¹³³ is included in Recital 22 of the DSA. The CJEU further explained that implementing technological measures aimed at detecting and ending copyright infringing material does not mean that the online service provider plays an active

role.¹³⁴ In other words, the CJEU conclusions in this respect, on one hand incentivised service providers to undertake voluntary measures, and on the other hand, confirms that such measures do not render the service provider active and therefore aware of the illegal content.

- 50 Finally, the DSA aligns with the CJEU ruling in *Eva Glawischnig v Facebook*,¹³⁵ by establishing that the absence of a general monitoring obligation does not mean that online service providers do not have an obligation to monitor in a specific case or when faced with an injunction from national authorities.¹³⁶

2. Good faith and diligence

- 51 With regards to the *good faith* safeguard, more specifically acting in an objective, non-discriminatory and proportionate manner, with due regards to the rights and legitimate interests of all the parties involved, there is limited case law on the nexus between this safeguard and (voluntary) content moderation measures. Thus, these elements will have to be assessed on a case-by-case basis and interpreted accordingly by the CJEU once the rules on liability exemptions for voluntary content moderation measures in the DSA have matured. The *objective* requirement, if given a literal interpretation of the definition, can be understood as acting based on facts and can be closely related to the principle of non-discrimination.¹³⁷ The *non-discriminatory* requirement can be understood as a condition that the online service providers, when engaging in voluntary content moderation measures to remove or disable access to illegal content, do not discriminate based on speaker, the content of his/her message or other characteristics.¹³⁸ Such an interpretation reflects the non-discrimination principle in the Charter of Fundamental Rights of

127 *Ibid.*

128 *Ibid.*, para.123.

129 Joined Cases C-236/08 to C-238/08 *Google France SARL and Google Inc. v Louis Vuitton Malletier SA and Others* [2010], para. 114 (except that the DSA no longer refers to the passive nature, but rather active nature of the online service provider).

130 *L'Oréal v eBay*, para.113.

131 Joined Cases C682/18 and C683/18 *Frank Peterson v Google LLC and Elsevier Inc. v Cyando AG* [2021], para.114.

132 *Ibid.*, para. 111.

133 *Ibid.*, para.113.

134 *Ibid.*, paras. 94 and 109.

135 Case C18/18 *Eva Glawischnig Piesczek v. Facebook Ireland Limited* [2019].

136 DSA, Recital 30.

137 van de Kerkhof, o.c.

138 See also Christoph Busch, ‘Platform Responsibility in the European Union’ (“While the DSA does not formulate an explicit requirement of platform neutrality, the reference to the principle of non-discrimination makes it clear that an arbitrary unequal treatment of content within the framework of content moderation would be a violation of the due diligence requirements”) (2022) <https://sites.tufts.edu/digitalplanet/files/2022/12/DD-Report_2-Christoph-Busch-11.30.22.pdf>, accessed 15 March 2024.

the European Union¹³⁹ and mentioned in Recital 3 of the DSA.

- 52 Regarding the *proportionality* requirement, the CJEU, in *Sabam v Netlog*, held that “an injunction [requiring the installation of a filtering system] would result in a serious infringement of the freedom of the hosting service provider to conduct its business since it would require that hosting service provider to install a complicated, costly, permanent computer system at its own expense”.¹⁴⁰ Therefore, when undertaking voluntary measures, online service providers must ensure that such measures are not excessively costly or burdensome on any of the parties involved and serve the purpose for which they are employed.¹⁴¹ This reflects the principle of proportionality as defined in the Treaty of the EU as being suitable and necessary to achieve the desired end and not impose a burden on the individual that is excessive in relation to the objective sought to be achieved.¹⁴²
- 53 The proportionality principle in Recital 26 of the DSA is intrinsically linked to the legitimate interests of both the recipients of the service and the service providers themselves. It entails, as indicated in Recital 22 of the DSA, the rights of all parties involved, not only the rights of the recipients of the service. Thus, in relation to the rights of the service providers, the *Sabam v Netlog* case tackles the principle of proportionality by looking at the service provider’s freedom to conduct business, which is also the meaning given to proportionality in Article 17(5) of the Directive 2019/790¹⁴³ and Article 3 of Directive

2004/48 (such measures “shall not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays”).¹⁴⁴

- 54 It is noteworthy that the *Sabam v Netlog* judgment prompted the CJEU to assert that requiring an online service provider to implement a filtering system would force them to actively monitor all user data, a practice prohibited by Article 15 of the Directive (now Article 8 of the DSA). Additionally, such a broad monitoring obligation would be inconsistent with Article 3 of Directive 2004/48,¹⁴⁵ which states that the measures referred to by the directive must be fair, proportionate, and not excessively costly.¹⁴⁶ Similar conclusions were reached in *Scarlet Extended*.¹⁴⁷ Recital 26 of the DSA confirms that online service providers can employ automated filtering tools when engaging in voluntary content moderation, provided that they do so diligently and minimize the rate of errors. Moreover, Article 7 of the DSA which guarantees eligibility for liability exemptions for voluntary content moderation, and the Commission’s confirmation¹⁴⁸ that online service providers can maintain their liability exemptions if they promptly remove the illegal content, seem to suggest that online service providers can still benefit from liability exemptions when undertaking voluntary measures. Nonetheless, reconciling general monitoring obligation with voluntary content moderation remains challenging.
- 55 With regards to the *diligence* safeguard, although not dealt by the CJEU, but by the ECtHR, the *Delfi v Estonia*¹⁴⁹ case offers insights into undertaking (voluntary) content moderation measures in a diligent manner. The case concerned the liability of Delfi, an Internet news portal, for defamation

139 EU Charter of Fundamental Rights, Article 21.

140 *SABAM v Netlog NV*, para. 46.

141 The Directive 2017/541 on combating terrorism confirms this view: “measures or removal and blocking [of online content constituting a public provocation to commit a terrorist offence] are limited to what is necessary and proportionate and that users are informed of the reason for those measures”, Article 21 (3).

142 Article 5(4) of the Treaty on European Union.

143 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, Article 17(5) and Recital 66. See also Advocate General Saugmandsgaard Øe in *C-401/19 Republic of Poland v European Parliament, Council of the European Union* [2021], para. 156 (“Article 17(5) of Directive 2019/790, [...] states that the measures to be taken by each supplier must be assessed, in the light of the principle of proportionality, with regard to factors such as the ‘size of the service’ or the ‘cost’ of available tools, seems to me to be more relevant to the question of compliance with the freedom to conduct a business, which is not the subject of the present case, than to freedom of expression”).

144 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004). This was confirmed by Advocate General Cruz Villalon in *C-314/12 UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft GmbH* [2014] para.79 (“the measure is neither ‘fair and equitable’ nor ‘proportionate’ within the meaning of Article 3 of Directive 2004/48”).

145 Directive 2004/48/EC, Article 3.

146 *Sabam v Netlog*, paras. 34 and 38.

147 *Scarlet Extended*, paras. 36 and 40.

148 Communication from the Commission COM(2017) 555, *supra* note 18.

149 *Delfi AS. v. Estonia*, App. nr. 64569/09 (European Court of Human Rights (Grand Chamber), 16 June 2015).

in its capacity as publisher¹⁵⁰ of the (anonymous) comments posted on its portal, despite the fact that it promptly removed the illegal comments upon receiving notification.¹⁵¹ Since Delfi was not an intermediary service it could not rely on the liability exemptions specified in Articles 12 to 15 of the Directive.¹⁵²

- 56 The Court ruled that the automatic word-based filter employed by Delfi, while it may have removed some defamatory comments, it failed to filter out and detect hate speech and incitement to violence. This failure limited Delfi's ability to expeditiously remove the defamatory comments with the consequence that the clearly illegal comments remained online for six weeks.¹⁵³ The Court found that the comments which were related to hate speech and incitement to violence *"did not require any linguistic or legal analysis since the remarks were on their face manifestly unlawful"*.¹⁵⁴ According to the Court, the majority of the comments lacked sophisticated metaphors, hidden meanings, or subtle threats. Instead, they were overt expressions *"of hatred and blatant threats"*.¹⁵⁵ Additionally, the Court noted that the comments did not contain any information that would necessitate excessive verification by the portal operator.¹⁵⁶ Recital 53 of the DSA reflects the same reasoning according to which a notice that contains sufficient information to enable a diligent operator to identify, without a legal detailed examination, the illegality of content gives rise to knowledge or awareness of illegality.¹⁵⁷ This aligns with the concept of apparent illegality as defined by the CJEU in the *L'Oréal v eBay* case, as being *"aware of facts or circumstances on the basis of which a diligent economic operator should have*

identified the illegality in question".¹⁵⁸

- 57 The Court's conclusions indicate that if a news portal, such as Delfi, voluntarily implements content moderation measures through automated tools or by establishing a team of moderators to remove illegal content but fails to eliminate all such content, it may be held liable for third-party content, particularly when the content displays apparent illegality, such as hate speech or incitement to violence. Should Delfi have been found to be an intermediary service, the outcome of this ruling on voluntary moderation to remove third-party illegal content remain uncertain. Nevertheless, the CJEU has not yet dealt with a case similar to Delfi¹⁵⁹ to allow us to draw parallels with it.

3. Fundamental rights

- 58 With regards to the fundamental rights of the recipients of service, which include freedom of expression and of information (Recital 22 of the DSA), the CJEU held in *Scarlet Extended* that the *"filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information"*.¹⁶⁰ Thus, the unjustified removal of content by automated tools can pose a potential threat to the protection of fundamental rights. By analogy, online service providers, when undertaking voluntary content moderation measures, especially by employing algorithmic filtering tools, must ensure the implementation of necessary safeguards to protect fundamental rights of users, such as freedom to receive and impart information.¹⁶¹

- 59 The CJEU held in *UPC Telekabel* that when complying with an injunction, the addressee of that injunction *"must ensure compliance with the fundamental right of internet users to freedom of information"* so that the measures implemented do not affect *"internet users who are using the provider's services in order to lawfully access information"*.¹⁶² The case is illustrative of how

150 Delfi was found to be in control of the comments and thus acting as a media publisher since it i) invited and encouraged comments on its website, ii) economically profited from the number of visits which in turn depended on a number of comments, and iii) set out the rules for the comments section and made changes to it (removed comments) if those rules were breached.

151 *Ibid.*, para. 65. The Grand Chamber ruled that there was no violation of Article 10 of the Convention of Human Rights.

152 *Ibid.*, para. 13.

153 *Ibid.*, para. 156.

154 *Ibid.*, para. 117.

155 *Ibid.*, para. 156.

156 *Ibid.*, para. 16.

157 DSA, Recital 53.

158 *L'Oréal SA v eBay*, para. 120.

159 Liudmila Sivetc, 'Future of Internet Portals After the Case of Delfi', Master thesis (2016), University of Turku.

160 *Scarlet Extended*, para. 50.

161 See for instance Riis and Schwemer, o.c. (*"The finding of the CJEU in the Scarlet Extended and Netlog judgments that an order to implement filtering technologies violates Article 15 of the E-Commerce Directive and fundamental rights, in principle, must also be considered applicable to other rules that create an obligation to implement proactive measures"*).

162 *UPC Telekabel*, paras. 55-56.

CJEU interprets the knowledge and take down approach for liability exemption by giving due weight to the rights of users¹⁶³ “whose content may be blocked or removed”.¹⁶⁴

II. United States

60 In the US, liability exemptions have only been updated once when Congress enacted in 2018 a law creating a sex trafficking exception¹⁶⁵ to the immunity provided by Section 230. Nonetheless, the breadth of case law available provides details about the judicial interpretation of Section 230(c), in particular subsection (c)(1). With regards to the Good Samaritan rule of Section 230(c)(2)(A), the case law dealt with either determining whether the removal of content was done in good faith or whether the content was indeed objectionable.

1. Knowledge

61 Pre-Section 230 enactment, the *Cubby* case upheld the common law distributor liability according to which distributors are liable for third-party content only if they have actual knowledge of the illegal character of the content.¹⁶⁶ Due to a contradictory ruling in *Stratton Oakmont*, Congress introduced Section 230 to address the issue of the moderator’s dilemma.¹⁶⁷

62 The Fourth Circuit was the first to interpret Section 230 after its enactment in *Zeran v. AOL*. The plaintiff brought negligence claims against AOL as AOL “had a duty to remove the defamatory posting promptly, [...], and to effectively screen future defamatory material”.¹⁶⁸ The Fourth Circuit Court asserted that Section 230(c)(1) creates a federal immunity for any cause of action that would make a service provider liable for information originating with a third-party.¹⁶⁹ It

thus led to preserving immunity of online service providers in situations where they negligently fail to¹⁷⁰ or chose to not remove content from their websites.¹⁷¹ Publishing, as well as removal and editing of material are considered basic editorial functions covered by Section 230 and confirmed consistently by the US Courts.¹⁷² Such basic editorial functions do not deem a service provider as publisher or speaker of the content provided by a third-party.

63 Following *Zeran v. AOL*, subsequent decisions have followed the broad interpretation of Section 230(c)(1),¹⁷³ providing sweeping immunity to online service providers for any tort action.¹⁷⁴ Under this wide interpretation courts have dismissed lawsuits on a large set of causes of action, including sex trafficking of minors (*Doe v. Backpage*¹⁷⁵), illegal sale of guns (*Gibson v. Craigslist*¹⁷⁶), defective sale of products (*Lemmon v. Snap*¹⁷⁷), the encouragement of terrorist acts (*Force v. Facebook*¹⁷⁸),¹⁷⁹ and racially discriminatory removal of content (*Sikhs for Justice*

163 Written comments in the case of *Delfi AS v. Estonia*, No 64569/09, 6 June 2014, <<https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2015/06/20140606-Delfi-intervention-FINAL.pdf>>, accessed 16 March 2024.

164 *UPC Telekabel*, para. 57.

165 The Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (“FOSTA”).

166 See *supra* note 81.

167 See *supra* note 86.

168 *Zeran v. AOL*.

169 *Ibid.*

170 See also *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir. 2008), *Doe* brought negligence claims against MySpace from failing to implement “basic safety measures to prevent sexual predators from communicating with minors on its Web site”.

171 See *supra* notes 93–95.

172 *Zeran v. AOL*, o.c., where the Fourth Circuit Court held that Section 230(c)(1) precludes “lawsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone, or alter content”. Such basic editorial functions were also noted in *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*, 521 F.3d 1157 (9th Cir. 2008).

173 Notably First, Third, and Tenth Circuit as indicated in *Force v. Facebook*, On a Petition For Writ of Certiorari, enquiring about the meaning of Section 230(c)(1).

174 Michael L. Rustad and Thomas H. Koenig, ‘The Case for a CDA Section 230 Notice-and-Take-Down Duty’ (2023) 23 NEV. L.J. 533.

175 *Jane Doe No. 1 v. Backpage.com, LLC*, 817 F. 3d 12 (1st Circuit 2016).

176 *Gibson v. Craigslist, Inc.*, 08-CV-7735, 2009 WL 1704355 (S.D.N.Y. June 15, 2009).

177 *Lemmon v. Snap, Inc.*, 440 F. Supp. 3d 1103 (CD Cal. 2020).

178 *Force v. Facebook, Inc.*, 934 F.3d 53 (2nd Cir. 2019).

179 *Franks*, o.c.

*v. Facebook*¹⁸⁰).¹⁸¹ The SCOTUS has recently issued an opinion in favour of Google holding that Section 230 protects YouTube's recommender systems from liability under the anti-terrorism act.¹⁸²

- 64 The wide consensus on the broad immunity of Section 230(c)(1) is not unanimously shared. The underlying reason of this conflicting approach is that there is a difference between immunizing only traditional functions and immunizing any activity of publishing.¹⁸³ Justice Thomas, writing on petition for writ of certiorari¹⁸⁴ in *Malwarebytes v. Enigma* provided a textual analysis of the provision which criticizes the consensus. He explained that Section 230(c)(1) applies when online service providers *unknowingly* leave up illegal third-party content, while 230(c)(2)(A) applies when they take down in good faith certain third-party content.¹⁸⁵ In supporting his argument, he stated that Section 502¹⁸⁶ of the CDA “*makes it a crime to knowingly display obscene material to children, even if a third party created that content*”.¹⁸⁷

180 *Sikhs for Justice Inc. v. Facebook, Inc.*, 697 Fed. Appx. 526 (9th Circuit 2017).

181 Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87.

182 *Reynaldo Gonzalez, et al., Petitioners v. Google LLC*, On a Petition For Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit, 18 May 2023.

183 *Force v. Facebook*, On a Petition For Writ of Certiorari, enquiring about the meaning of Section 230(c)(1).

184 A Petition for Writ of Certiorari is an appellee's formal request to a state Supreme Court or to the Supreme Court of the United States to review a case for error or violation that occurred in a lower court.

185 Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87.

186 See Vincent Dumas, ‘Enigma Machines: Deep Learning Algorithms As Information Content Providers Under Section 230 of The Communications Decency Act’ (“*The Senate and House introduced two amendments, one from each chamber, as part of a unified CDA: Sections 223 and 230. Section 223 criminalized the transmission of obscene material or harassing communications over the internet*”). <https://wlr.law.wisc.edu/wp-content/uploads/sites/1263/2023/01/14-F_Dumas-Camera-Ready-1581%E2%80%931616-PDF-.pdf>, accessed 16 March 2024, and Danielle K. Citron and Benjamin Wittes, ‘The Problem Isn’t Just Backpage: Revision Section 230 Immunity’ 2 *Georgetown Law Technology Review* 453 (2018) (“*Section 502 of the final legislation contained the Senate’s additions to 47 U.S.C. § 223. Section 509 contained the House’s new Section 230*”).

187 Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87.

What has instead prevailed in the Courts is that Section 230(c)(1) confers immunity even when a company distributes content that it *knows* is illegal as in *Zeran v. AOL*.¹⁸⁸ Courts have narrowly interpreted Section 230(f)(3) which defines a content creator as anyone “*responsible, in whole or in part, for the creation or development*” of the content to cover only extensive edits.¹⁸⁹ Referring to *Barnes v. Yahoo*, which held that “*Subsection (c)(1), by itself, shields from liability all publication decisions, whether to edit, to remove, or to post, with respect to content generated entirely by third parties*”,¹⁹⁰ Justice Thomas stated that Courts have restricted the limits Congress placed on removal decisions.¹⁹¹ His opinion was based on the dissenting opinion of Judge Katzman in *Force v. Facebook* who rejected the notion that Section 230(c)(1) should be construed broadly.¹⁹²

- 65 The conflicts among the circuits¹⁹³ regarding the meaning of section 230(c)(1) have led the Courts of appeals to disagree not only about when section 230(c)(1) exempts service providers from liability, but also about what type of defence it is.¹⁹⁴ A majority of the Courts of appeals follow the *Zeran* reasoning and hold that Section 230(c)(1) immunity applies to any service provider that acts as a publisher of third-party content.¹⁹⁵ Thus, the immunity provided by Section 230(c)(1) depends on the nature of the defendant's *conduct* and whether the *defendant can show* it was acting as a publisher, and if available would apply to *all types of claims*.¹⁹⁶ The Seventh Circuit, on the other hand, holds that section 230(c)(1) does not create a form of immunity at all, but it is

188 *Ibid.*

189 *Ibid.*

190 *Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1105 (9th Cir. 2009).

191 Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87.

192 *Force v. Facebook*, On a Petition For Writ of Certiorari, enquiring about the meaning of Section 230(c)(1).

193 The US Court of Appeals are the intermediate appellate courts of the United States federal judiciary and are divided into 13 Circuits. The US district courts are the trial courts of the US federal judiciary. District courts' decisions are appealed to the US court of appeals for the Circuit in which they reside, except for certain specialized cases that are appealed to the US Court of Appeals for the Federal Circuit or directly to the U.S. Supreme Court. (Source: Wikipedia).

194 *Force v. Facebook*, *supra* note 192.

195 *Ibid.*

196 *Ibid.*

rather a definition.¹⁹⁷ Thus, the defence provided by Section 230(c)(1) is limited to claims which require a plaintiff to show that the defendant was a publisher.¹⁹⁸

2. Good faith

66 Since there is no statutory definition of the term *good faith*, the Courts have given interpretations of what it means when an online service provider does not act in good faith. For instance, plaintiff's claims that the defendant acted under an anticompetitive motive and therefore not in good faith were allowed to proceed¹⁹⁹ in several cases such as *e-ventures Worldwide v Google*,²⁰⁰ *Spy Phone v Google*,²⁰¹ or *Darnaa v Google*.²⁰²

67 In *e-ventures Worldwide v. Google*, the Middle District Court of Florida denied Google's motion to dismiss under Section 230(c)(2) due to e-ventures presenting sufficient evidence about Google's anticompetitive motivations.²⁰³ The Court asserted that moderation based on anticompetitive motives does not constitute good faith. Google however won the case on the basis that its decision to de-index all of e-ventures' websites so they would no longer appear in Google search results constituted speech protected under the First Amendment.²⁰⁴

68 In *Spy Phone v. Google*, the Northern District Court of California examined the good faith covenant by

197 See for instance *Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003).

198 *Force v. Facebook*, *supra* note 192.

199 CRS, *supra* note 92.

200 *e-ventures Worldwide v. Google*, 2:14-CV-646-FTM-29CM, 2016 U.S. Dist. LEXIS 62855 (M.D. Fla. May 12, 2016).

201 *Spy Phone Labs LLC v. Google Inc.*, 15-CV-03756-KAW, 2016 WL 6025469, at *8 (N.D. Cal. Oct. 14, 2016).

202 *Darnaa LLC v. Google, Inc.*, 2015 WL 7753406 (N.D. Cal. Dec. 2, 2015), Order by Judge Ronald M. Whyte granting 15 Motion to Dismiss with leave to amend.

203 Ashley Johnson and Daniel Castro, 'The Exceptions to Section 230: How Have the Courts Interpreted Section 230?' (ITIF, 22 February 2021) <<https://itif.org/publications/2021/02/22/exceptions-section-230-how-have-courts-interpreted-section-230/>>, accessed 16 March 2024.

204 *e-ventures Worldwide v. Google, Inc.*, 2:14-cv-00646-PAM-CM (M.D. Fla. Feb. 8, 2017) where the Court held that "the First Amendment protects these decisions, whether they are fair or unfair, or motivated by profit or altruism".

looking at whether Google's decision to remove Spy Phone app for violating its anti-spyware policy was "pretextual" since no such policy existed. The plaintiff's claim was that Google, "by selling the keywords "Spy Phone" to developers of parental monitoring apps" and granting priority placement to the purchaser of those keywords for its competitive app in Google Play, placed the plaintiff at a competitive disadvantage.²⁰⁵ The same Court examined YouTube's decision to remove a video for an inflated view count which allegedly violated its terms of use in *Darnaa v. Google*. The Court found that "the allegations in the complaint are sufficient to support a claim for contractual breach of the covenant of good faith and fair dealing".²⁰⁶ In reaching that conclusion, the Court explained that YouTube's terms of service regarding its rights to remove and relocate videos were ambiguously drafted.

69 The good faith requirement has been discussed in other cases such as *Jurin v. Google*²⁰⁷ where the Eastern District Court of California dismissed a breach of the duty of good faith and fair dealing by Google for not adhering to the terms of its Adwords policy. The Court noted that "good faith and fair dealing is satisfied where the conduct at issue is either expressly permitted or at least not prohibited".²⁰⁸ The Court ruled that Google followed the terms of its policy "and because this conduct was expressly permitted, good faith is satisfied".²⁰⁹ It further held that "the implied covenant [of good faith] cannot override express provisions".²¹⁰ The claims were barred by the immunity provided by Section 230 and the case was quoted by the Northern District Court in *King v Facebook* where King alleged that Facebook removed multiple posts that Facebook considered to be in violation of its terms of use and "that Facebook treats black activists and their posts differently than it does other groups".²¹¹ Because "each of King's claims against Facebook seeks to hold it liable as a publisher for either removing his posts, blocking his content, or suspending his accounts",²¹² the Court applied Section 230(c)(1) to dismiss the case.

205 *Spy Phone v. Google*.

206 *Darnaa v. Google*.

207 *Daniel Jurin v. Google Inc.*, No. 2:09-cv-03065-MCE-KJM, Memorandum of Order (E.D. Cal. Feb.15, 2011).

208 *Ibid.*

209 *Ibid.*

210 *Ibid.*

211 *King v. Facebook, Inc.*, No 19-cv-01987-WHO (N.D. Cal. Sept. 5, 2019).

212 *Ibid.*

3. Objectionable content

70 Some Courts have interpreted ‘otherwise objectionable’ broadly because Section 230(c)(2)(A) states that the provider or user is the one who determines whether the content is objectionable.²¹³ The subjective nature of objectionable content was considered in *e360Insight v. Comcast*,²¹⁴ where the Northern District Court of Illinois ruled that commercial unsolicited and bulk email could be deemed objectionable under Section 230(c)(2)(A) and that online service providers are immune from liability when they block content that they subjectively consider to be objectionable.²¹⁵ In *Holomaxx v. Yahoo*, the judge for the Northern District Court of California noted that “no court has articulated specific, objective criteria to be used in assessing whether a provider’s subjective determination of what is “objectionable” is protected by [Section] 230(c)(2).”²¹⁶ The Court eventually acknowledged that the harassing nature of the emails were sufficient to reasonably conclude that the content was objectionable.²¹⁷

71 The Western District Court of Washington in *Zango v. Kaspersky* also considered the subjective nature of ‘otherwise objectionable’ since it is the provider or the user who determines what content is objectionable.²¹⁸ In its concurring opinion for the Ninth Circuit in *Zango v. Kaspersky*,²¹⁹ Judge Fisher warned that ‘otherwise objectionable’ may be invoked by a blocking software provider to block content for anticompetitive reasons. The interpretation of ‘otherwise objectionable’ was ultimately not examined since the plaintiff did not raise it and thus waived it.²²⁰

72 Blocking for anticompetitive reasons was later

²¹³ CRS, *supra* note 92.

²¹⁴ *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605 (N.D. Ill. 2008).

²¹⁵ *Ballon, o.c.*

²¹⁶ *Holomaxx Technologies v. Yahoo, Inc.*, CV-10-4926-JF (N.D. Cal. March 11, 2011).

²¹⁷ *Ibid.*

²¹⁸ *Zango, Inc. v. Kaspersky Lab, Inc.*, No. 07-0807-JCC, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007).

²¹⁹ *Zango v. Kaspersky*, *supra* note 110.

²²⁰ Eric Goldman, ‘Anti-Spyware Company Protected by 47 USC 230(c)(2) - *Zango v. Kaspersky* (Technology & Marketing Law Blog, 26 June 2009) <https://blog.ericgoldman.org/archives/2009/06/antispyware_com.htm>, accessed 16 March 2024.

addressed by the Ninth Circuit in *Enigma Software v. Malwarebytes*²²¹ which ruled that Section 230(c)(2)(B) did not apply²²² because objectionable content in Section 230(c)(2)(A) does not include blocking access to content for anticompetitive reasons.²²³ By looking at the statute’s policy goals to determine whether the competitors’ content was objectionable and therefore its removal justified, the Court on appeal held that Section 230 objective is to promote the advancement of tools that maximise user control by granting immunity to “providers of such tools, such as Malwarebytes, regardless of motive [...] But, to prevent misuse of those tools, [they must restrict content] by acting in good faith”.²²⁴ This perspective implies that what the user or provider considers to be objectionable is not unlimited,²²⁵ but must fall within the specific categories of content which are either enumerated in Section 230(c)(2)(A) or align with the policy goals of Section 230.

73 In *Song Fi v. Google*, the Northern District Court denied immunity under Section 230(c)(2) to YouTube for removing a video because its view count was considered by YouTube to have been artificially inflated and thus “its content violated YouTube’s Terms of Service”.²²⁶ The Court did not consider that the inflated view count qualifies as objectionable content as it was not in line with the policy goals

²²¹ *Enigma Software v. Malwarebytes*, where, according to the plaintiff, Malwarebytes’ decision to block unwanted programs of Enigma served as a ‘guise’ for anticompetitive conduct. The Court concluded that “if a provider’s basis for objecting to and seeking to block materials is because those materials benefit a competitor, the objection would not fall within any category listed in the statute and the immunity would not apply”.

²²² According to Eric Goldman, this decision overruled *Zango v. Kaspersky* which provided immunity to providers of malware software. The difference was that in *Zango v. Kaspersky* the interpretation of ‘otherwise objectionable’ had not been fully examined because there was no dispute over the objectionable nature of the blocked content, *supra* note 221.

²²³ *Johnson and Castro, o.c.*

²²⁴ *Enigma Software v. Malwarebytes*, No. 5:17-cv-02915-EJD (2019), On Appeal from the United States District Court for the Northern District of California, Petition For Panel Rehearing and Rehearing En Banc.

²²⁵ Annemarie Bridy, ‘Remediating Social Media: A Layer-Conscious Approach’ (2018) Boston University Journal of Science and Technology Law, 24(193-228).

²²⁶ *Song Fi v. Google*.

of the CDA.²²⁷ It therefore construed the term ‘otherwise objectionable’ more narrowly to avoid allowing online service providers to remove any content they wish.²²⁸

- 74 The cases dealing with the interpretation of ‘good faith’ and ‘otherwise objectionable’ content suggest that there is an overlap between the two terms. Some Courts interpreted the decision to remove or restrict access to material provided to have been done in good faith by looking at whether the material removed fell under the categories listed in Section 230(c)(2)(A) and was indeed objectionable. As Judge Fisher concurring opinion in *Zango v. Kaspersky* suggests, blocking software for anticompetitive reasons by invoking ‘otherwise objectionable’ can be considered to be acting in bad faith.²²⁹

III. Analysis

- 75 Although *Delfi v. Estonia* was not reviewed by the CJEU, but by ECtHR which does not have a jurisdiction to apply EU law,²³⁰ and *Stratton Oakmont* was reviewed before Section 230 was enacted, these two notable cases are useful for setting the scene regarding the liabilities of news portals²³¹ for unsuccessful content moderation.
- 76 Similar to *Delfi*, *Prodigy* faced liability for defamatory comments posted by anonymous users on its bulletin board, whether it knew about the content or not. *Stratton Oakmont* and *Delfi v. Estonia* share resemblances in that both *Prodigy* and *Delfi* were found to be publishers on the basis

of exercising editorial control over illegal content, including efforts to remove such content but failing to remove some of it. *Prodigy*’s content moderation policies, technological measures, and employment of moderators (board leaders) to act as editors for the bulletin boards, contributed to the finding that it is a publisher. This parallel is evident in *Delfi*’s engagement in automatic content filtering, the establishment of rules for the comments section, and the removal of comments, all of which granted it editorial control over the content and resulted in its classification as a publisher. Although the CJEU might have led to opposite conclusions had *Delfi* been an information society service, the case offers some perspectives and anticipates questions about how to determine the circumstances under which an online service provider can lose immunity for unsuccessful content moderation measures (i.e. failing to remove all illegal content).

- 77 The Courts’ interpretation of the immunity available under Section 230(c)(1), as well as what constitutes ‘good faith’ and ‘objectionable’ content, provides valuable insights into the similarities and differences regarding the provisions offering immunity to online service providers for hosting and removing content in both jurisdictions.
- 78 Under a narrow interpretation of Section 230(c), the following similarities regarding the immunity provisions in Section 230(c) and Article 6 and 7 of the DSA can be noted.
- 79 First, both Section 230(c)(1) and Article 6(1)(a) of the DSA offers immunity to online service providers that *unknowingly* host illegal content on their websites. Under Section 230(c)(1), if the service provider acted as a publisher, it can still benefit from immunity under Section 230(c)(2)(A) by voluntarily removing the content in good faith. Under Article 6 of the DSA, if online service providers become aware of the illegal content, either through third-party notices or own-initiative investigations, it can still benefit from immunity under Article 6(1)(b) by promptly removing the content.
- 80 Second, the Courts’ narrow interpretation of good faith and objectionable content suggest that similar to the EU requirements for voluntary content moderation measures, the good faith standard under Section 230(c)(2)(A) is expected to be assessed from an objective perspective. Similarly, the term ‘otherwise objectionable’ has been given an objective reading and confirm the principle of *ejusdem generis* in interpreting objectively the term ‘otherwise objectionable’. This narrow interpretation would render the removal decisions of online service providers to be objective and therefore non-discriminatory as it is required under the DSA.

227 Eric Goldman, ‘Section 230(c)(2) Gets No Luv From the Courts—Song Fi v. Google’(Technology & Marketing Law Blog, 12 June 2015) <<https://blog.ericgoldman.org/archives/2015/06/section-230c2-gets-no-luv-from-the-courts-song-fi-v-google.htm>>, accessed 16 March 2024.

228 CRS, *supra* note 92.

229 *Zango v. Kaspersky* (“Unless § 230(c)(2)(B) imposes some good faith limitation on what a blocking software provider can consider “otherwise objectionable,” or some requirement that blocking be consistent with user choice, immunity might stretch to cover conduct Congress very likely did not intend to immunize”).

230 ECtHR, Guide on the case-law of the European Convention on Human Rights, European Union law in the Court’s case-law (2022) <https://www.echr.coe.int/documents/d/echr/Guide_EU_law_in_ECHR_case-law_ENG>, accessed 16 March 2024.

231 *Delfi* was deemed a publisher and not an information society service provider which would have made it eligible for liability exemptions under Article 14 of the Directive.

- 81 Finally, the DSA explicitly mandates that online service providers diligently remove illegal content, especially when it can be established without a detailed legal examination that such content is illegal.²³² Although Section 230(c)(2)(A) does not explicitly require online service providers to moderate content diligently, the US Courts have, to some extent, reflected this requirement by asserting that good faith moderation efforts involve the removal of content which is indeed objectionable.
- 82 Under a broad interpretation of Section 230(c), the following differences between the immunity provisions in the two jurisdictions can be noted.
- 83 First, Section 230(c)(1) immunizes online service providers for any cause of action, including any decision to *knowingly* host objectionable content or even facilitate and encourage illegal activity. This is in contrast with the provisions in the DSA which immunizes service providers if they *unknowingly* host illegal content or promptly remove content upon obtaining knowledge.
- 84 Second, if ‘otherwise objectionable’ is anything that the user or provider finds objectionable, then the term constitutes a subjective standard.²³³ Such a subjective approach would allow voluntary content moderation policies to be discriminatory as they would favour certain types of views or messages.²³⁴
- 85 Third, embracing this broad interpretation stemmed from policy considerations and purpose arguments to justify the promotion of unrestricted speech on the internet.²³⁵ The Courts’ overemphasis on free speech is, however, made to the detriment of public safety and welfare.²³⁶ Additionally, the Courts’ frequent reliance on Section 230(c)(1) instead of (c)(2) implies a primary consideration of fostering free speech and a secondary focus on addressing illegal content. In contrast, the CJEU has given significant consideration to the freedom of expression and right to information of service recipients when examining injunctions to remove or disable access to illegal content. This suggests an effort at striking a balance between the rights and interest of all parties involved and the objective of fighting illegal content online.

232 See *supra* note 48.

233 Candeub, *o.c.*

234 *Ibid.*

235 Klapper, *o.c.* See also Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87.

236 Meeran, *o.c.*

- 86 Finally, neither the statute nor the US case law suggests that content moderation measures should take into account the principle of proportionality, which under the DSA mean that voluntary content moderation measures should be implemented without unduly infringing upon the rights of other parties, including the freedom of online service providers to conduct their business. Nonetheless, the broad interpretation of Section 230(c)(1) has been based on the purposive argument of protecting free speech, such that service providers have the right, under the First Amendment to host or not host any content they want.²³⁷

D. Proposals to reform Section 230(c)(2)

- 87 In view of growing harms resulting from hate speech, disinformation, and the proliferation of other illegal content available on the internet, especially material related to pornography and child sexual abuse, there have been calls to amend Section 230 to give impetus to online service providers to keep and remove “slime” off their websites.²³⁸ Most of the proposed amendments to Section 230 seek to define the meaning of the terms ‘good faith’ and ‘otherwise objectionable’ content pertaining to Section 230(c)(2)(A) and to clarify the interaction between Section 230(c)(1) and Section 230(c)(2) when it comes to providing immunity for removal decisions.
- 88 A number of proposals have been put forward to clarify the ambiguities in Section 230, particularly the lack of a statutory definition of good faith and objectionable content in Section 230(c)(2)(A). The proposals aim to depart from the subjective standard of the terms, by ensuring that removal decisions do not apply a selective enforcement of the policies²³⁹ or are only undertaken when the provider or user has an objectively reasonable belief that the content is objectionable.²⁴⁰ The proposals also highlight a gap

237 Daphne Keller, ‘Who Do You Sue? State and Platform Hybrid Power Over Online Speech’ (2019) 1902 Aegis Series Paper.

238 U.S. Sen. Ron Wyden in an interview with Esquire: “I would like the big tech companies to do more to step up and deal with the slime that’s on their platform. The companies are clearly capable of doing it when they think it helps their bottom line”. (2019), <<https://classic.esquire.com/article/2019/4/1/legislate-against-the-machine>>, accessed 17 March 2024.

239 S.3983 (“Limiting Section 230 Immunity to Good Samaritans Act”) proposed by Sen. Josh Howley in July 2020 <<https://www.congress.gov/bill/116th-congress/senate-bill/3983/text?r=6&s=1.>>, accessed 17 March 2024.

240 H.R. 3827 (‘Protect Speech Act’) introduced by US Rep.

between what Section 230(c)(1) is meant to apply to (i.e. claims for content that is left up)²⁴¹ and what in practice is used for (i.e. claims for content that is both left up and taken down).²⁴² A proposed bill would remove liability exemptions if the providers were aware of the illegal content or activity.²⁴³

- 89 There are also some reform efforts on the State level. For instance, a Texas law that forbids large service providers from removing or moderating content based on a user's viewpoint is awaiting review from the SCOTUS.²⁴⁴ The law would violate online service providers' free speech rights under the First Amendment as it would force them to carry content that violates their content moderation policies. Although the law does not propose to amend Section 230, it may be in contradiction with the immunities afforded by it.²⁴⁵
- 90 Finally, suggestions for reforms have also come from academia to remove the 'good faith' covenant from Section (c)(2)(A) as it only "invites judicial confusion [...] only to reach the same result: a pre-vailing defendant".²⁴⁶ Others, like Keats Citron and Wittes, have suggested that online service providers should be afforded immunity from liability if they could show that they have taken reasonable steps to prevent the illegal uses of their services.²⁴⁷ Rustad

and Koenig have recommended linking liability exemption to the lack of actual knowledge,²⁴⁸ reflecting the common law distributor liability described in *Cubby v. CompuServe*.²⁴⁹ A similar recommendation is that the test for liability exemption should be that the plaintiff first alleges that the defendant had actual knowledge of the illegality of content, after which the burden of proof switches to the defendant to show that it did not have knowledge and can invoke immunity under Section 230(c).²⁵⁰ The test stems from the common law distributor liability described in *Cubby*, where a provider would be held liable for third-party content only if it knew or should have known about the unlawful content.²⁵¹

- 91 The proposals to reform Section 230 are a consequence of the fact that the current provisions (or at least their interpretation by the Courts) affording immunity to online service providers no longer reflect the realities of how online service providers operate nowadays compared to when CDA was enacted more than twenty years ago. They also suggest a growing dissatisfaction with the online service providers' content moderation policies. Furthermore, it is evident for some that the broad immunity afforded to online service providers enabled them to act in bad faith contrary to the requirements of the Good Samaritan rule.

- 92 The approach to voluntary content moderation measures in Article 7 of the DSA diverges from Section 230(c)(2)(A) in that they are more explicit regarding the standards of acting in good faith and in a diligent manner, and with due regards to the fundamental rights of users. However, the proposals to amend Section 230(c)(2)(A) tend to align with the requirements of acting in good faith in the DSA. Specifically, the proposals seek to define objectionable content and the good faith covenant as acting in an objective and non-discriminatory manner, as it has been interpreted in a few cases by the US Courts. The proposed definitions would prevent removal decisions to be animated by pretextual, discriminatory or fraudulent motives, often inconsistent with their terms of service. Some recommendations to amend Section 230 would align the test of Section 230(c)(1) to that in Article 6 of the DSA which is based on whether the service provider

Jordan in June 2021.

241 CRS, *supra* note 92 ("One conception of these two provisions is that Section 230(c)(1) applies to claims for content that is "left up,") See also Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87 ("the statute suggests that if a company unknowingly leaves up illegal third-party content, it is protected from publisher liability by §230(c)(1)") and *supra* note 186 and the accompanying text.

242 CRS, *supra* note 92 ("In practice, however, courts have also applied Section 230(c)(1) to "take down" claims"). See also Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87 ("This modest understanding is a far cry from what has prevailed in court [...] courts have relied on policy and purpose arguments to grant sweeping protection to Internet platforms").

243 PACT Act, S. 4066, 116th Cong. § 6 (2020).

244 Texas bill HB20, <<https://capitol.texas.gov/BillLookup/History.aspx?LegSess=872&Bill=HB20>>, accessed 17 March 2024.

245 The Fifth Circuit did not consider whether the law is preempted by Section 230.

246 Goldman, *supra* note 113.

247 Danielle Keats Citron and Benjamin Wittes, 'The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity', (2017) 86 Fordham L. Rev. 401, <<https://ir.lawnet.fordham>.

[edu/flr/vol86/iss2/3](https://www.fordham.edu/flr/vol86/iss2/3)>, accessed 17 March 2024.

248 Rustad and Koenig, *o.c.*

249 *Cubby, Inc. v. CompuServe Inc.*,

250 Meeran, *o.c.*

251 *Ibid.*

has actual knowledge of the illegality of content.²⁵²

- 93 The proposals advocate for more transparency when removing content by attaching certain requirements to objectionable content and good faith covenant and by requesting online service providers to be more transparent in their terms of service. The DSA already covers transparency obligations over voluntary content moderation, including for the use of automated tools.²⁵³ Such transparency requirements would ensure that voluntary content moderation measures have met the requirements of objectivity, proportionality, and non-discrimination. Additionally, they would verify that the safeguards of limiting errors and avoiding unjustifiable removal of content have been implemented.

E. Conclusions

- 94 The purpose of this research paper was to provide a comparative analysis of online service providers' liability exemptions when undertaking good faith voluntary content moderation measures in the EU and the US. The objective was to determine to what extent the provisions in the two jurisdictions allow online service providers to keep their immunity, while at the same time achieving the objective of combating illegal and objectionable content online. The research paper has shown that under a narrow interpretation of Section 230(c)(1) CDA, both Section 230(c)(1) and Article 6(1)(b) of the DSA apply to online service providers that unknowingly host third-party illegal content. As for immunity for voluntary content moderation in Section 230(c)(2)(A) and Article 7 of the DSA the language of the statute suggests that both provisions apply to online service providers that remove or restrict access to illegal or objectionable content in good faith. In this respect, this research paper has shown that both provisions require (i) a nexus between liability exemption and the action of moderating content,²⁵⁴ (ii) a good faith requirement which in both jurisdictions seems to be understood as being an objective standard, implicitly requiring a non-discriminatory approach, (iii) a decision to remove content that is either manifestly illegal or based on a reasonable belief that it is objectionable.

- 95 Under the DSA, the effectiveness of applying

252 See Rustad and Koenig, o.c., proposing to reform Section 230 so that online service providers are liable only if they have actual knowledge "and fail to expeditiously disable access to the posted illegal content". See also *supra* note 251.

253 DSA, Recital 66, Article 15.

254 See *supra* note 119.

these standards will determine the online service providers' eligibility for liability exemptions. Whether taking a more explicit stance on these standards will effectively fight illegal content online and serve as the advocate for liability exemptions will become clearer once the jurisprudence on voluntary good faith moderation measures under DSA will mature. What we can learn from the US is that open terms such as 'good faith' or 'otherwise objectionable' content "invites judges to introduce their own normative values into the consideration".²⁵⁵ Given that good faith and diligence requirements in Article 7 of the DSA are standards, it is likely that the CJEU may still have to determine what acting in good faith and diligent manner requires in the circumstances of the specific case, similar to how it has been done in the US.

- 96 Under a broad interpretation of Section 230(c)(1), online service providers have enjoyed immunity even when they knew about the illegal activity, "deliberately left up unambiguously unlawful content"²⁵⁶, and encouraged or facilitated illegal content.²⁵⁷ By relying on Section 230(c)(1) to protect online service providers from any cause of action, the defendants prevailed in cases of sex trafficking of minors, illegal sale of guns, defective sale of products and even the encouragement of terrorist acts.²⁵⁸ It also reduced their incentives to moderate content and fight illegal content online. This, in turn, is one of the reasons prompting calls for a reform of Section 230. The proposed reforms reveal not only the shortcomings in the Courts' interpretation of the statute, but they also suggest an alignment with some of the requirements attached to the good faith and diligence standards in the DSA, such as objectivity and non-discrimination.
- 97 The few cases dealt under Section 230(c)(2)(A) suggest that bad faith content moderation will lead to a loss of immunity, whereas the cases dealt under Section 230(c)(1) suggest that bad faith content moderation can still guarantee immunity depending on the Court of Appeal that examines the case. Since Section 230(c)(1) does not require a good

255 Goldman, *supra* note 120.

256 Danielle Keats Citron and Marie Anne Franks, 'The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform' (2020), 2020(3) University of Chicago Legal Forum, <<https://chicagounbound.uchicago.edu/uclf/vol2020/iss1/3>>, accessed 17 March 2024.

257 Klapper, o.c., page 1258 and 1305 and referring to *Doe v. Backpage.com, LLC*, 817 F.3d 12, 22 (1st Cir. 2016), where the defendant prevailed under Section 230(c)(1) even though it facilitated illegal conduct.

258 Franks, o.c.

faith action and extends its protection to all types of action, defendants prevailed in Courts by invoking Section 230(c)(1) and thus bypassing the good faith standard required under Section 230(c)(2)(A). Such a broad interpretation diverges from the conditions for liability exemptions in the DSA which require that the online service providers do not have actual knowledge of the illegal content and when they do, they act promptly to remove it.

the other is a matter of policy choice.

98 Interpreting Section 230(c)(1) to apply to any cause of action, including any removal decisions, allows service providers to bypass the good faith²⁵⁹ standard in Section 230(c)(2)(A) or to benefit from immunity even when knowingly facilitating illegal activity online. But providing sweeping immunity for any type of actions,²⁶⁰ under the pretext of promoting unfettered speech on the internet,²⁶¹ does not align with Congress's original intent when enacting Section 230 to protect minors from indecent material on the internet. It also reduces the incentives to moderate and fight illegal content online. The DSA aims to strike a balance between protecting various interests and fundamental rights, including users' freedom of expression and other rights enshrined in the EU Charter and maintaining the service providers' liability exemptions for voluntary content moderation measures. Whether this balance will effectively fight illegal content online will require further examination. The issue could be potentially clarified by the CJEU once it has the opportunity to examine a case on liability exemptions and voluntary content moderation measures under the DSA.

99 Liability exemptions for lack of *actual knowledge* has also been advocated as a measure to reform Section 230,²⁶² reflecting the common law distributor liability upheld in *Cubby*. Although such proposal may be controversial in many respects for the supporters of Section 230,²⁶³ the knowledge standard is nevertheless used for addressing copyright infringements under the DMCA and has been the pillar of the EU liability regime for over two decades. While the notice and take-down regime in the EU is more effective at fighting illegal content online, the US system of shielding online service providers for failure to remove illegal content is more effective at protecting free speech. Choosing one regime over

259 *Murphy v. Twitter, Inc.*, 2021 WL 221489 (California Appeal Court, Jan. 22, 2021).

260 Statement of Justice Thomas in *Malwarebytes v. Enigma*, *supra* note 87.

261 See *supra* note 235.

262 See *supra* note 252.

263 *Meeran, o.c.*

How the AI Act Applies to E-Commerce

by Elif Cansu Yaşar *

Abstract: This article researches the following questions: To what extent do the provisions of the AI Act apply to e-commerce companies that use AI? To what extent is this in line with the objectives of the AI Act, considering the risks in relation to the use of AI for e-commerce?

The AI Act has a risk-based approach. For e-commerce companies to comply with the AI Act, it is important to know how applicable it is to their activities.

Some e-commerce activities might be under the prohibited practices in the AI Act. However, most of the e-commerce activities are not entirely regulated by it since they are not classified as high-risk AI systems under the AI Act. Since e-commerce can pose serious risks, especially regarding manipulation and discrimination, the AI Act leaves a regulatory gap in the use of AI in e-commerce.

Keywords: AI; AI Act; E-Commerce

© 2024 Elif Cansu Yaşar

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Elif Cansu Yaşar, How the AI Act Applies to E-Commerce, 15 (2024) JIPITEC 38 para 1.

A. Introduction

1 E-commerce made its appearance almost simultaneously with the rise of the internet. Because of the risks and challenges brought by economic growth and advancing technologies, it soon attracted regulatory attention. E-commerce has been regulated in various aspects under the EU law since A European Initiative in Electronic Commerce in 1997¹.

2 In recent years, online shopping has gained popularity, with the rise of online platforms and more recently, with the Covid-19 pandemic. Europe

E-commerce's 2022 report states that "in 2021, total European e-commerce grew to €718bn with a growth rate of 13%"² and the changes in the sector, such as digitalisation, require businesses to invest more in the future to keep up with them.³ With this digitalisation trend, the use of AI in e-commerce activities such as big data analytics, data management, customer insights, personalisation, marketing, custom-made advertisements and targeting has also increased.⁴

3 Currently, in addition to the Directive on Electronic

* PhD Candidate, Radboud Business Law Institute (OO&R), Radboud University, Nijmegen (The Netherlands). cansu.yasar@ru.nl

1 Commission, 'A European Initiative in Electronic Commerce', (Communication) COM (97) 157 final

2 Ecommerce Europe, EuroCommerce for retail & wholesale, 'European E-Commerce Report' (2022) <https://ecommerce-europe.eu/wp-content/uploads/2022/06/CMI2022_FullVersion_LIGHT_v2.pdf> accessed 12 October 2023, 2

3 Ecommerce Europe (n 2), 3

4 Ecommerce Europe (n 2), 2, 3, 20 24, 28, 34, 38, 48, 55, 58, 82

Commerce,⁵ there are EU rules regulating various aspects of e-commerce activities. This includes rules in the areas of product safety and liability, fundamental rights⁶ and consumer rights.⁷ In principle, these rules are fully applicable regardless of the involvement of AI.⁸ For example, if personal data is processed through the use of AI, the GDPR applies. Most notably, Article 22 of the GDPR specifically regulates “automated individual decision-making, including profiling”.⁹

- 4 The Shaping Europe’s Digital Future program aims to ensure that EU rules are technologically, economically, and socially compatible with the digital

age.¹⁰ This includes the Digital Services Act¹¹ and the Digital Markets Act.¹² Another important regulation is the Regulation laying down harmonised rules on artificial intelligence (AI Act).¹³ The AI Act adopts a risk-based approach and prohibits, regulates, or leaves unregulated certain AI practices depending on their classification into risk categories. From the e-commerce perspective, some of the rules in the AI Act such as those on the prohibited practices may overlap to some extent with other legislation. However, The AI Act differs from the previous instruments since it introduces transparency rules for certain AI systems.

- 5 It is important for practitioners and legal scholars to examine the AI Act from the e-commerce perspective. E-commerce companies which increasingly use AI in their activities must know to what extent this new regulation applies to them. In order to understand their obligations, they must know which risk category they belong to, their roles under the AI Act, and which of their activities require more legal attention. For legal scholars and legal practitioners, it is important to know the AI techniques used in e-commerce, purposes and reasons for using different techniques so that they can evaluate the legal implications of these techniques and see to what extent the AI Act addresses them.

5 Directive 2000/31/EC of the European Parliament And of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

6 Such as Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119, 04.05.2016 (GDPR) in data protection and privacy

7 Such as 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/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 (OJ L 149, 11.6.2005, p. 22–39) (Unfair Commercial Practices Directive) and Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council OJ L 304, 22.11.2011, p. 64–88 (Consumer Rights Directive)

8 European Commission, ‘White Paper on Artificial Intelligence - A European approach to excellence and trust’ COM (2020) 65 final, 13

9 About AI and the application of the GDPR, see also: Sebastião Barros Vale, ‘GDPR and the AI Act Interplay: Lessons from FPF’s ADM Case-Law Report’ (Future of Privacy Forum, 3 November 2022) <<https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/>> accessed 12 October 2023

10 Commission, ‘Shaping Europe’s Digital Future’ (19 February 2020) <https://commission.europa.eu/document/download/84c05739-547a-4b86-9564-76e834dc7a49_en?filename=communication-shaping-europes-digital-future-feb2020_en.pdf> accessed 6 March 2024

11 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L 277, 27.10.2022

12 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265, 12.10.2022 (Digital Markets Act)

13 European Parliament, ‘European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))’ (Texts Adopted) P9_TA(2024)0138

- 6 The risks that may arise from the use of AI in e-commerce have previously been examined from data protection and privacy law,¹⁴ consumer law,¹⁵ and discrimination law¹⁶ perspectives. However, although there has been literature about how the AI Act regulates issues such as manipulation,¹⁷

discrimination,¹⁸ and data protection,¹⁹ current literature has not dealt with the question of whether the AI Act applies to e-commerce companies and what does the AI Act mean for e-commerce. Examining the use of AI in e-commerce from an AI Act perspective therefore complements earlier work in the literature.

- 7 This article researches the following questions: *To what extent do the provisions of the AI Act apply to e-commerce companies that use AI? To what extent is this in line with the objectives of the AI Act, considering the risks in relation to the use of AI for e-commerce?* To answer this question, this article will first determine the extent to which the AI Act applies to the use of AI in e-commerce activities. Then, it will assess whether the risks of using AI in e-commerce should be regulated under the AI Act or whether the protection against these risks in existing EU legislation is sufficient. This article finds out that some activities of e-commerce companies might be prohibited under the AI Act. However, the prohibited practices under the AI Act require many conditions that will not always be met. E-commerce activities do not fall into the high-risk classification under the AI Act, which includes a large part of the obligations. However, the transparency obligations for certain AI systems apply to e-commerce activities.
- 8 Within the scope of the article, “e-commerce” refers to the activities of companies that sell their own products on their websites and on platforms. The online platforms that facilitate these e-commerce companies are outside of the definition. This article is limited to B2C e-commerce activities of companies that sell physical goods online. However, the analysis may also be relevant for services. The AI Act may intersect with other legislation. Such as the GDPR, especially in the provisions related to data quality.

14 European Parliament, Directorate-General for Parliamentary Research Services, Giovanni Sartor, Francesca Lagioia, ‘The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence’ Panel for the Future of Science and Technology PE 641.530 – June 2020; Jozef Andraško, Matúš Mesarčík, Ondrej Hamulák, ‘The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework’ (2021) 36 AI & Society 623

15 Marco Lippi and others, ‘The Force Awakens: Artificial Intelligence for Consumer Law’ (2020) 67 Journal of Artificial Intelligence Research 169; Agnieszka Jabłonowska and others, ‘Consumer law and artificial intelligence: challenges to the EU consumer law and policy stemming from the business’ use of artificial intelligence : final report of the ARTSY project’ (2018) EUI Department of Law Research Paper No. 2018/11 <<https://ssrn.com/abstract=322805>> accessed 16 March 2024

16 Frederik Zuiderveen Borgesius, ‘Discrimination, Artificial Intelligence, and Algorithmic Decision-Making’ (Council of Europe, Directorate General of Democracy, 2018); Frederik Zuiderveen Borgesius, Joost Poort, ‘Online Price Discrimination and EU Data Privacy Law’ (2017) Journal of Consumer Policy

17 Huixin Zhong, Eamonn O'Neill, Janina A. Hoffmann, ‘Regulating AI: Applying insights from behavioural economics and psychology to the application of article 5 of the EU AI Act’ (The 38th Annual AAAI Conference on Artificial Intelligence, Canada, 20 February 2024 - 27 February 2024 <<https://arxiv.org/pdf/2308.02041.pdf>> accessed 16 March 2024; Matija Franklin and others, ‘Missing Mechanisms of Manipulation in the EU AI Act’ (The International FLAIRS Conference Proceedings 35, 4 May 2022) <<https://journals.flvc.org/FLAIRS/article/view/130723>> accessed 16 March 2024; Risto Uuk, ‘Manipulation and the AI Act’ (Future of Life Institute, 18 January 2022) <https://futureoflife.org/wp-content/uploads/2022/01/FLI-Manipulation_AI_Act.pdf> accessed 16 March 2024

18 Marvin van Bakkum, Frederik Zuiderveen Borgesius, ‘Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?’ (2023) 48 Computer Law & Security Review 105770; Salih Tayfun İnce, ‘European Union Law and Mitigation of Artificial Intelligence-Related Discrimination Risks in the Private Sector: With Special Focus on the Proposed Artificial Intelligence Act’ (2021) 71 Annales de la Faculté de Droit d’Istanbul 71

19 Barros Vale (n 9); Raphaël Gellert, ‘The role of the risk-based approach in the General data protection Regulation and in the European Commission’s proposed Artificial Intelligence Act: Business as usual?’ (2021) 3 Journal of Ethics and Legal Technologies 15; Joanna Mazur, ‘Artificial Intelligence vs Data Protection: How the GDPR Can Help to Develop a Precautionary Regulatory Approach to AI?’ in Angelos Kornilakis and others (eds), *Artificial Intelligence and Normative Challenges: International and Comparative Legal Perspectives* (Springer, Cham 2023)

Although the AI Act may include provisions on the use of (both personal and non-personal) data, it focuses more on the safety of AI systems. Data protection issues are regulated by the GDPR. Therefore, in line with the focus on the AI Act, this article will focus on the risks and safety issues when using AI, rather than the data protection issues. The AI Act may also intersect with the Unfair Commercial Practices Directive regarding the prohibited practices and might introduce complementary rules to issues that are already regulated in consumer law. However, as this article seeks to find out whether the AI Act is applicable to e-commerce, an analysis of consumer law falls outside of its scope.

- 9 Section B explores how AI can be used in e-commerce activities. Section C examines the risks arising from these activities. Section D analyses the AI Act and its risk-based approach in relation to the risks of e-commerce activities. Since the AI Act brings different requirements for different risk levels, applicability will be analysed separately for each risk level.
- 10 After the European Commission's Proposal in 2021,²⁰ the Council of the European Union published its General Approach on 6 December 2022, and the European Parliament adopted its Negotiating Position on 14 June 2023. They have reached a provisional agreement on 9 December 2023. The Compromise Text was published on 26 January 2024.²¹ On 13 March 2024, the European Parliament adopted the AI Act and in May 2024, it was approved by the Council. Unless stated otherwise, this article refers to the Adopted Text by the European Parliament.²²

20 Commission, 'Proposal for A Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM/2021/206 final (AI Act).

21 Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement' (Note) 5662/24

22 European Parliament, 'European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))' (Texts Adopted) P9_TA(2024)0138

B. AI Use in E-Commerce

- 11 Artificial Intelligence is a technology that is difficult to capture in a precise definition. However, it can be explained in terms of its function. It could be defined as "technologies programmed to analyse the world around them and take action to achieve specific goals",²³ or as "a collection of technologies that combine data, algorithms and computing power".²⁴
- 12 AI systems can be used in e-commerce in many ways. The uses can be broadly divided into the analysis of data, making business decisions according to the inferences from the collected data, and using AI during the sales or after sales. Since these systems often interact with each other, it is not possible to clearly distinguish the phases. Personalisation, for instance, can be used in many stages of e-commerce activities such as marketing, sales, and after-sales. However, considering the business steps of an e-commerce company, the use of AI can be examined as follows.

I. Customer Insights, Predictions, and Pricing

- 13 Firstly, businesses can use AI to gain more insight on existing or potential customers. Analysing customer behaviour (such as purchasing behaviour) is crucial for e-commerce businesses. It allows them to shape their services accordingly.²⁵ AI may answer questions such as: do customers compare prices before buying or how likely are they to make a purchase? Customer behaviour analysis can be used to identify online browsing and purchase behaviours of customers.²⁶ Companies can learn what kind of products customers search for, how much time they spend on these pages, their buying patterns,

23 European Commission, 'Artificial Intelligence' (Shaping Europe's digital future, last update 31 august 2022) <<https://digital-strategy.ec.europa.eu/en/policies/artificial-intelligence>> accessed 12 October 2023

24 COM (2020) 65 final, 2

25 Lucas Micol Policarpo and others, 'Machine learning through the lens of e-commerce initiatives: An up-to-date systematic literature review' (2021) 41 Computer Science Review 100414, 2

26 Countants, 'Why Consumer Behavior Analysis Is So Relevant to the eCommerce business?' (Medium, 6 January 2020) <<https://medium.datadriveninvestor.com/why-consumer-behavior-analysis-is-so-relevant-to-the-e-commerce-business-8f49c250ca9c>> accessed 12 October 2023

and how they react to personalisation or discounts.²⁷ Customer behaviour on websites and mobile apps can be analysed for this,²⁸ as well as email behaviour such as whether emails have been read or redirected customers to the website.²⁹

- 14 Companies can make use of customer segmentation to group customers according to various attributions such as age, location, gender, and shopping patterns,³⁰ and offer personalised services to different groups. Companies can use predictive analytics to understand the past behaviours of customers and make predictions about their preferences in the future.³¹ Data such as “past click through behaviour, shopping history, browsing patterns, product preferences” can be analysed to answer questions such as how much money customers are likely to pay for a product or to make personalised recommendations.³² Churn prediction can be used to retain customers by noticing if customers stop their regular purchases and offering personalised discounts to them.
- 15 AI can also be used in pricing strategies. Dynamic pricing can be beneficial to increase sales since it allows businesses to determine competitive prices and reach more customers.³³ AI systems can take different factors into account when using dynamic pricing. They can use data about the company rather

than the customer, such as supply and demand or the fees of other companies.³⁴ They can also use data about customers such as age, location, devices they use or their shopping habits.³⁵ Personalised offers and personalised pricing can help to increase sales by making the customer feel more recognised by the company.³⁶

II. Marketing

- 16 Once companies analyse the data and know more about their customers, they can benefit from using AI in promoting their products to their customers. Firstly, AI can determine the most suitable time for an advertisement, or the most effective channel, such as email, social media, or phone notifications.³⁷ Email communications with customers can be personalised and can be used for various purposes. It is possible to send a reminder email for an abandoned cart, for personalised offers or announcements.³⁸
- 17 Recommender systems can be widely used for marketing. It is often possible to implement them according to the different needs and purposes of companies. Depending on the implemented technique, data such as user feedback, user ratings, number of purchases, item price, purchase history, browsing history or product characteristics can be used for making recommendations.³⁹ Personalisation can increase sales by offering personalised recommendations to customers who are not sure what they are searching for, or who find it difficult to make a decision because of the number of products

²⁷ *Ibid*

²⁸ Countants, ‘How Artificial Intelligence is transforming the E-commerce Industry’ (Medium, 10 May 2019) <<https://medium.com/@Countants/how-artificial-intelligence-is-transforming-the-e-commerce-industry-countants-scalable-custom-73ae06836d35>> accessed 12 October 2023

²⁹ Countants, ‘Why Consumer Behavior Analysis Is So Relevant to the eCommerce business?’ (n 26)

³⁰ ProjectPro, ‘10 Machine Learning Projects in Retail You Must Practice’ (ProjectPro, last updated 12 October 2023) <<https://www.projectpro.io/article/machine-learning-projects-in-retail-and-ecommerce/498>> accessed 12 October 2023

³¹ IQLECT, ‘The Importance of Predictive Analytics for E-commerce Stores’ (Medium, 14 November 2018) <<https://medium.com/swlh/the-importance-of-predictive-analytics-for-e-commerce-stores-d7ef0ce2d32e>> accessed 12 October 2023

³² *Ibid*

³³ Cem Dilmegani, ‘Ecommerce Dynamic Pricing in 2023: Guide & Examples’ (AI Multiple, Published 25 October 2021, Updated 12 October 2023) <<https://research.aimultiple.com/dynamic-pricing-ecommerce/>> accessed 12 October 2023

³⁴ Cem Dilmegani, ‘Ultimate Guide to Dynamic Pricing in 2023: Roadmap & Vendors’ (AI Multiple, Updated 4 August 2023) <<https://research.aimultiple.com/dynamic-pricing/>> accessed 12 October 2023

³⁵ *Ibid*

³⁶ ‘Ecommerce Personalization: How to Make Each Customer Feel Like a VIP’ (Big Commerce) <<https://www.bigcommerce.com/articles/ecommerce/personalization/>> accessed 12 October 2023

³⁷ ‘How to leverage AI in marketing: three ways to improve consumer experience’ (Deloitte) <<https://www2.deloitte.com/si/en/pages/strategy-operations/articles/AI-in-marketing.html>> accessed 12 October 2023

³⁸ Brittany Shulman, ‘How to launch a successful personalized marketing strategy’ (Bazaarvoice, 4 January 2022) <<https://www.bazaarvoice.com/blog/how-to-launch-a-successful-personalized-marketing-strategy/#h-what-is-personalized-marketing>> accessed 12 October 2023

³⁹ *Ibid*, 81-82 Table 1

to choose from.⁴⁰ Customer loyalty programs with personalised rewards can increase the loyalty of customers to the seller.⁴¹

III. Sales and After-Sales

- 18 AI can be used in sales and after-sales to provide convenience to the customers and the company.
- 19 Search-related AI applications help customers find what they are looking for more easily and therefore, increase sales. Using autocomplete in search buttons can help customers find what they are looking for, suggest the products they missed, or show them relevant results in case they misspell the product name.⁴² Search results can be personalised, or recommendations for certain groups or locations can be used.
- 20 Voice search allows customers to find what they are looking for more easily, without having to type anything.⁴³ With visual search, customers can take a photo and search for similar products. Product tags can be used in images so that the customers can purchase the different products in one image.⁴⁴ With Augmented Reality, customers can virtually try on products such as clothes and cosmetics, and they can see how furniture or home decoration will look in their homes before purchasing them.⁴⁵

21 Chatbots can answer product-related questions, act as an always-available customer service tool, or make product recommendations.⁴⁶ This reduces the company's workload and increases the customer satisfaction by enabling them to reach the company at any time.

22 Sentiment analysis can be used to better understand purchasing decisions or the overall opinion of customers. By analysing the product reviews on the e-commerce website or social media with Natural Language Processing (NLP) techniques, companies can have an insight into the customers' view of the company and the product and make future business plans accordingly.⁴⁷ NLP can also be used for intelligent search, which helps customers to find the products they are searching for by making accurate predictions.⁴⁸ These techniques can be used together with personalisation and recommendations, and therefore be very effective for the business.⁴⁹

C. Risks of Using AI In E-Commerce

23 AI systems entail various risks for both customers and companies.⁵⁰ On one hand, algorithmic decision-making can leave customers vulnerable, and customers might worry that AI will have unforeseen effects and that it can be used with malicious intent. Although there are regulations protecting the fundamental rights of individuals, the use of AI can make their implementation more difficult due to some specific features of it.⁵¹ On the other hand, companies might worry about the (uncertain)

40 'Ecommerce Personalization: How to Make Each Customer Feel Like a VIP' (Big Commerce) <<https://www.bigcommerce.com/articles/ecommerce/personalization/>> accessed 12 October 2023

41 *Ibid*

42 Jon Silvers, '15 Best Practices for 2022 to Improve E-commerce Site Search' (Algolia, 31 July 2023) <<https://www.algolia.com/blog/ecommerce/15-best-practices-for-ecommerce-on-site-search/>> accessed 12 October 2023

43 Nick Brown, 'How to Optimize Voice Search Feature for Your Ecommerce Store' (Big Commerce) <<https://www.bigcommerce.com/blog/voice-search-ecommerce/>> accessed 12 October 2023

44 'How Visual Search has transformed the modern shopping experience', (Visenze, 21 March 2019) <<https://www.visenze.com/blog/2019/03/21/how-visual-search-has-transformed-the-modern-shopping-experience/>> accessed 12 October 2023

45 Helen Papagiannis, 'How AR Is Redefining Retail in the Pandemic' (Harvard Business Review, 7 October 2020) <<https://hbr.org/2020/10/how-ar-is-redefining-retail-in-the-pandemic>> accessed 12 October 2023

46 Cem Dilmegani, 'Sales Chatbots in 2023: Top Use Cases & Best Practices' (AI Multiple, Updated 9 October 2023) <<https://research.aimultiple.com/sales-chatbot/>> accessed 12 October 2023

47 Begüm Yılmaz, 'E-Commerce Sentiment Analysis in 2023: Top 3 Applications' (AI Multiple, Updated 8 September 2023) <<https://research.aimultiple.com/ecommerce-sentiment-analysis/>> accessed 12 October 2023

48 'The Future of Shopping: Natural Language Processing Applications in E-Commerce' (Defined AI, 29 July 2020) <<https://www.defined.ai/blog/the-future-of-shopping-natural-language-processing-applications-in-e-commerce/>> accessed 12 October 2023

49 *Ibid*

50 EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) para 2

51 COM (2020) 65 final, 10

implications of relevant legal provisions when AI is used.⁵² However, the AI Act focuses on the risks of AI systems for natural persons. Therefore, this article will focus only on these risks.

- 24 Since the AI Act has a risk-based approach, its obligations depend on the risks of an AI system. This section will examine the risks of AI use in e-commerce independently from the provisions of the AI Act. The most important risks for customers brought by the use of AI in e-commerce can be divided into two main groups. These are manipulation and discrimination risks.

I. Manipulation

- 25 Manipulation can be used to sell certain products, sell more products or trigger impulse buying. Companies often use manipulation in marketing to influence customers' decision-making by deceiving them or "playing on a vulnerability".⁵³ Not every technique that drives customers to buy a particular product is manipulative. These can also be persuasion methods based on accurate information.⁵⁴ However, especially with the developing technology, it became easier to manipulate customers through methods such as deliberately hiding some information or presenting it to customers at a certain time.⁵⁵
- 26 Manipulation can be in extreme forms, such as dark patterns. Dark patterns are design choices intended to deceive people with false suggestions such as that various prices will only stay this way for a certain period or that there is less product in stock than there actually is.⁵⁶ In addition to the AI Act, various EU legislation such as the Unfair Commercial Practices Directive and the GDPR include rules that may apply to certain aspects of dark patterns. For example, the Unfair Commercial Practices Directive

protects customers against practices that "impair consumer's ability to make an informed decision".⁵⁷ In cases where personal data is involved, the GDPR may provide protection against dark patterns with rules such as the fairness principle⁵⁸ and privacy by design and default obligation.⁵⁹ However, the European Parliament found that the existing legislation on addictive design choices such as dark patterns did not provide sufficient protection to consumers and called on the Commission to close the regulatory gaps regarding the "addictive design of online services".⁶⁰

- 27 Manipulation can be used for targeting vulnerable groups and exploiting their vulnerability. It also has negative effects on the average customer. Manipulation can have economic or psychological consequences. It can cause economic damage to customers by making them buy products that they did not actually want to buy.⁶¹ Moreover, it can harm "autonomy" by affecting people's right to make their own decisions about themselves.⁶²
- 28 AI and especially personalisation can be used by e-commerce companies to trigger impulse buying. Impulsive buying refers to the inability to resist buying.⁶³ Impulsive buying can be stimulated by personalisation. Even though personalisation can be very beneficial for both customers and companies, over-personalisation also has downsides. It can be used to make customers spend more money rather than benefit them.⁶⁴ If customers, especially

52 *Ibid*, 9

53 Shlomo Sher, 'A Framework for Assessing Immorally Manipulative Marketing Tactics' (2011) 102 *Journal of Business Ethics* 97, 99, 100

54 Gilles N'Goala, 'Opportunism, transparency, manipulation, deception and exploitation of customers' vulnerabilities' in Bang Nguyen, Lyndon Simkin, Ana Isabel Canhoto (eds) *The Dark Side of CRM Customers, Relationships and Management* (Routledge 2015)

55 Tal Zarsky, 'Privacy and Manipulation in the Digital Age' (2019) 20(1) *Theoretical Inquiries in Law* 157, 158

56 Ray Sin and others, 'Dark patterns in online shopping: do they work and can nudges help mitigate impulse buying?' (2022) *Behavioural Public Policy* 1, 3

57 Unfair Commercial Practices Directive art 2(e), 5(2)

58 GDPR art 5(1)(a)

59 GDPR art 25; For an evaluation of various EU legislation regarding dark patterns see: Inge Graef, 'The EU Regulatory Patchwork for Dark Patterns: An Illustration of an Inframarginal Revolution in European Law?' TILEC Discussion Paper No. 2023-07, (Tilburg Law School Research Paper)

60 European Parliament, 'Addictive design of online services and consumer protection in the EU single market European Parliament resolution of 12 December 2023 on addictive design of online services and consumer protection in the EU single market (2023/2043(INI))' (Texts Adopted) P9_TA(2023)0459

61 Zarsky, 'Privacy and Manipulation in the Digital Age' (n 55) 172, 173

62 *Ibid*, 173, 174

63 Dennis W. Rook, 'The Buying Impulse' (1987) 14 *The Journal of Consumer Research* 189, 191

64 Aniko Hannak and others, 'Measuring Price Discrimination

from vulnerable groups cannot adequately protect themselves from these techniques designed to make them spend more, this can lead to overspending and negative economic effects.

II. Discrimination

- 29 Another important problem that can arise with the use of AI is discrimination. In e-commerce, discrimination may lead to price discrimination, limited or no access to goods/services, or differences in the quality of the products. People might be subjected to discrimination as a result of the inferences made from their shopping habits or age, gender, or zip code.
- 30 Especially the opacity of some AI systems can make it difficult to determine whether discrimination exists and, if so, on what basis.⁶⁵ Discrimination can be direct or indirect. Direct discrimination is the discrimination of people over a “protected characteristic” such as gender or race.⁶⁶ Indirect discrimination is when an application that appears neutral at first discriminates over any protected characteristic.⁶⁷ In e-commerce, it is more likely to encounter indirect discrimination than direct discrimination. For example, it is possible that more people from a certain racial group live in a particular zip code area.⁶⁸ Different results that people may see on websites are more likely to be due to the zip code, rather than racial origin.
- 31 Discrimination can be intentional or unintentional. If organisations have the intention to discriminate, they can choose factors such as “target variable” and “class label” that will affect the AI’s decision-making according to their intentions.⁶⁹ The target variable means to express the result that the organisation wants to reach in a technical way that

the algorithms can understand.⁷⁰ Class labels are labelling of the data used to reach these results.⁷¹ For example, in e-commerce, the target variable could be finding the type of customer most likely to buy a product. To reach this result, different variables can be considered such as the number of purchases the customers have made, the products they have purchased, or the amount of money they have spent. Companies can choose which of these variables to consider. However, the choices made in this target variable and class labels can also cause unintentional indirect discrimination.⁷² In addition, if the training data used in an AI system are biased, the AI system might reflect this bias.⁷³

- 32 E-commerce companies can constantly change their prices and show different prices to certain groups or even individuals. This is because a company would like to charge the highest price customers are willing to pay for a particular product.⁷⁴ The more data companies have about customers, the easier it gets to determine the highest price customers will pay for a product.⁷⁵ However, seeing different prices on websites cannot always be attributed to personalisation, and there might be different reasons such as the stock status, updates to the website or technical reasons.⁷⁶ A study on this subject found that only one of the ten retail websites they examined showed different prices to iOS and Android users, and the price difference was very low in practice.⁷⁷ Due to the opacity of AI, it is difficult to determine whether the different prices seen on e-commerce sites are based on personalisation. There may also be commercial or technical reasons for these different prices.

- 33 Since companies use personal data such as IP

and Steering on E-commerce Web Sites’ (2014) IMC ‘14: Proceedings of the 2014 Conference on Internet Measurement Conference 305, 305

- 65 Zuiderveen Borgesius, ‘Discrimination, Artificial Intelligence, and Algorithmic Decision-Making’ (n 16), 10
- 66 *Ibid*, 18
- 67 *Ibid*, 19
- 68 *Ibid*, 13
- 69 *Ibid*, 10,11; Solon Barocas, Andrew D. Selbst, ‘Big Data’s Disparate Impact’ (2016) 104 California Law Review 671, 678, 692

-
- 70 Barocas, Selbst (n 69), 678

- 71 *Ibid*, 678

- 72 Zuiderveen Borgesius, ‘Discrimination, Artificial Intelligence, and Algorithmic Decision-Making’ (n 16), 11

- 73 *Ibid*, 10, 12

- 74 Marc Bourreau, Alexandre de Streel, Inge Graef, ‘Big Data and Competition Policy: Market power, personalised pricing and advertising’ (Project Report, Centre on Regulation in Europe, 2017), 39

- 75 *Ibid*, 40

- 76 Aniko Hannak and others, ‘Measuring Price Discrimination and Steering on E-commerce Web Sites’ (2014) IMC ‘14: Proceedings of the 2014 Conference on Internet Measurement Conference 305, 307

- 77 *Ibid*, 315,316

addresses and cookies to identify customers, these practices mostly fall within the scope of data protection rules.⁷⁸ However, price discrimination also has economic effects. It can have a positive economic impact on companies as it allows them to charge more for the same product than people who are willing to pay more. On the other hand, considering the “distribution of welfare” between companies and customers, the economic consequences will be negative for customers.⁷⁹

D. AI Act and the Risk Based Approach

- 34 The AI Act lays down “harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems (‘AI systems’) in the Union”⁸⁰ and aims to bring a “legal framework for trustworthy AI”.⁸¹ The specific objectives mainly focus on the safety of AI systems. On one hand, there are economic objectives such as strengthening the single market with safe AI and on the other hand, there are objectives related to the fundamental rights and Union values.⁸²
- 35 The responsibilities in the AI Act differ according to the roles and the risk levels. Therefore, it is important to identify the roles of e-commerce companies to find out to what extent the AI Act applies to them. If the companies develop their own AI systems, they shall be considered providers.⁸³ If they only use AI systems that are developed by others, they shall be considered deployers.⁸⁴
- 36 If an e-commerce company is a provider and places on the market or puts into service AI systems in the Union⁸⁵ or the “output produced by the system is used in the Union”,⁸⁶ it will be subject to the AI Act. If it is a deployer, it must be “located within the

Union”⁸⁷ or the “output produced by the system” must be “used in the Union”.⁸⁸

- 37 Chapter II explains the prohibited AI practices and the conditions and exemptions for these prohibitions (unacceptable risks). Chapter III covers the high-risk AI systems and explains the classification of AI systems as high risk (Section 1), requirements for high-risk AI systems (Section 2), obligations of providers and deployers of high-risk AI systems and other parties (Section 3), notifying authorities and notified bodies (Section 4), standards, conformity assessment, certificates, registration (Section 5). Chapter IV brings transparency obligations for providers and deployers of certain AI systems. The “certain AI systems” here is what we may see as a “limited risk” group. Finally, Chapter X introduces a mechanism to formulate codes of conduct for minimal or no-risk groups, which it mentions as “AI systems other than high-risk AI systems”.⁸⁹ It is possible to address the four levels of risks in the AI Act as “unacceptable risk, high risk, limited risk, and minimal or no risk” AI systems.⁹⁰
- 38 Section D.I will examine the manipulative practices and social scoring of the prohibited practices from the e-commerce perspective to find out whether e-commerce activities might be prohibited under the AI Act. To evaluate whether using AI in e-commerce is safe enough not to be subject to high-risk AI obligations of the AI Act, Section D.II will then compare the risks of e-commerce activities with the AI Act’s criteria in Article 7(2) to be considered a high-risk AI system. Sections D.III and D.IV will explain the meaning of limited and minimal risk groups for e-commerce.

I. Unacceptable Risk AI Systems: Prohibited Practices

- 39 The AI Act prohibits AI practices that could be classified under the unacceptable risk group. These practices include subliminal techniques,⁹¹ exploiting

78 Zuiderveen Borgesius, Poort, ‘Online Price Discrimination and EU Data Privacy Law’ (n 16), 357

79 *Ibid*, 354

80 AI Act art 1(2)(a)

81 AI Act Proposal Explanatory Memorandum, 1

82 AI Act Proposal Explanatory Memorandum, 3

83 AI Act art 3(3)

84 AI Act art 3(4)

85 AI Act art 2(1)(a)

86 AI Act art 2(1)(c)

87 AI Act art 2(1)(b)

88 AI Act art 2(1)(c)

89 AI Act art 95(1)

90 European Commission, ‘Regulatory framework proposal on artificial intelligence’ (Shaping Europe’s digital future, last update 20 June 2023) <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 12 October 2023

91 AI Act art 5(1)(a)

vulnerable groups,⁹² biometric categorisation systems based on special categories of personal data,⁹³ social scoring,⁹⁴ real-time remote biometric identification in publicly accessible spaces for law enforcement purposes,⁹⁵ risk assessments for criminal activities,⁹⁶ facial image scraping from CCTV footages,⁹⁷ and emotion inferences in workplace and education institutions.⁹⁸ The prohibited practices that are most likely to occur in e-commerce are the manipulative practices in Articles 5(1)(a) and 5(1)(b) and social scoring in Article 5(1)(c). These prohibited practices create risks in relation to manipulation and discrimination. The other prohibited practices in Chapter II of the AI Act will not be examined here.

1. Manipulative Practices

a.) Subliminal Techniques

- 40 The first prohibited practice in Article 5(1)(a) is the “placing on the market, putting into service or use of an AI system that deploys subliminal techniques”. Article 5(1)(a) requires using “subliminal techniques beyond a person’s consciousness or purposefully manipulative or deceptive techniques with the objective to or the effect of materially distorting a person’s or a group of persons’ behaviour by appreciably impairing the person’s ability to make an informed decision”, and significant harm to occur or be likely to occur because of this use.
- 41 As explained in section C.I, manipulation can be seen often in e-commerce activities, especially in marketing. Manipulative practices can be to hide some information from customers, to use misleading language, to mislead customers with “fake countdown timers”.⁹⁹ However, not every

technique to sell a product is manipulation and not every manipulation is covered by the prohibition in the AI Act. In order to consider a technique manipulation in the sense of the AI Act, subliminal techniques must be applied to sell a product.

- 42 In the Proposal, the article required the intention to materially distort a person’s behaviour in a manner that causes or is likely to cause harm when using subliminal techniques.¹⁰⁰ However, in practice, distorting a person’s behaviour is possible, even if it is not intentional. Therefore, this is changed in the Adopted Text to include the unintentional cases.
- 43 Subliminal techniques are not defined in the text. In the recitals, they are explained as techniques that affect autonomy or decision-making abilities even though they cannot be perceived as subliminal techniques, or they cannot be controlled even though perceived.¹⁰¹ In e-commerce, such extreme techniques are not likely to be used in practice.
- 44 The text excludes some important situations from the scope of the article. Some manipulation techniques can still cause serious harm even if they are not subliminal. Companies might use manipulation techniques that customers can perceive. They might send the customers timed advertisements when customers are vulnerable and more likely to buy a certain product. This may be left to other legislation such as the Unfair Commercial Practices Directive in accordance with the intentions of the AI Act that aims to be not too restrictive, but it is a weak part of it to regulate only some of the manipulative practices and not regulate the rest, which may cause the same amount of harm.
- 45 Another condition in the article is that the subliminal technique used must cause significant harm. Manipulation techniques can have an impact on people’s decision-making, causing them to buy products that they would not normally buy, or to buy more than they intended, and overspend. However, it is not clear how to measure the degree of significant harm. Whether the damage is serious enough to fall within the scope of the article must be assessed on a case-by-case basis. In cases where all these conditions are met, this practice will be prohibited. The article is very limited because it contains very difficult and specific conditions to meet, and it does not seem very likely to have all the conditions in these provisions met at the same time.¹⁰² Therefore, this article will not be likely to

92 AI Act art 5(1)(b)

93 AI Act art 5(1)(g)

94 AI Act art 5(1)(c)

95 AI Act art 5(1)(h)

96 AI Act art 5(1)(d)

97 AI Act art 5(1)(e)

98 AI Act art 5(1)(f)

99 European Commission, ‘Consumer protection: manipulative online practices found on 148 out of 399 online shops screened’ (European Commission, 30 January 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_418> accessed 12 October 2023

100 AI Act Proposal art 5(1)(1)

101 AI Act recital 29

102 Michael Veale, Frederik Zuiderveen Borgesius, ‘Demystifying the Draft EU Artificial Intelligence Act’ (2021)

apply to e-commerce practices.

b.) Vulnerable Groups

- 46 Article 5(1)(b) protects a person or a specific group of persons such as children, disabled persons or in a specific social or economic situation and prohibits the use of an AI system that exploits the vulnerabilities of these groups. Similar to Article 5(1)(a), the requirement of intent to materially distort the behaviour is changed in the Adopted Text and now the article covers also unintentional distortion. The Proposal did not include specific social or economic situations. They are included among the disadvantaged groups in the Adopted Text.
- 47 Situations like Article 5(1)(b) are more likely to be seen in practice. For its applicability is sufficient to exploit any vulnerability of a specific group of persons. For its application, the use of subliminal techniques is not required. In e-commerce, manipulation techniques to sell products to children, for example, will be covered in the article. Moreover, since the article includes specific social and economic situations, manipulating people with certain addictions by discovering their addictions through their purchasing histories may be in the scope of the article if these amendments are approved.
- 48 Again, the manipulation must cause or be likely to cause significant harm. Since the article states that the person who will be harmed can be a person other than the person from the specific group, it will be a prohibited practice if, for example, the families of children who have faced this harm or are likely to face it. It is not clear what will be considered significant harm. However, the article is important for e-commerce since it covers harms that are likely to arise from e-commerce while still preventing insignificant risks from being included unnecessarily. Similar to Article 5(1)(a), practices must be considered case-by-case basis.

c.) Complementary Aspect of the AI Act

- 49 Some of the manipulative practices might already be covered by other EU legislation. The Unfair Commercial Practices Directive prohibits materially

distorting,¹⁰³ misleading¹⁰⁴ or aggressive practices.¹⁰⁵ In addition to those, Annex I of the Directive lists the commercial practices that are prohibited under all circumstances. For example, Annex I Article 7 prohibits “falsely stating that a product will only be available for a very limited time” time which may trigger impulsive buying. The AI Act states in the recitals that the AI Act’s prohibitions of manipulative techniques are complementary to the prohibitions of the Unfair Commercial Practices Directive, which its prohibitions apply regardless of whether AI is used.¹⁰⁶ Moreover, by giving the example of advertising, it is stated that “common and legitimate commercial practices” that comply with the applicable law will not be considered harmful manipulative AI practices.¹⁰⁷ Therefore, in Articles 5(1)(a) and 5(1)(b), the AI Act mostly prohibits activities that are already prohibited.

2. Social Scoring

- 50 Article 5(1)(c) concerns social scoring. For the AI system to be prohibited under the article, both the conditions leading to the social score and the results caused by the social score must meet the criteria listed in the article. First, a social score must be created by evaluating or classifying a natural person’s “social behaviour or known or predicted personal or personality characteristics” over a certain period of time. Then, this social score must lead to detrimental or unfavourable treatment by using the data in an unrelated context compared to what it was originally collected for or by using the data in an unjustified or disproportionate manner considering the social behaviour.¹⁰⁸ Therefore, social scoring that does not lead to these results is not prohibited.
- 51 Social scoring includes credit scores. This is the creation of a financial trustworthiness score about natural persons by evaluating their actions in different contexts.¹⁰⁹ However, scoring in the broad

103 Unfair Commercial Practices Directive art 5(2)(b)

104 Unfair Commercial Practices Directive arts 6, 7

105 Unfair Commercial Practices Directive art 8

106 AI Act recital 29

107 *Ibid*

108 AI Act art 5(1)(c)

109 ‘Social scoring systems: current state and potential future implications’ (Kaspersky Daily) <<https://www.kaspersky.com/blog/social-scoring-systems/>> accessed 13 October 2023

sense is not limited to this, and it is possible to collect information about a person in various contexts and evaluate them in another context.¹¹⁰ The AI Act does not define social scoring in the text. However, it is defined in the recitals as “such AI systems evaluate or classify natural persons or groups thereof based on multiple data points related to their social behaviour in multiple contexts or known, inferred or predicted personal or personality characteristics over certain periods of time.”¹¹¹

- 52 In e-commerce, scoring in the traditional sense would be the case where customers are denied access to certain services or charged a higher price for them. For example, if customers cannot see some products on the website according to the score created about them, this will be considered a traditional scoring. Scoring can be commonly used in e-commerce through predictive analytics and consumer scores. E-commerce companies may have lawfully obtained data about customers such as name, address, age, and gender. In addition, they can make inferences about customers leading to consumer scores using predictive analytics. While the data that can be collected about the customers in physical stores are limited, much more data which are not limited to the shopping itself can be collected about them in the case of online shopping.¹¹²
- 53 In order to predict whether the customer will buy a certain product, “clickstream data”, “customer demographics” and “historical purchase data” can be analysed.¹¹³ When the data collected about customers are combined with other data, inferences can be made about them. This may cause data protection, privacy, and autonomy problems.¹¹⁴ Even when the collected and processed data are not particularly sensitive, the inferences made based on these data can relate sensitive personal data. For example, buying certain foods or not shopping on certain days due to religious reasons may lead to inferences about religion.¹¹⁵ Using the inferences about a person’s religion in another context, for a detrimental or unfavourable treatment, will fall

under Article 5(1)(c)(i). It is not clear what counts as a different context in the article. While the consequences of making inferences about a person’s religion might be problematic within the scope of privacy or discrimination law, for example, showing this person similar products purchased by this group on the same website will not be a different context in the sense of the AI Act. However, it is not clear whether the context will be considered different if this inference is used on another e-commerce website. In any case, the use of this inference in another sector such as health or education and detrimental or unfavourable treatment based on this inference or using the inferences from different sectors in e-commerce will fall within the scope of Article 5(1)(c)(i).

- 54 Moreover, since predictive analytics can divide people into certain groups, some people may not be able to take advantage of economic benefits.¹¹⁶ Some discounts may not be shown to certain groups, or people may be subjected to price discrimination because of a prediction. However, although the restriction of access to certain products and the fact that they cannot see them at all can be considered within the scope of Article 5(1)(c)(ii), the fact that they cannot benefit from some discounts cannot be considered as a disproportionate treatment.
- 55 It is possible for e-commerce activities to meet the conditions of both Article 5(1)(c)(i) and 5(1)(c)(ii) since companies often make inferences about customers and create scores about them. This article in the Proposal was not applicable to e-commerce as it did not include private actors. However, this approach was criticised. For example, EDPB and EDPS stated that the imposition of such specific requirements for prohibited AI systems was an approach that possibly limits the practical effectiveness of the AI Act.¹¹⁷ They suggested that the prohibition should cover any type of social scoring since it can also be conducted by private companies.¹¹⁸ This is changed in the Adopted Text to include private actors as well. Therefore, the prohibition is now applicable to e-commerce activities if the conditions in the article are met.

110 *Ibid*

111 AI Act recital 31

112 Dirk Van den Poel, Wouter Buckinx, ‘Predicting online-purchasing behaviour’ (2005) 166 European Journal of Operational Research 557, 557

113 *Ibid*, 561-566

114 Shaun B. Spencer, ‘Privacy and Predictive Analytics in E-Commerce’ (2015) 49 New England Law Review 629, 640

115 Tal Z. Zarsky, ‘Understanding Discrimination in the Scored Society’ (2014) 89 Washington Law Review 1375, 1395

116 Spencer (n 114), 629

117 EDPB-EDPS Joint Opinion (n 50), para 28

118 *Ibid* para 29

II. High Risk AI Systems

1. Is E-Commerce High Risk According to the AI Act?

- 56 A large part of the AI Act is allocated to the rules regarding high-risk AI systems. High-risk AI systems can be examined in two main parts: those with health and safety risks (Article 6(1)) or those with fundamental rights risks (Article 6(2)).¹¹⁹ For an AI system to be considered a high-risk AI system according to Article 6(1), the AI system must be a safety component of a product or a product itself, that is covered by the Union harmonisation legislation listed in Annex II and is required to undergo a third-party conformity assessment. Article 6(2) states that “in addition to the high-risk AI systems referred to in paragraph 1, AI systems referred to in Annex III shall also be considered high-risk”.¹²⁰
- 57 As a result of the classification of an AI system as high risk, the AI systems will need to comply with the requirements such as the risk management system,¹²¹ data and data governance,¹²² technical documentation,¹²³ record keeping,¹²⁴ transparency,¹²⁵ human oversight,¹²⁶ accuracy, robustness and cybersecurity.¹²⁷
- 58 Since Article 6(1) and Annex II refer to the list of Union harmonisation legislation and relate to product safety, it is not relevant for e-commerce. Article 6(2) and Annex III relate to fundamental rights. It appears that the risks of e-commerce activities are not considered high risk under Annex III of the AI Act since Article 6(2) refers to specific areas such as biometrics, critical infrastructure, education and vocational training, employment, access to

essential private services¹²⁸ and public services, law enforcement, border control management and administration of justice.

- 59 The Commission can adopt delegated acts and update the list in Annex III according to Articles 7 and 97. However, it can only add the AI systems intended to be used in the already existing areas mentioned above, and it cannot add any new areas to this list.¹²⁹ The sub-areas can be updated, but only if they involve equivalent or greater risk to health and safety or fundamental rights than already existing ones.¹³⁰ The criteria to be applied to compare these risks are specified in Article 7(2).
- 60 Since the high-risk AI systems are determined in the Annexes of the AI Act and e-commerce is not included in them, most of the AI systems used here are out of scope. However, as explained in Section C, e-commerce activities can also pose serious risks. Section D.II.2 will analyse whether these risks are comparable to other high-risk systems in the AI Act, and it will use Article 7(2) for this purpose.

2. Should E-Commerce Be Considered High Risk?

- 61 In order to compare the risks of e-commerce to the high-risk AI systems in Annex III, the risks existing in this sector need to be examined from the perspective of Article 7(2). Since the list in Annex III is exhaustive and it is not possible to add new areas to the list, the comparison within the scope of Article 7(2) will only be made to assess whether the risks of using AI in e-commerce *should be* classified as high risk or not. The criteria in Article 7(2) are examined below, following the order in the article. The issues considered as risks in e-commerce may have already been covered by Union legislation. In this case, According to Article 7(2)(k), the Commission will evaluate all these factors together and will not make any amendments if it considers that sufficient

119 AI Act Proposal Explanatory Memorandum, 13

120 AI Act art 6(2)

121 AI Act art 9

122 AI Act art 10

123 AI Act art 11

124 AI Act art 12

125 AI Act art 13

126 AI Act art 14

127 AI Act art 15

128 AI Act Recital 58 gives the examples of using creditworthiness and credit scores. These can be used in e-commerce, such as payments with instalments or buy now pay later systems. However, it should also be evaluated whether e-commerce can be considered essential. Essential private services are not defined in the text. It might be possible for e-commerce to be considered high-risk if some platforms become very dominant and considered essential in the future, and if AI is used to access them. For now, it is not likely for e-commerce to be considered high-risk for being used in access to essential private services.

129 AI Act art 7(1)(a)

130 AI Act art 7(1)(b)

redress mechanisms exist.

- 62 First, the intended purpose and the extent of the use of the AI system are considered.¹³¹ Even though AI can also be used to provide convenience to customers, it is usually primarily intended for the benefit of businesses. The purposes of companies of using the AI systems can change as explained in Section B. Therefore, it is not possible to make a general assessment of the use of AI in e-commerce. The extent of the risks of AI systems must be found based on each application. Different implementations of each system, the algorithms, and the customer data used may change this evaluation.
- 63 “The nature and amount of data processed and used by the AI system” are also considered.¹³² The article emphasises special categories of data since greater use of such data increases the risks to fundamental rights. In e-commerce, special categories of data can both be used and inferred from other data and this may pose risks to fundamental rights.
- 64 The level of autonomy of AI systems and of people over the AI system are considered.¹³³ This evaluation depends on the AI system used and the company itself. For example, while the risks may be less on a website of a company selling its own products and visited by fewer users, it may not be as easy for larger platforms with many users to provide human oversight to the decisions or recommendations made by AI.
- 65 Then, harm to health and safety and the adverse impact on fundamental rights are considered. Here, both previously encountered harms¹³⁴ and potential harms¹³⁵ are taken into account. As explained above, the use of AI in e-commerce may create risks, especially manipulation and discrimination. In addition, data protection problems may arise due to the nature of AI using a great amount of data. As it was mentioned, the AI Act imposes detailed conditions that are not always possible to meet at the same time. For example, manipulating a person can be done without using subliminal techniques. In this case, this practice will remain unregulated under the AI Act. However, it might be more appropriate to consider these practices as high-risk practices and take precautions accordingly.
- 66 Moreover, collecting personal data through information brokering and using it for advertising purposes may also cause data protection problems. Profiles of people created by data brokers by collecting and combining information from various sources may cause some problems¹³⁶ such as assessing the credibility of people based on data other than financial data (“credit scoring”),¹³⁷ inaccuracies of the profiles if the source information is incorrect or discrimination.¹³⁸ Practices such as Real Time Bidding (RTB) may cause privacy breaches while collecting data in the background and without people being aware of it.¹³⁹ In addition to the privacy breaches, RTB is also dangerous because even if people have consented to the further use of their data under the GDPR, they may not fully understand the scope of this further use.¹⁴⁰
- 67 Another point to consider is the extent of the dependency of the people affected by these practices on the outcomes reached by AI, and the possibility of opt-out from these outcomes.¹⁴¹ The article puts focus on practical reasons for this opt-out option as well. Customers may have to accept some conditions while shopping online to see the website, or purchase something. For example, while shopping online, cookies on the website may be rejected, except for essential cookies. However, this will still not prevent the collection of some data about the customer. While the collection of this data may not be in itself unlawful according to the data protection rules, practices such as profiling and making inferences about customers can lead to unlawful results such as discrimination. Moreover, sometimes technical impossibilities can cause problems. For example, in RTB, once the data are shared with third parties,

136 Shivangi Mishra, ‘The dark industry of data brokers: need for regulation?’ (2021) 29 International Journal of Law and Information Technology 395, 399

137 *Ibid*, 399

138 *Ibid*, 401

139 Johnny Ryan, ‘The Biggest Data Breach, ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe’ (Irish Council for Civil Liberties, 16 May 2022) <<https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf>> accessed 13 October 2023

140 IAB Europe, IAB Tech Lab, ‘GDPR Transparency and Consent Framework’ <<https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/pubvendors.json%20v1.0%20Draft%20for%20Public%20Comment.md#About-the-Framework>> accessed 13 October 2023

141 AI Act art 7(2)(g)

131 I Act arts 7(2)(a), 7(2)(b)

132 AI Act art 7(2)(c)

133 AI Act art 7(2)(d)

134 AI Act art 7(2)(e)

135 AI Act art 7(2)(f)

technically it is not possible to restrict the use of these data.¹⁴² It can be argued that it is not compulsory for the customer to shop online if these conditions are not acceptable. However, especially today, it is not practically reasonable to expect this from customers, and customers may tend to accept these conditions without reading them carefully or considering the consequences.

68 The position of the affected person “in relation to the user of the AI system” is also a point to be considered, especially in terms of “imbalance of power, or potentially harmed or suffer an adverse impact” “due to status, authority, knowledge, economic or social circumstances, or age”.¹⁴³ In e-commerce, there is a “power imbalance” between customers and sellers, both economically and in terms of knowledge regarding the sale.¹⁴⁴ The customer is in a more vulnerable position than the seller and this can affect the autonomy of the customers in online shopping. The price and product information presented to customers affects their online purchasing behaviours.¹⁴⁵ Not only the information presented but also “how and when it is displayed” can influence the behaviour of customers and can be used to manipulate them.¹⁴⁶

69 Whether the “outcome produced with an AI system is easily corrigible or reversible” is also a point to be evaluated.¹⁴⁷ It is stated in the article that the outcomes affecting the “health, safety, fundamental rights shall not be considered as easily reversible”.¹⁴⁸ Here, manipulation and its effects on mental health can be considered in terms of health and safety. The use of manipulation in a way that leads to making customers spend more money than they intend to, and these material consequences, therefore, can be considered easily reversible. Nevertheless, in e-commerce, it is more likely to encounter risks such as discrimination and privacy than health and safety risks. These issues should also be evaluated separately according to each AI system applied and the outcomes it produces.

70 Finally, the extent to which existing Union

legislation protects against these risks and redress mechanisms must be evaluated.¹⁴⁹ Claims for damages are excluded from the assessment of the “effective measures of redress”.¹⁵⁰ For example, in data protection and privacy issues, the GDPR gives data subjects the right to compensation.¹⁵¹ However, it also provides protection with the rights of the data subject¹⁵² such as the right to rectification, right to erasure, and right to restriction of processing. The effective redress under the AI Act Article 7(2)(k) refers to rights. Whether this is an effective redress against the outcome reached by the AI system may change case by case. For e-commerce, each case will be different depending on whether this redress is effective or not. If the redress is not effective, the practice would fall under the scope of high risk, considering the other conditions as well.

71 Regarding the discrimination risks, even though the non-discrimination law provides some solutions for them, there are cases that these risks may not be covered.¹⁵³ AI systems can discriminate based on different characteristics that are not protected in non-discrimination law.¹⁵⁴ For example, prices that customers see may differ according to the browser used.¹⁵⁵ Therefore, current legislation may not always provide effective protection against the use of AI.

72 However, whether the AI Act must provide extra protection must be evaluated by examining all these conditions in Article 7(2) together. Most AI uses in e-commerce fall outside the scope of high-risk according to these criteria, and it would not be proportionate to place e-commerce entirely within the scope of high-risk. However, there may be cases where AI applications that cause serious manipulation, discrimination or data protection risks meet all the criteria of Article 7(2) and therefore should be considered within the scope of high-risk AI systems. Furthermore, it is appropriate to consider some practices such as manipulation and social scoring, which do not meet all the criteria to be included in the scope of prohibited practices, within

142 IAB Europe, IAB Tech Lab (n 140)

143 AI Act art 7(2)(h)

144 Lippi and others (n 15), 171

145 Eliza Milk, ‘The erosion of autonomy in online consumer transactions’ (2016) 8 Law, Innovation and Technology 1, 1

146 *Ibid*, 2

147 AI Act art 7(2)(i)

148 AI Act art 7(2)(i)

149 AI Act art 7(2)(k)

150 AI Act art 7(2)(k)(i)

151 GDPR art 82

152 GDPR Chapter III

153 Zuiderveen Borgesius, ‘Discrimination, Artificial Intelligence, and Algorithmic Decision-Making’ (n 16), 20

154 *Ibid*, 35

155 *Ibid*, 35, 36

the scope of high-risk.

III. Limited Risk AI Systems ("Transparency Obligations for Providers and Deployers of Certain AI Systems"¹⁵⁶)

73 Article 50 regulates transparency obligations for providers and deployers of certain AI systems. What obligations e-commerce companies must comply with will vary depending on whether they develop their own AI systems or use AI systems developed by third parties.

74 Article 50(1) brings an obligation of disclosure to providers. If an AI system is "intended to directly interact with natural persons" the providers must inform the natural persons that this is an AI system. However, if it is obvious from the "circumstances and the context of use", disclosure will not be necessary.¹⁵⁷ Chatbots are AI systems that interact with natural people. Many e-commerce companies can use chatbots on their websites. However, the disclosure responsibility is on the provider. If e-commerce companies use the chatbots that they design on their own, they must design them in a way that the natural persons interacting with these chatbots are aware that they are interacting with an AI system. In case e-commerce companies are using chatbots developed by third parties and the developers of the chatbot have failed to design it in this way, e-commerce companies are not obliged to inform the natural persons as deployers. However, since the purpose of the article is to protect natural persons, it may be good practice for companies to not use chatbots that are not compliant with this obligation.

75 Article 50(3) states that "deployers of an emotional recognition system or biometric categorisation system shall inform of the operation of the system the natural persons exposed thereto". Veale and Zuiderveen Borgesius noted that while it is not clear what this provision adds to the existing data protection obligations, the intention of the article might be to apply to AI systems that do not process personal data as well.¹⁵⁸

76 E-commerce companies might use emotion recognition systems in their activities. Techniques

such as sentiment analysis, which are used to analyse people's opinions about a subject,¹⁵⁹ can work without processing personal data. For example, customer reviews on websites might be analysed to find out a positive or negative opinion about a particular product without using any personal data of the customer. However, whether these techniques fall within the scope of emotional recognition under the AI Act is not clear.

77 Article 50(4) also brings obligations for the deployers and relates to deep fakes. Deployers are obliged to disclose if an "image, audio or video content constituting a deep fake" is "artificially generated or manipulated".¹⁶⁰ Article 50(2) brings a similar disclosure obligation to providers as well.¹⁶¹ However, this article does not mention deep fakes and covers "synthetic audio, image, video or text content".¹⁶² The contents relating to these two obligations are mentioned as "synthetic"¹⁶³ and "falsely appear to a person to be authentic"¹⁶⁴ in the recitals. In the context of e-commerce, generated content within the meaning of Article 50(2) is more likely to be used in practice. For example, if the images of the products sold are AI-generated, this should be disclosed by the company. Such a situation may not occur very often in practice unless it is about underdeveloped prototypes or AI-generated images showing how clothes would fit customers. Nevertheless, whether they are providers or deployers, e-commerce companies have various disclosure obligations under Articles 50(2) and 50(4).

78 This article will be applied in addition to the high-risk requirements and obligations in Chapter III.¹⁶⁵ Although it is not specified in the article, it is clear that the AI systems mentioned in this article cannot be used in any way if they fall within the scope of the AI Act's prohibited practices.

¹⁵⁶ AI Act Chapter IV

¹⁵⁷ AI Act art 50(1)

¹⁵⁸ Veale, Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (n 102), 107

¹⁵⁹ Pansy Nandwani, Rupali Verma, 'A review on sentiment analysis and emotion detection from text' (2021) 11 Social Network Analysis and Mining 81, 81

¹⁶⁰ AI Act art 50(4)

¹⁶¹ AI Act art 50(2)

¹⁶² *Ibid*

¹⁶³ AI Act recital 133

¹⁶⁴ AI Act recital 134

¹⁶⁵ AI Act art 50(6)

IV. Minimal / No-Risk AI Systems

- 79 AI systems other than the above-mentioned risk groups are considered as minimal / no risk and there is no obligation for them under the AI Act. The AI systems used in e-commerce activities that do not fall under the scope of the prohibited practices, high-risk or limited risk AI systems, they will fall under the minimal / no-risk scope. Other EU legislation such as data protection, non-discrimination, and consumer protection law will continue to be applied to these AI systems. However, the AI Act does not impose any additional obligations on them.
- 80 The AI Act introduces a mechanism to drawing up and voluntary application of Codes of Conduct in Chapter X for AI systems other than those classified as high-risk. This is to encourage the voluntary implementation of the some or all of the requirements in Chapter III, Section 2, relating to high-risk AI systems.¹⁶⁶ Article 95(3), states that codes of conduct can be drawn up by both individual providers or deployers and the organisations representing them, and deployers and interested stakeholders can be involved in this process.
- 81 The implementation of voluntary codes of conduct will entail large numbers of obligations for e-commerce companies. In Chapter III, Section 2, obligations for high-risk AI systems are specified. These are detailed obligations regarding risk management system, data and data governance, technical documentation, record-keeping, transparency and provision of information to deployers, human oversight, and accuracy, robustness and cybersecurity. It may not be realistic to expect e-commerce companies to comply with these extra rules that are not mandatory. Adding these obligations to those that already must be complied with can be a heavy burden for companies, both financially and in terms of resources. However, complying with them may put them in a better position in terms of public prestige and credibility than other companies that choose not to implement voluntary codes of conduct.

E. Conclusion

- 82 AI has many benefits and is therefore often used in e-commerce. With the help of AI, companies can have abundant and accurate information about their customers and the market, make predictions and adjust their actions accordingly. AI enables companies to be efficient, reduce workload and increase profits. However, the use of AI may also

cause some risks related to transparency, human control, and accountability.¹⁶⁷ The two most serious risks that the use of AI may bring are manipulation and discrimination.

- 83 The AI Act is an important piece of legislation by the EU in this area and it has adopted a risk-based approach. According to the risk-based approach, the AI Act prohibits some practices, imposes obligations about some AI systems, or leaves some of them unregulated. The applicability of the AI Act to e-commerce activities is determined according to these risk levels. This article researches the following questions: *To what extent do the provisions of the AI Act apply to e-commerce companies that use AI? To what extent is this in line with the objectives of the AI Act, considering the risks in relation to the use of AI for e-commerce?*
- 84 The applicability of the AI Act in e-commerce depends on the AI techniques used, and the role of the e-commerce company as a provider or deployer. The prohibited practices in the AI Act are for both providers and deployers. The prohibited practices that might relate to e-commerce activities in the AI Act are the subliminal techniques in Article 5(1)(a), vulnerable groups in 5(1)(b) and social scoring in 5(1)(c). However, since Article 5 has many conditions that are difficult to meet at the same time, it will be unlikely for e-commerce activities to be in the scope of the article. Furthermore, practices that fulfil all those conditions may also be prohibited under existing law such as the Unfair Commercial Practices Directive. Nevertheless, the practices must be evaluated on a case-by-case basis to see whether they would be prohibited or not.
- 85 According to the AI Act, AI systems that are used in e-commerce are not high-risk AI systems. However, these AI systems may still cause serious risks. The AI Act lists high-risk AI systems in specific areas, and it is not possible to add new areas to the existing areas. This approach excludes AI systems that may pose significant risks. Although not all use of AI in e-commerce poses risks serious enough to be considered high-risk according to the AI Act, some applications may pose serious risks enough to meet the criteria in Article 7(2), especially in practices such as manipulation and social scoring. If the AI system in question is not a high-risk or limited-risk AI system and does not fall within the scope of prohibited practices only because it does not meet one of the many conditions in the article, it can be left completely unregulated under the AI Act. For example, a manipulative practice may not be considered a prohibited practice only because it does not use subliminal techniques. Similarly, not all practices that lead to risks may be prohibited

166 AI Act art 95(1)

167 EDPB-EDPS Joint Opinion (n 50), para 3

under the Unfair Commercial Practices Directive. Regulating such practices at least to a certain degree would provide better protection by the AI Act against these risks. Furthermore, such regulation would complement existing rules by imposing obligations on the AI systems themselves, instead of only on the use of such systems in specific situations.

- 86** Article 52 regulates transparency obligations for certain ‘limited risk’ AI systems. Obligations related to these vary depending on whether the e-commerce company is a provider or a deployer. There are no obligations for the AI systems that are considered minimal or no-risk AI systems. However, companies can apply the obligations for high-risk systems in the AI Act by implementing codes of conduct. This may increase their reliability and give them a competitive advantage. Voluntary compliance with these obligations will be beneficial in mitigating some of the risks of using AI in e-commerce. However, these are serious risks that should not be left to companies’ discretion and instead of voluntary compliance, addressing them somewhere else in the AI Act could be a better approach.
- 87** The AI Act leaves a regulatory gap in the use of AI in e-commerce, considering the risks. The two important objectives of the AI Act are product safety and fundamental rights. However, the AI Act seems to concentrate more on product safety. AI systems in e-commerce are left largely unregulated, even though they can also create serious risks comparable to those of high-risk systems. The AI Act could be more effective if it did not exclude such important risks and had a larger scope.

Online Intermediaries and Trademark Owners: The Legal Position and Obligations of Online Intermediaries to Trademark Owners Prior and post-Louboutin v Amazon

by Dania van Leeuwen, Mark Leiser and Lotte Anemaet *

Abstract: This article argues that the legal standing of the online intermediary towards trademark holders has undergone a significant shift. Generally, only secondary liability was assumed, as the online intermediary was not held to be able to bear its own “primary” liability for conduct not directly attributable to itself, such as offering counterfeit products. However, in the Louboutin v. Amazon case, the CJEU provided a new standard for interpreting “commercial communication”, which is required for an “active role” in the infringing use. According to the CJEU, this should include the perspective of the informed

and reasonably observant internet user. This reasoning is remarkable, as this perspective has not previously been considered when assessing whether there is active behaviour. The combination of the Louboutin v. Amazon judgement and the advent of the DSA with its associated new obligations mean that not only has the responsibility of online platforms increased, but they may also be held directly liable for infringing goods offered on their platform.

Keywords: Trademarks; Online Intermediaries; Trademark Use, Digital Service Act

© 2024 Dania van Leeuwen, Mark Leiser and Lotte Anemaet

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Dania van Leeuwen, Mark Leiser and Lotte Anemaet, Online Intermediaries and Trademark Owners: The Legal Position and Obligations of Online Intermediaries to Trademark Owners Prior and post-Louboutin v Amazon, 15 (2024) JIPITEC 56 para 1.

A. Introduction

1 Information sharing predominantly occurs on online platforms, which serve as foundational technological mediums for delivering or aggregating digital services and content accessible to end-users.¹ These platforms manifest in diverse formats, including but not limited to app stores, social media platforms, and search engines. Such platforms

have become so integral to contemporary society that envisioning our current era without them is challenging. Concurrently, the economic landscape has transitioned to the digital domain. Beyond companies’ proprietary websites where products can be directly showcased and purchased, a myriad of online sales platforms, often termed ‘online marketplaces’, have emerged. These marketplaces function as neutral digital environments, seamlessly connecting sellers and buyers. Typically, the entity managing an online marketplace facilitates transactions between these parties², providing

1 O. Batura, N. van Gorp & P. Larouche, ‘Online Platforms and the EU Digital Single Market’ (2015) <https://ec.europa.eu/information_society/newsroom/image/document/2016-7/nikolai_van_gorp_-_response_e-economics_to_the_uk_house_of_lords_call_for_evidence_14020.pdf> accessed 23 July 2023.

2 EUIPO, ‘Case-law Collection on the Liability and Obligations of Intermediary Service Provider’ (2019) <<https://euipo.europa.eu/ohimportal/nl/-/news/ipr-enforcement->

sellers with an efficient means to present their products to a vast audience. Consequently, the rising popularity of online marketplaces among European Union (EU) businesses is evident, with one million EU businesses vending products through these platforms. Moreover, over 50% of small and medium-sized enterprises (SMEs) utilising these online marketplaces engage in cross-border sales.³ The European Commission appropriately recognises online marketplaces as pivotal catalysts for innovation within the digital marketplace.⁴

- 2 Online marketplaces allow third parties to offer their goods for sale. These parties are the “business users” of the online platform: private individuals acting in a commercial or professional capacity or any legal person who, through online platforms, offers goods to consumers for purposes relating to their trade, business, craft or profession.⁵ These companies have built their business and products independently of the online intermediary and use the online marketplace to make their goods available to the ever-increasing public. Business users can be established companies, but they can also be start-ups that aim for quick and easy brand awareness through these platforms. An online marketplace only has value when buyers use it. These buyers, often *consumers*, search the internet for a particular product. An online marketplace makes it clear to the buyer what is on offer for that product. It may also be that the buyer is not looking for a specific product but only visits the online marketplace to ‘look around’. Either way, the online marketplace is the ideal place for both business users and consumers to do business with each other remotely, which in the previous century was only conceivable on location.
- 3 Despite the countless different types of goods that end up on online marketplaces, the vast majority of them have one thing in common: they are each linked to a brand. This allows consumers to determine the product’s origin by linking the brand to the product. The recognition of this brand is often

case-law-collection-on-the-liability-and-obligations-of-intermediary-service-providers-in-the-european-union> accessed 23 July 2023.

- 3 European Commission, ‘Online Platforms’ <<https://digital-strategy.ec.europa.eu/de/policies/online-platforms>> accessed 23 July 2023.
- 4 European Commission, ‘Online Platforms’ <<https://digital-strategy.ec.europa.eu/de/policies/online-platforms>> accessed 23 July 2023.
- 5 Article 2(1) Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

the result of significant investments by the business behind the product. To ensure transparency in the market, protect the consumer and accommodate the product provider, trademarks can be legally protected through trademark law, which is part of the intellectual property domain.⁶ In that case, the provider can be regarded as the *trademark holder* with an exclusive right to the trademark to prohibit unauthorised third parties from using their trademark in trade concerning goods and services.⁷

- 4 The threshold for being able to act as a business user of an online marketplace is relatively low and is specially designed to be accessible to all types of companies or individuals acting in a commercial or professional capacity. As a result, the online competition is fierce. The advantages that an online marketplace offers, combined with the low threshold for anticipating in the online digital market, attract third parties who want to ride on the success of a strong brand. A common type of free riding is the use of counterfeit products. Counterfeit products cloud the sought-after transparent (digital) market, mislead consumers, undermine trademark holders, and are undesirable.⁸ The digital nature of an online marketplace entails the difficulty for consumers to determine whether a product is counterfeit. Especially when the online platform is given high brand recognition, consumers are generally more likely to assume the legitimacy of the goods offered. The speed at which online platforms inspire this trust among consumers and business users is remarkable.⁹ However, the trademark holder is not left empty-

-
- 6 A. Kur & M.R.F. Senftleben, *European Trade Mark Law: A Commentary* (Oxford University Press 2017) 6-10. This enumeration lists several functions of trademark law. Nowadays, trademark law has taken on a broader meaning; for example, trademarks are often used as means of communications.

- 7 Article 10 EUTMD; Article 9 EUTMR.

- 8 Studies conducted by the EUIPO, and the OECD have calculated that counterfeit and pirated goods worth EUR 119 billion were imported into the EU in 2019, representing 5.8 percent of EU imports. One in three Europeans think it is acceptable to buy fake products if the original product’s price is too high. This number is even at 50% among young people. See: EUIPO, *European Citizens and Intellectual Property: Perception, Awareness, and Behaviour* (2023), p. 9; EUIPO-Europol, *Intellectual Property Crime Threat Assessment 2022*, p. 2. The number of counterfeit products traded worldwide accounts for approximately 2.5 percent of global trade. See: OESO/EUIPO, *Global Trade in Fakes: A Worrying Threat*, Illicit Trade, OECD Publishing, Parijs, 2021, p. 9.

- 9 L.G. Verburg, ‘Online platformen en platformarbeid: een eerste verkenning’ (2019) O&R 116, 6.1.1.

handed. In many cases, these counterfeit products fall under the scope of trademark protection. The conditions for trademark infringement are listed in Article 2.20 Benelux Convention on Intellectual Property (“BCIP”)¹⁰ for Benelux trademarks and in Article 9 EU Trademark Regulation (“EUTMR”)¹¹ for EU trademarks. If an unlawful use by a third party is established, that party will be liable towards the trademark holder.

- 5 Both the BCIP and the EUTMR are influenced by the EU Trademark Directive (“EUTMD”)¹² and are, therefore, subject to interpretation by the Court of Justice of the EU (“CJEU”). The critical condition of trademark infringement is the concept of “use”. The interpretation of this concept has long been subject to debate.¹³ The CJEU has had to consider more than once whether there is use within the meaning of Article 2.20 BCIP and Article 9 EUTMR. The answer to this question is all the more complex in cases involving an intermediary, which is the case of an online marketplace. Holding the online platform liable rather than the providers of the infringing goods may be more favourable, as, in many instances, they are more reachable, influential, and financially empowered. However, it has appeared to be questionable whether these online intermediaries could fall within the scope of the concept of use.
- 6 A landmark ruling in this context is the *Louboutin v. Amazon* case.¹⁴ The CJEU answered positively to whether an online intermediary can be held directly liable for counterfeit products a third party offers.

10 Benelux Convention on Intellectual Property (Trademarks and Designs) 2005.

11 Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trade Mark.

12 Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks.

13 A-G Szpunar noted that “the case-law of the Court has never provided a more thorough definition of that condition and that that question has also not been considered in more detail in legal literature, with the result that it is not clear what is covered by the concept of ‘use of a sign in an intermediary’s own commercial communication’. The exclusively negative use of that condition, which has served to demonstrate only that a sign has not been used even in the case which led to its discovery, largely accentuates that lack of precision.” See: C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:C:2022:422, Opinion of A-G Szpunar, para. 53.

14 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016.

This outcome is novel, as legal scholars and the CJEU assumed that online platforms’ actions were not directly related to the infringing use of a trademark and cannot be held directly liable based on Article 2.20 BCIP and Article 9 EUTMR.¹⁵ Potentially, this ruling has far-reaching implications for interpreting the concept of use and, therefore, the liability and obligations of online intermediaries. Despite the trademark nature of this judgement, its implications extend beyond the intellectual property domain. With the advent of the Digital Service Act¹⁶ (“DSA”), online intermediaries are involved in liability issues and various obligations. How this new set of rules should be interpreted is ambiguous, considering the *Louboutin v. Amazon* case. The pre-existing provisions of the E-Commerce Directive¹⁷ (“ECD”) may also take on an altered significance. The multitude of relevant judgements, the landmark *Louboutin v. Amazon* case and the advent of new European legislation make it unclear what online intermediaries’ current (and future) position towards trademark holders constitutes. This article aims to provide clarity for both intermediaries and trademark owners. The main question at the centre of this article is:

How do the provisions of EU trademark law and the European Union’s new Digital Services Act delineate the legal obligations of online marketplaces vis-à-vis trademark rights holders?

- 7 The article focuses primarily on online intermediaries that facilitate online marketplaces as a service. Still, the sources and case law are mainly relevant to online intermediary platforms. To obtain an understanding of various case laws, the liability and obligations of intermediaries and the interpretation of the judgement of the *Louboutin v. Amazon* case, Section 1 first outlines the legal framework of trademark infringement. This section thus forms the basis for the subsequent sections where the legal trademark position of online intermediaries is further discussed. Next, Section 2 focuses on case law, using previous rulings to establish the former legal position of the online intermediary. A case law analysis of the *Louboutin v. Amazon* case follows this. Referring to

15 For example: E. Rosati, ‘The *Louboutin/Amazon* cases (C-148/21 and C-184/21) and Primary Liability Under EU Trade Mark Law’ (2022) EIPR 435-440, C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267 and C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474.

16 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC.

17 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronics commerce, in the Internal Market.

this analysis and the established prior position, the reasoning complications are addressed. Section 3 is devoted to European legislation, specifically the ECD and the DSA, focusing on interpreting the provisions in light of the *Louboutin v. Amazon* case. This allows the current legal standing of the online intermediary to be established. Finally, Section 4 focuses on the future and discusses what developments can be expected regarding the legal position of online intermediaries. This section closes with a summary conclusion in which an unequivocal answer to the article's central question is formulated.

B. Trademark Infringement

- 8 Online intermediaries are taking on a significant role due to the still increasing importance of the internet. Their influence reaches as far as the intellectual property domain. This has had an impact on trademark law. To determine what the *Louboutin v. Amazon* judgement entails and its effect on intellectual property law and beyond, it is essential to form a legal framework to which it relates. Article 2.20 BCIP and Article 9 EUTMR define trademark infringement cases for EU trademarks. In both articles, a non-exhaustive list stipulates situations where a third party uses a trademark “use”. This “use” can be declared infringing under certain circumstances. Thus, the unlawfulness of online intermediaries’ conduct towards trademark holders will be determined primarily by interpreting these circumstances. Many rulings preceded the judgement from the *Louboutin v. Amazon* case. The CJEU has more often given interpretation of trademark infringement. For example, the discussion of whether an online intermediary itself “uses” a trademark right or whether it is only partially responsible for this infringing “use” has been addressed numerous times by the CJEU. The outcome of this issue determines whether and to what extent the online intermediary is liable for the unlawful use of the protected trademark. In this context, legal scholars often distinguish between primary and secondary liability.¹⁸ In assessing this issue, the CJEU had to consider the fair balancing of different rights and interests of the parties involved. The interpretation of trademark infringement dictates the scope of trademark protection and the extent of the exclusive right belonging to the trademark holder. Ultimately, the outcome of these cases determines the obligations and conduct required by online intermediaries.
- 9 To arrive at an understanding of trademark infringement, this section will first explain the

relevant legal framework. The outline of the conditions and content of the trademark right will follow this. Next, the core of trademark infringement will be discussed, focusing on the use concept. Finally, in anticipation of the next section, the matter of trademark infringement by (online) intermediaries will be addressed. Therein, the distinction between primary and secondary liability will be discussed.

I. Content of the Trademark

- 10 Trademarks give products an identity and are, therefore, a means of identification par excellence.¹⁹ It must satisfy two main conditions to garner legal protection over a trademark. The sign must have a distinctive character and be clearly and precisely represented in the register.²⁰ Once the trademark is registered, then the right is acquired.²¹
- 11 Article 10(1) EUTMD states that the trademark right includes an *exclusive right* for the proprietor of the registered right. Article 10(2) EUTMD regulates under which circumstances the trademark holder can act against infringing use and to what extent their right is limited. The types of infringement are detailed in the succeeding sections a-c of Article 10(2) EUTMD. The text of this provision is fully reproduced in Article 2.20 BCIP and Article 9 EUTMR.²² The trademark holder has a total of three infringement rules at its disposal by which it can prevent or counter the unauthorised use of their trademark. They are divided under subparagraphs (a), (b) and (c) of Article 10(2) EUTMD.
- 12 Firstly, Article 10(2)(a) EUTMD concerns trademark infringement where the third party uses a sign identical to the registered trademark about goods or services that are identical to those for which the trademark is registered. This includes counterfeiting since there is the so-called use of dual identity.²³ To

18 G. Fresio, *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) ch 4.

19 P.G.F.A. Geerts & A.M.E. Verschuur (eds.), *Kort begrip van het intellectuele eigendomsrecht* (Deventer: Wolters Kluwer 2022) 279.

20 Article 2.1 BCIP and Article 4 EUTMR.

21 Article 2.2 BCIP and Article 6 EUTMR.

22 The BCIP has added a fourth section and which therefore falls outside the harmonization of the EUTMD, leaving the BCJ in charge of interpreting this section. This concerns cases where the sign is used other than to distinguish goods and services. This provision is mainly invoked to attack trade names used only to distinguish a company.

23 A. Kur & M.R.F. Senftleben, *European Trade Mark Law: A Commentary* (Oxford University Press 2017) 294.

successfully invoke this provision, both the use of the identical sign and the use of this sign about identical goods or services must be proven.²⁴ Furthermore, it must be established that the use is or may be detrimental to the functions of the trademark to guarantee to the consumer the origin of the goods or services.²⁵

- 13 Secondly, Article 10(2)(b) EUTMD defines the infringement scenario where a third party uses an identical or similar sign for identical or similar goods. That third party causes a likelihood of confusion. Likelihood of confusion exists if the relevant public confuses the products in question (direct confusion) or expects the products to originate from the same or related companies (indirect confusion).²⁶ When assessing the likelihood of confusion, a global assessment should involve the relevant circumstances of the case.²⁷
- 14 Thirdly, Article 10(2)(c) EUTMD formulates the protection of trademarks that have a reputation in Member State(s), with which the legislator mainly intended to protect their goodwill function.²⁸ Applying this infringement provision does not require a likelihood of confusion, nor does it matter to what extent the goods or services are similar. However, the signs must be identical or similar. In addition, there must be an impairment of the goodwill function or unfair advantage taken of the distinctive character or reputation of the trademark. Taking undue advantage occurs if the third party benefits from using the sign. This is also known as “free riding”.²⁹ Any damage to the trademark is

irrelevant in this respect.³⁰

- 15 The third party may evade liability if they can provide a *due cause* for using the identical or similar sign. This justification relates to balancing the interest of the trademark holder in maintaining the essential function of its trademark against the interest of a third party in using such a sign in the course of trade to designate the goods and services it markets.³¹ Finally, for a successful invocation of Article 10(2) (a-c) EUTMD, the (unlawful) use of a trademark *in the course of trade* must be ascertained. “In the course of trade” entails that the sign is used in a commercial activity that seeks an economic advantage, not in the private domain.³² Any infringement or imminent infringement of the trademark may give rise to enforcement. This may lead to a court injunction, often sanctioned by a penalty payment. If a national court grants such an injunction, the injunction applies in principle to the entire territory in which that trademark has effect.³³

II. The Concept of “Use”

- 16 The various forms of trademark infringement have in common that there must be a *use* for which the third party against whom infringement is sought can be held responsible.³⁴ The interpretation of “use” ultimately determines which party is responsible for an infringing situation. Article 10(3) EUTMD lists acts of use that may qualify as infringing and may, therefore, be prohibited:

- a. affixing the sign to the goods or the packaging thereof;
- b. offering the goods or putting them on the market, or stocking them for those purposes;
- c. under the sign, or offering or supplying services thereunder; importing or exporting the goods under the sign;
- d. using the sign as a trade or company name or part of

24 C-690/17 *OKO-test verslag* [2019] ECLI:EU:2019:317, para. 43.

25 C-17/06 *Céline* [2007] ECLI:EU:C:2007:497, para. 27; C-487/07 *L'Oréal v. Bellure* [2009] ECLI:EU:C:2009:378, para. 58.

26 C-251/95 *Sabel v. Puma* [1997] ECLI:EU:C:1997:528, paras. 22, 26; C-39/97 *Canon v. Cannon* [1998] ECLI:EU:C:1998:442, para. 29.

27 C-251/95 *Sabel v. Puma* [1997] ECLI:EU:C:1997:528, para. 23; C-328/18 *Equivalenza* [2020] ECLI:EU:C:2020:156, paras. 58, 74.

28 P.G.F.A. Geerts, in: *T&C Intellectuele Eigendom*, art 2.20 BVIE, note 9.. See also: C-487/07 *L'Oréal v. Bellure* [2009] ECLI:EU:C:2009:378; C-252/07 *Intel v. Intelmark* [2008] ECLI:EU:C:2008:655; C-383/12 *Environmental Manufacturing v. OHIM* [2013] ECLI:EU:C:2013:741.

29 A “free rider” can be defined as a person or entity who benefits from the effort of others without making -in the eye of the beholder- an appropriate contribution to those efforts. See: M. Grynberg, ‘Trademark Free Riders’ (2022) *BTJLJ* 3.

30 C-487/07 *L'Oréal v. Bellure* [2009] ECLI:EU:C:2009:378, paras. 41, 50.

31 C-85/16 and C-86/16 *Kenzo Tsujimoto v. EUIPO* [2014] ECLI:EU:C:2018:349; C-65/12 *Leidseplein Beheer v. Red Bull* [2014] ECLI:EU:C:2014:49, paras. 30, 45.

32 C-206/01 *Arsenal v. Reed* [2002] ECLI:EU:C:2002:651, para. 40.

33 P.G.F.A. Geerts, in: *T&C Intellectuele Eigendom*, art 2.20 BVIE, note 3.

34 C-179/15 *Daimler v. Egyud* [2016] ECLI:EU:C:2016:134, para. 39.

a trade or company name;

e. using the sign on business papers and in advertising;

f. using the sign in comparative advertising in a manner that is contrary to Directive 2006/114/EC.

- 17 This enumeration is not exhaustive, as evidenced by the wording “in particular, “ confirmed in case law.³⁵ One will have to assess, based on the circumstances of the case, whether there is such use and whether this is considered unlawful. In cases where it becomes unclear if a third party is using an infringing sign, the use question comes into play even more. This essentially boils down, as will be discussed further below, to whether this third party has used the trademark. Such is the case with online intermediaries facilitating and administering a marketplace online.
- 18 Should infringing goods be offered on this marketplace by someone other than this intermediary, the question arises whether the supplier of these goods and the intermediary can be held liable by the trademark holder. This discussion is still very much alive in both case law and literature. According to the CJEU, there need to be two conditions satisfied to qualify if use is unauthorised by a third party. The person or entity must exhibit active behaviour (or conduct) and thus exercise direct or indirect control over the act that constitutes the use. In addition, the use must take place on its initiative and in its name, or other words, for its *commercial communication*.³⁶ This requirement is fulfilled if the customarily informed and reasonably observant recipient of such communication establishes a link between the said sign and the goods marketed or services provided by the undertaking.³⁷

III. Primary and Secondary Liability

- 19 The question of to what extent intermediaries should be held directly liable not only affects trademark law but also plays out in a broader spectrum of intellectual property. For example, the CJEU has repeatedly ruled on the discussion of whether the intermediary in question was liable based on

35 E.g. C-179/15 *Daimler v. Egidio* [2016] ECLI:EU:C:2016:134, para. 40.

36 C-324/09 *L'Oréal v. eBay* [2011] ECLI:EU:C:2011:474, para. 102; C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267, paras. 37-39, 47; C-193/19 *Mitsubishi* [2020] ECLI:EU:C:2020:594, paras. 38-39.

37 C-17/06 *Céline* [2007] ECLI:EU:C:2007:497, para. 23.

copyright law.³⁸ In addition, (online) intermediaries receive special attention in the DSA and the ECD. Thus, there are different degrees of liability depending on the online intermediary's role in (for example) disseminating the infringing content. In this context, the distinction between primary and secondary liability is made.³⁹ Primary liability focuses on whether the online intermediary infringes (for example) someone else's trademark. The online intermediary is liable for users' infringements in secondary liability.

C. The *Louboutin v. Amazon* case

- 20 The *Louboutin v. Amazon* judgement⁴⁰ distinguishes between trademark law's past, present and future as applicable to online intermediaries and their obligations to trademark holders. This section will discuss case law that preceded *Louboutin v. Amazon* to establish the legal obligations of online intermediaries towards trademark holders. After a comprehensive case analysis of the facts and judicial reasoning used in *Louboutin v. Amazon*, the substance and implications of this judgment become clear.

I. Previous Position of Intermediaries

- 21 In some cases, it may need to be evident who the trademark infringer is. In the case of online intermediaries, it can be challenging to determine whether the online intermediary is using the protected trademark if, in principle, it is only acting as an intermediary. The fact that an intermediary takes care of the technical provision necessary for using a sign by a third party and is reimbursed for it does not automatically mean that that intermediary also uses the sign itself.⁴¹ In such cases, it is challenging to identify the boundary when the intermediary acts more than just as a passive party. Therefore, there has been a lot of case law on this issue, especially on interpret-

38 C-360/10 *Sabam v. Netlog* [2021] ECLI:EU:C:2012:85; C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503..

39 G. Frosio (red.), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 8; A. Kur & M.R.F. Senftleben, *European Trade Mark Law: A Commentary* (Oxford University Press 2017) 275-277, 290.

40 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016.

41 C-622/16 *Google v. Google France* [2010] ECLI:EU:C:2010:474, para. 57.

ing the various terms in the context of the online intermediary.

- 22 The bar for “use” regarding trademark infringement was quite low. Article 10(3) EUTMD contains a non-exhaustive enumeration that intended a broad meaning of acts of use. Several judgements indicate that the CJEU intended to extend this broad interpretation into practice. *BMW v. Deenik*⁴², *Arsenal v. Reed*, and *Adam Opel v. Autec* are examples of the CJEU consistently labelling the act of a third party as used within the meaning of Article 10(3) EUTMD. However, the CJEU seems to have taken a different route regarding online intermediaries.

Google v. Louis Vuitton

- 23 In *Google v. Louis Vuitton*,⁴³ the CJEU had to consider whether Google was liable for trademark infringement if it allowed advertisers to select signs identical to trademarks as keywords, then store those signs and display its customers’ ads based on them. For a fee, the ads were then placed above standard search results. Advertisers selected trademarks such as “Louis Vuitton” and “LV” as keywords and linked them to sponsored ads for imitation products of the brand. The CJEU ruled that a search engine does not use a trademark when it helps advertisers select trademarks as keywords, store those signs for them, and display advertisements based on them. This is because Google does not use the trademark in its communication context but merely provides the technical facilities necessary to use the trade mark.⁴⁴ This is no different if Google is paid for the search engine advertising service.⁴⁵ In contrast, the advertiser uses the trademark if it chooses trademarks as keywords and links advertisements of its products to them.⁴⁶

L’Oréal v. eBay

- 24 Another vital predecessor to the *Louboutin v. Amazon*

case is the *L’Oréal v. eBay* judgement.⁴⁷ L’Oréal thought that eBay did not show sufficient commitment to stop the sale of counterfeit products. The CJEU ruled that an online marketplace did not use the trademark if it allowed third parties to display infringing products on its website.⁴⁸ It does if an online marketplace advertises its website and its infringing sales offers. eBay advertised L’Oréal brands as keywords via Google in return for payment, so ad links to sales offers for L’Oréal products appeared on eBay. Under subparagraph (a), there is infringement about the sales offers if the advertisement makes it impossible or difficult for the usually informed and reasonably observant internet user to know whether the goods offered come from the trademark owner or a third party.⁴⁹ About advertising for its platform, there is no infringement of subparagraph (a). Still, a reliance on sub-paragraph (c) is possible as the sign was not used for identical or similar goods or services.⁵⁰ Service providers like eBay may additionally not rely on the exemption from liability for service providers under Article 14 of the E-commerce Directive if they play an active role and have knowledge or control over stored information. This is the case if they promote sales offers or help optimise the presentation of ads.⁵¹ Even if the service provider has no active role, it cannot rely on the exemption ‘if it was aware of facts or circumstances based on which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously by Article 14(1)(b) of Directive 2000/31.’⁵²

Daimler v. Együd

- 25 In the *Daimler v. Együd* case, the CJEU had to rule on whether a garage owner was liable after the termination of its customer service agreement with Mercedes-Benz for internet advertisements posted under its name in which it was still presented as an ‘authorised Mercedes-Benz garage owner’.⁵³ The garage owner tried several times to end any use of the brand that could give the public the impression that a contractual link still existed. Despite several

42 C-63/97 *BMW v. Deenik* [1999] ECLI:EU:C:1999:82, para. 39.

43 C-236-238/08 *Google v. Louis Vuitton* [2010] ECLI:EU:C:2010:159.

44 C-236-238/08 *Google v. Louis Vuitton* [2010] ECLI:EU:C:2010:159, paras. 55-56. In the analogue world, the CJEU ruled that merely filling cans with a trademark depicted on them could not lead to trademark infringement, as the intermediary only provides the technical facilities to enable the use of the trademark by a third party. See: C-119/10 *Winters v. Redbull* [2011] ECLI:EU:C:2011:937, paras. 28-30.

45 C-236-238/08 *Google v. Louis Vuitton* [2010] ECLI:EU:C:2010:159, para. 57.

46 C-236-238/08 *Google v. Louis Vuitton* [2010] ECLI:EU:C:2010:159, para. 51.

47 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474.

48 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474, para. 105.

49 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474, paras. 92-94, 97.

50 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474, paras. 89-90.

51 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474, para. 116.

52 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474, para. 124.

53 C-179/15 *Daimler v. Együd* [2016] ECLI:EU:C:2016:134.

attempts to remove the internet ads, they continued to pop up beyond their control. According to the CJEU, a trader uses a trademark only if it involves active behaviour and direct or indirect control over the third party's actions.⁵⁴ This is not the case if the trader has expressly asked for the advertisement removed and it is still placed on the internet by third parties without its will.⁵⁵ However, a trader must be able to stop trademark use and comply with the prohibition.⁵⁶

Coty v. Amazon

- 26 Coty held various registered trademarks for its luxury cosmetic products. Coty products fell victim to counterfeit products offered for sale on Amazon's online marketplace. Coty argued that Amazon had infringed upon its trademarks by allowing third-party sellers to list these counterfeit or unauthorised products on its online platform. The central question was whether a party who stores goods for a third party that infringes a trademark right without being aware of that infringement falls within the scope of Article 10(3)(b) EUTMD. The Advocate General ("A-G") answers this in the negative. In doing so, he points to the wording "for those purposes", which refers to the requirement that this third party must itself have the intention to offer or market the goods.⁵⁷ The CJEU agrees with this reasoning, referring to the fact that the BJC found that Amazon lacked any intention to offer these goods. For use in its economic activity, the operator of an online marketplace must be active in the presentation, advertising, or optimisation of products offered for sale by third-party sellers.⁵⁸

II. Louboutin v. Amazon

1. Context of the Case

- 27 Christian Louboutin ("Louboutin") worked on

prototype heels in his Parisian workshop in 1992.⁵⁹ His assistant was wearing a bright shade of red nail polish, which gave Louboutin the following idea: he picked up the nail polish and started to paint the previously black sole in this bright red colour with the small nail polish brush. This turned out to be a golden move: these red soles of the high heels have become a huge success. Today, Louboutin is an established high-end fashion designer brand for luxury footwear and handbags. The red-soled, high-heeled shoes have been registered as a trademark, including Pantone 18-1663TP for the iconic red colour. This concerns both a registered Benelux and an EU trademark.⁶⁰ Besides the iconic look of the shoes, the Louboutin brand attracts attention due to the exclusivity of the shoes. Due to the high prices (the heels are offered between €695 and €2195)⁶¹, the brand attracts a specific target group. In the case at hand, Louboutin sought to sue internet giant Amazon.

- 28 Amazon, founded in 1994 by Jeff Bezos, has grown from an online bookseller to the world's largest online retailer.⁶² Among many other platforms, Amazon operates the Amazon Marketplace, which enables third-party retailers to showcase and sell their products alongside Amazon items. The shipping of the products may be handled either by those third parties or by Amazon, which then stocks the goods in its distribution centres and ships them to purchasers from its warehouses. In addition, Amazon uses a uniform method for presenting the sales offers published on its website, simultaneously displaying its sales offers and those of third-party sellers. Its logo as a reputable distributor appears on all such sales offers.⁶³ Jeff Bezos claimed from the very beginning that Amazon was not merely a retailer of consumer products but argued that Amazon was a technology company whose business was simplifying online transactions for consumers. As shown in the previous section, Amazon has often been involved in infringement cases. Allowing third parties to offer their products on Amazon's online

54 C-179/15 *Daimler v. Együd* [2016] ECLI:EU:C:2016:134, paras. 39-40.

55 C-179/15 *Daimler v. Együd* [2016] ECLI:EU:C:2016:134, para. 39.

56 C-179/15 *Daimler v. Együd* [2016] ECLI:EU:C:2016:134, para. 41.

57 C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267, Opinion of AG Campos Sánchez-Bordona, para. 67.

58 C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267, para. 37.

59 Christian Louboutin, 'La vie en red (sole)' <https://eu.christianlouboutin.com/nl_en/red-sole> accessed 23 July 2023.

60 Benelux registration 874489 of 6 January 2010 (Louboutin); EUTM registration 008845539 of 10 May 2016 (Louboutin).

61 Christian Louboutin, 'Pumps' <https://eu.christianlouboutin.com/nl_en/ladies/shoes/pumps/> accessed 23 July 2023.

62 M. Hall, 'Amazon.com' Britannica (2023) <<https://www.britannica.com/topic/Amazoncom>> accessed 23 July 2023.

63 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 35.

platform (the online marketplace) has created the risk of illegal content, such as counterfeit products, entering the digital market. As in several previously discussed cases, the central issue is the extent to which Amazon, as an online marketplace operator, is directly liable for counterfeit products.

- 29 The case concerns a merger of two cases, as *Louboutin* sought to sue different subsidiaries of Amazon. The cases have been pending before the District Court of Luxembourg (C148/21) and the Brussels Companies Court (C-184/21). Both courts have raised preliminary questions regarding interpreting Article 9(2)(a) EUTMR, particularly ambiguity concerning the concept of use and Amazon's role as an online intermediary.⁶⁴ The courts question whether the operating method of the Amazon online sales websites may lead to use by the operator of those platforms owing to the inclusion of third-party sellers' advertisements by displaying that sign in its commercial communications. In addition, the courts question whether the public's perception is essential for interpreting an "active role". Lastly, they question whether an operator like Amazon should be regarded as using a sign identical to a protected trademark if it undertakes to ship the goods bearing that sign.

2. Judicial Reasoning

- 30 On 22 December 2022, the CJEU answered the questions raised by the District Court of Luxembourg and the Brussels Companies Court. With its preliminary ruling, the CJEU effectively provides an interpretation of Article 9(2)(a) EUTMR. The critical question at the heart of the case can be formulated as follows. Can the operator of an online sales website that integrates an online marketplace, in addition to its own sales offers, be deemed to be itself using a sign identical to an EU trademark of another for the same goods as those for which that trademark is registered when third-party sellers in that marketplace offer such goods for sale bearing that sign without the consent of the proprietor of that trademark?⁶⁵
- 31 In answering this question, the CJEU first notes that the EUTMR needs to define the use concept and then refers to various case laws to interpret this concept. The ordinary meaning of use (as was also evident from Section 2.2.) requires active behaviour and direct or indirect control over the act in which

the use consists.⁶⁶ As regards the display of signs identical or similar to a trademark in sales offers on online marketplaces, the CJEU refers to the *L'Oréal v. eBay* and *Coty v. Amazon* cases: such signs are used exclusively by the customer-sellers of the operator of that marketplace and, therefore not by the operator itself.⁶⁷ The CJEU adds that the mere fact that providing the technical facilities necessary for the use of a sign and being reimbursed for doing so does not mean that the party providing this service itself is using the sign, even if it is acting in its financial interest.⁶⁸ This is also the case when the online marketplace operator offers storage services to infringing third-party sellers, provided that the online intermediary was unaware of the infringement and did not intend to market these products.⁶⁹

- 32 So far, the CJEU appears to be mainly aligning itself with the *L'Oréal v. eBay* and *Coty v. Amazon* cases by formulating the same standards. This unanimity seems to end when, from §33, the CJEU seeks to highlight the differences in the facts and circumstances of these cases and the present case. After that, the CJEU defines the concept of "commercial communication". This includes any communication to third parties promoting its activity, goods, or services. This presupposes that, from the point of view of third parties, the sign in question is displayed as an integral part of that communication and, thus, as part of that company's activity.⁷⁰
- 33 According to the CJEU, a service provider does not use the sign if the service provided cannot, by its nature, be compared to a service to promote the marketing of goods bearing that sign and does not imply a link between that service and that sign.⁷¹ To establish such a link, the CJEU presents a new standard. To determine whether an online sales website operator

64 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, paras. 17, 21.

65 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 23.

66 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 27.

67 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 30, with referring to C-324/09 *L'Oréal v. eBay* [2011] ECLI:EU:C:2011:474, paras. 102, 103 and C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267, para. 40.

68 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 31.

69 C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267, paras. 45, 53.

70 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 39.

71 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 40.

with an integrated online marketplace uses an infringing sign, it is necessary to determine whether a customarily informed and reasonably attentive website user would establish a link between the operator's services and the sign-in question.⁷² This formulated standard is highly noteworthy, as this is the first time that the consumer-user of the online marketplace has been considered a relevant factor in determining the liability of the online marketplace operator.⁷³ It would seem that the CJEU felt it necessary to justify itself. The CJEU mentions that when assessing a similar situation (namely in *L'Oréal v. eBay*), it did not include the user's perception of the online marketplace but did not seek to exclude this perception.⁷⁴ This differs from the *A v. B* case in which the CJEU still held that the assessment of whether there is trademark use can only be based on objective data.⁷⁵

- 34 The CJEU then elaborates on the newly formulated assessment. It constitutes an overall assessment of the circumstances of the present case, with reference to how the advertisements, individually and as a whole, are presented on the website in question and the nature and scope of the services provided by the website operator.⁷⁶ The CJEU concludes the judgement by addressing these two factors. Regarding presenting those published advertisements, it could make a difference if the operator used a uniform method, simultaneously displaying its advertisements and those third-party sellers and indicating its logo as a reputable distributor with the offers.⁷⁷ Moreover, terms such as

“bestseller”, “most sought after”, or “most popular” can reinforce the impression that the promoted products are offered on behalf of the operator of the online marketplace.⁷⁸ In addition, the nature and scope of the services offered to third-party sellers by the online marketplace operator are essential in the assessment. For example, the operator's handling of users' queries about the goods in storage, shipping, and return policy may be an indication to the user to determine the origin of those goods.⁷⁹

- 35 The summary answer to the central question is thus as follows: Article 9(2)(a) EUTMR must be interpreted as meaning that the operator of an online marketplace which integrates an online marketplace in addition to its own sales offers may be deemed to be itself using an infringing sign when third-party sellers on that marketplace offer goods containing such signs without the consent of the trademark holder if a customarily informed and reasonably attentive user of that website establishes a link between the services of that operator and the sign in question.⁸⁰

III. The Importance of the Judgement

- 36 The outcome of the *Louboutin v. Amazon* case is noteworthy, given that there was a legitimate expectation of a negative answer to the questions raised by the national courts. This is because even the A-G in this case, believed that Amazon does not use the sign and, therefore, cannot be (directly) liable.⁸¹ This is considered remarkable within the EU, as the European Commission's website highlights the particularity of this event: ⁸²*“Although not binding, the Advocate General's opinions are usually in line with the rulings of the CJEU. But this time, it was not the case!”*

ECLI:EU:2022:1016, para. 51.

72 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 43.

73 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 44: ‘... that the Court's existing case-law has not taken the perception of users into consideration.’. See also: R. de Beer & J. Visser, ‘Terugblik Merkenrecht 2022-2023, BIE 2023/4, p. 197: ‘...more generally, one can speak of a principled reversal in the ECJ's approach: third-party communication on the platform becomes, through the user's perception, the platform's commercial communication.(transl.)’

74 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 45.

75 C-772/18 *A v. B* [2020] ECLI:EU:C:2020:341, para. 22. See also: E. Rosati, ‘The Louboutin/Amazon cases (C-148/21 and C-184/21) and primary liability under EU trade mark law’, *European Intellectual Property Review* (2022) 44(7), 435-440.

76 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 49.

77 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022]

78 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 52.

79 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 53.

80 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 54.

81 Court of Justice of the European Union, ‘Advocate General's Opinion C-148/21 and C-184/21’ <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220096en.pdf>> accessed 23 July 2023.

82 European Commission, ‘Louboutin – Amazon case (C-148/21 and C-184/21)’ <https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/louboutin-amazon-case-c-14821-and-c-18421-2023-01-31_en> accessed 23 July 2023.

37 One can draw the following conclusion from the judicial reasoning of *Louboutin v. Amazon*. As a result of this judgment, holding an online intermediary that takes the form of an operator of an online marketplace directly liable has become conceivable. With the introduction of a new criterion to determine “own commercial communication” — essential for “use” as defined by Article 9 EUTMR and consequently for trademark infringement — it becomes evident that, under specific conditions, an online intermediary can be deemed as a user of the infringing sign, regardless of the infringing product’s third-party origin. The CJEU stated that it is ultimately for the referring courts to assess whether Amazon, in its capacity as operator of an online marketplace, uses a sign identical to the trademark at issue about goods which are identical to those for which that trademark is registered within the meaning of Article 9(2)(a) EUTMR.⁸³ The CJEU promptly clarified that it would furnish the courts with interpretative insights pertinent to EU law, aiding their assessments. Considering the anticipated interpretation of the directive by national courts, it’s plausible that the ultimate resolution of these cases will resonate with the CJEU’s stance. The nature of this being a preliminary ruling suggests that its rhetoric has broad applicability, potentially influencing subsequent national court decisions.

38 Section D will elucidate that online platforms, particularly online marketplaces, are anticipated to exercise substantial due diligence. While a trademark holder has the prerogative to enforce specific measures against trademark infringement, previous cases suggest that the CJEU does not typically infer primary liability from online intermediaries. Consequently, in addition to seeking injunctive relief, a trademark holder can pursue financial damages from the online marketplace using their legitimate trademark rights.⁸⁴ This judgement implies a potential realignment in party liability. Given the incredible allure of trademark holders targeting prominent enterprises like Amazon rather than potentially obscure, minor entities that market the infringing products, this ruling could incentivise trademark holders to pursue litigation more aggressively. Consequently, this decision paves the way for previously inaccessible legal avenues.

39 Traditionally, trademarks primarily functioned as

indicators of the origin of goods or services, assuring consumers of authenticity and enabling them to differentiate between products from diverse sources. While this concept remains foundational in European law, modern trademark law also emphasises protection against dilution and unauthorised exploitation as a critical function.⁸⁵ The CJEU has given increasing significance to the goodwill function of the trademark.⁸⁶ Trademark law seeks to strike a balance among its primary stakeholders: consumers, trademark holders, and third parties. In light of the *Louboutin v. Amazon* verdict and the introduction of the DSA, there appears to be a discernible shift towards enhanced consumer protection. This is evidenced by the reinforced safeguards against consumers erroneously associating infringing branded products with esteemed platforms, which could lead to confusion and damage the brand’s reputation. Simultaneously, trademark holders benefit from expanded protection for their marks. Nonetheless, it warrants consideration whether this recalibrated equilibrium unduly impinges upon competition.⁸⁷ Much will depend on the interpretation of the new standard and to what extent the average consumer is aware of the platform’s business model in question.⁸⁸

85 P.G.F.A. Geerts & A.M.E. Verschuur (eds.), *Kort begrip van het intellectuele eigendomsrecht* (Deventer: Wolters Kluwer 2022) 278..

86 C-337/95 *Dior v. Evora* [1997] ECLI:EU:C:1997:517; C-487/07 *L’Oréal v. Bellure* [2009] ECLI:EU:C:2009:378; C-323/09 *Interflora v. Marks & Spencer* [2011] ECLI:EU:C:2011:604; C-193/19 *Mitsubishi* [2020] ECLI:EU:C:2020:594.

87 And thereby indirectly harm the interests of consumers who benefit from access to sufficient alternative products. In addition, too high a monitoring obligation could lead to a disproportionate burden on intermediaries which is not justified in the light of the nature of the services provided by such intermediaries, their expertise and the remuneration usual in the industry for the services. See G. van der Wal, S. Said, ‘De voortdurende vraag naar de rol van de tussenpersoon in het merkenrecht’, IER 2021/3, para. 6.3.

88 For example, A-G Szpunar ruled that the mere fact that Amazon’s logo is attached to all advertisements does not indicate that the consumer is going to see offers from third-party sellers as Amazon’s own communication (C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:C:2022:422, Opinion of A-G Szpunar, paras. 85-86). Instead of the consumer who has little interest in knowing with whom the sale is concluded, because for them only the product and its price are decisive, it is also possible, for example, to adopt as a benchmark precisely the consumer for whom this is decisive to establish. See also: C-148/21 and C-184/21 *Louboutin v. Amazon* ECLI:EU:C:2022:422, Opinion of A-G Szpunar, para. 72. The latter consumer is less likely to assume a link, as this consumer will be more attentive to this point. The modern internet user may know that

83 C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 38.

84 M. Stief, ‘Louboutin v. Amazon: direct liability of online platforms for third-party trademark infringement’ (2023) <<https://www.managingip.com/article/2bcah77qtiqh5qil65ts/expert-analysis/local-insights/louboutin-v-amazon-direct-liability-of-online-platforms-for-third-party-trademark-infringement>> accessed 23 July 2023.

D. Obligations Imposed by Regulations

- 40 Now that it has emerged in the previous Section that the CJEU places greater responsibility on online intermediaries, what obligations this entails for them remains. The answer to this question can only be found by involving the ECD and the DSA. Indeed, the analysis of several CJEU rulings shows that the CJEU wanted to stress the importance of the responsibility of the online platforms, even if it did not establish the liability of that online platform.⁸⁹ Given the nature of the ECD and the recent advent of the DSA, combined with the developments of the discussed case law, it is necessary to include these regulations in the research to determine a comprehensive final answer to the article's central question. This Section, therefore, elaborates on the obligations these regulations entail and whether these regulations should be interpreted differently in the context of the previous Sections. First, a brief introduction to both regulations will follow. Then,

the ads displayed on a platform can come not only from the platform itself but also from third parties with which the platform has nothing to do. For instance, Amazon can be seen as a highly renowned distributor but it is also renowned for its marketplace activity. Consumers therefore probably know that the website both makes sales offers for goods sold directly by Amazon and has sales offers posted by third-party sellers (See: C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:C:2022:422, Opinion of A-G Szpunar, para. 86). The CJEU ruled also in the *Google France and Google* case that where the provider of a search engine advertising service which stores, on behalf of a number of customers, signs corresponding to trademarks as keywords and displays advertisements on the basis thereof, is merely carrying out its usual activity and therefore, in the eyes of an informed internet user familiar with the use of that service, does not appear to be using the signs in question for its own commercial communication (C-236/08-C-238/08, *Google France and Google* [2010] EU:C:2010:159, para. 55; C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:C:2022:422, Opinion of A-G Szpunar, para.70). For instance, in the *Tempur/Medicomfort* case, the Court of Appeal of The Hague ruled that the normally informed and observant internet user was aware that when they typed in a brand name as a keyword on the search page of a search engine provider, not only search results linked to the brand owner would appear, but also third-party advertisements (Court of Appeal of The Hague, 22 November 2011, 200.083.709-01, ECLI:NL:GHSGR:2011:BU6275 (*Tempur/Medicomfort*), para. 17. See also: G. van der Wal, S. Said, 'De voortdurende vraag naar de rol van de tussenpersoon in het merkenrecht' (2021) IER 3, 5.2.

⁸⁹ For example, in C-324/09 *L'Oréal v. eBay* [2011] ECLI:EU:C:2011:474 and C-567/18 *Coty v. Amazon* [2020] ECLI:EU:C:2020:267.

several provisions will be discussed, in which the most critical exemptions and obligations for online intermediaries will come to light. The Section concludes with an overview of the implications of *Louboutin v. Amazon* for the discussed provisions.

I. Background and Relevance of ECD and DSA

- 41 The ECD established a legal framework governing digital services. Its primary objective was to harmonise regulations across EU Member States and provide a basis for free movement of online services. The ECD presented an initial definition for online providers acting as intermediaries: the "Information Society Service Providers" ('ISSPs'). As previously noted, the ECD could not provide a clear and specific definition of an online intermediary to classify intermediaries such as the operator of an online marketplace. With an effective date in 2000, the ECD was drafted at a time when online platforms with the size and influence of today did not exist. The fast-growing and fast-developing digital environment requires modernisation. Given the emerging challenges, the EU recently presented a new regulation: the DSA. With a publication date of October 2022 and the entry into force of 16 November 2022, the DSA has rapidly sailed through the European legislative process. The need for an updated regulation for (among others) online intermediaries was highly desirable. The DSA aims to provide better protection to users and fundamental rights online, establish a robust transparency and accountability framework for online platforms and provide a single, uniform framework across the EU.⁹⁰ Therefore, the main aim of the DSA is to modernise the regulatory framework for digital services. In doing so, the DSA notably follows on from the ECD, which has similar content but was considered somewhat outdated.

- 42 The DSA relates to the ECD in two ways.⁹¹ For one, the DSA is required to safeguard the provisions of the ECD and seeks to preserve the ECD's intermediary liability framework. This is reflected, for example, in Articles 4, 5 and 6 DSA, which essentially correspond to Articles 12, 13 and 14 ECD. Incidentally, Article 6(3) DSA contains a new consumer protection law

⁹⁰ European Commission, 'Questions and Answers: Digital Service Act' (2023) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> accessed 23 July 2023.

⁹¹ F. Wilman, 'Between preservation and clarification: The evolution of the DSA's liability rules in light of the CJEU's case law'(2022) <<https://verfassungsblog.de/dsa-preservation-clarification/>> accessed 23 July 2023.

regulation. This provision covers the liability of online platforms that allow consumers to conclude distance contracts with traders (in other words, online marketplaces). On the other hand, the DSA aims to clarify issues from the ECD, as has become apparent, for example, in establishing the definition of “online intermediary”.

- 43 An essential difference between the ECD and the DSA can be found in their nature. The ECD is a so-called directive and thus must be implemented in national law. Therefore, directly relying on these provisions is impossible; the relevant national law must be invoked.⁹² In contrast, the DSA is a regulation that can be directly invoked. After it enters into force, all European Union citizens can invoke the provisions of the DSA.⁹³
- 44 In previously discussed case law, the CJEU connected the interpretation of trademark infringement and the definitions and scope of different European legislation.⁹⁴ This makes the provisions from the ECD and the DSA, among others, relevant to the legal standing of online intermediaries towards trademark holders. In this regard, other regulations regarding intermediaries’ liabilities and obligations may also be relevant. For example, the DSM Copyright Directive⁹⁵ (‘DSM’) looks at the *lex specialis* liability of “online content-sharing services”. However, the DSM does not clearly define this term. Authors assume that many hosting services and online platforms do not fall under this definition.⁹⁶ Therefore, given the nature of an online marketplace and the type of infringement subject to this article, the DSM will be further disregarded.

92 A.S. Hartkamp, *C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 3. Vermogensrecht algemeen. Deel I. Europees recht en Nederlands vermogensrecht* (Deventer: Wolters Kluwer 2023) 152.

93 A.S. Hartkamp, *C. Assers Handleiding tot de beoefening van het Nederlands Burgerlijk Recht. 3. Vermogensrecht algemeen. Deel I. Europees recht en Nederlands vermogensrecht* (Deventer: Wolters Kluwer 2023) 152.

94 For example, in C-148/21 and C-184/21 *Louboutin v. Amazon* [2022] ECLI:EU:2022:1016, para. 37.

95 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

96 R. Chavannes, A. Strijbos & D. Verhulst, ‘Kroniek technologie en recht’ (2023) *NJB* 1084 2.2.b.

II. Key Provisions

- 45 The ECD has established several pivotal obligations tailored to online service providers, often called ISSPs. The ECD outlines a limited liability framework for intermediaries, carving out provisions that exempt ISSPs and hosting platforms from liability for illicit content, provided they were unaware of its existence. Furthermore, the ECD introduced the “Notice and Takedown Procedure,” mandating intermediaries promptly remove or restrict access to illegal content upon receiving a notification.⁹⁷ In addition to introducing precise definitions for “online platforms” and “online intermediary services”, the DSA offers significant advancements. While the ECD hesitates to allocate responsibilities to ISSPs, the DSA emphasises enhanced accountability for online platforms. A defining feature of the DSA is its principle: the more intimately a service provider engages with user content, the more pronounced its obligations become.⁹⁸ The DSA introduces the notion of “Very Large Online Platforms” (VLOPs) and imposes extensive obligations and regulations upon them. Additionally, the DSA sets forth new requirements for other online platforms, encompassing transparency stipulations, risk assessments, and protective measures against illicit content.

1. An Online Intermediary

- 46 By operating the platform for the online marketplace, the operator offers what is termed an “information society service” (ISSP) under EU Directive 2015/1535.⁹⁹ This service typically involves transactions conducted remotely, electronically, and upon specific requests from service recipients. The ECD has traditionally encapsulated this concept using the abbreviation “ISSP”.

97 However, Wolters and Gellert are critical of the N&A process in the DSA. They point out that content providers lack effective and accessible options to challenge decisions that are negative for them. A clear justification is lacking in many cases when their content is removed from the platform. See: P.T.J. Wolters & R.M. Gellert, ‘Het “notice and action-mechanisme” van de DSA: een adequaat evenwicht tussen de betrokken belangen?’ (2022) *Computerrecht* 218, 4.3, 5.2.

98 R. Chavannes, A. Strijbos & D. Verhulst, ‘Kroniek technologie en recht’ (2023) *NJB* 1084 2.3.

99 Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure or the provision of information in the field of technical regulations and of rules on Information Society services (codification).

47 Since operators of online marketplaces perform an essential link in trading or offering goods to the public, it was suspected that these operators act as intermediaries.¹⁰⁰ However, there was little consensus among legal scholars, courts, and legislators on defining an “online intermediary” and under what circumstances they would fall within the scope of ISSPs.¹⁰¹ With the recently enacted DSA, more clarity can be provided. The DSA formulates an initial definition for “intermediary services”. This includes, among others, a hosting service “consisting of the storage of information provided by, and at the request of, a recipient of the service”.¹⁰² The fact that an online marketplace can be considered a “hosting service” and, therefore, an “intermediary service” is rendered by Article 3(i) DSA, which contains a comprehensive definition of the term “online platform”. According to this provision, online platforms are a form of hosting services and are considered intermediary services.

48 This analysis is supported by the Digital Market Act¹⁰³ (“DMA”), which, referring to Regulation (EU) 2019/1150¹⁰⁴, addresses the specific definition of “online intermediation services”.¹⁰⁵ The online marketplace operates as an information society service, allowing business users to present goods to consumers and foster direct transactions. This service is rendered to the business user through established contractual agreements with the provider. Consequently, the online marketplace is designated a “provider of online intermediation services,” satisfying all stipulated criteria.¹⁰⁶ Whereas formerly, it was merely an assumption, it can now be said with certainty that the operator of an online marketplace can be defined as an *online intermediary*.

100 G. van der Wal, ‘De voortdurende vraag naar de rol van de tussenpersoon in het merkenrecht’ (2021) IER 3,2.1.

101 Frosio (red.), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 6.

102 Article 3(g)(iii) DSA.

103 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.

104 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.

105 Article 2(5) DMA.

106 Article 2(2) Regulation 2019/1150.

2. Safe Harbour

49 Article 6 DSA states:

“Where an ISSP is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider does not have actual knowledge of illegal activity or illegal content (...) or upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.”

50 This provision thereby describes the so-called *safe harbour*. An online intermediary can “escape” liability under certain circumstances if it meets the conditions of this liability exemption. The DSA’s liability exemptions apply to intermediary liability, regardless of the nature of the liability.¹⁰⁷ This renders the DSA relevant for trademark law. Failure to meet the conditions of the liability exemptions does not automatically mean that the online intermediary is liable.¹⁰⁸ The provisions of the DSA should not be reasoned a-contrario in that context. The liability question must, therefore, be answered by reference to applicable rules of EU or national law.¹⁰⁹

51 The safe harbours for hosting providers (such as online platforms) have been moved from the ECD to the DSA. As a result, the direct effect of the DSA entails that the national implementations of Articles 14-16 ECD have become obsolete (for the Netherlands, this is Article 6:196c Dutch Civil Code) and can now be invoked directly under the DSA. Given that the text of Article 6 DSA is almost like Article 14 ECD, it can be assumed that the interpretation of Article 14 ECD applies *mutatis mutandis* to Article 6 DSA. Online platforms facilitating buying and selling between two parties (such as online marketplaces) can invoke the safe harbour provision of Article 6 DSA.¹¹⁰

52 The applicability of Article 6 DSA is assessed according to the degree of the “active role” the provider of the online platforms had. The “active role” criterion is an open standard interpreted several times by the CJEU. An online marketplace can successfully invoke the safe harbour provision if that operator does not play an active role that enables

107 Recital 17 DSA.

108 Recital 17 DSA.

109 C-622/16 *Google v. Google France* [2010] ECLI:EU:C:2010:474, para. 107.

110 N.A. de Werd & T.C. Bokhoeve, ‘Wat is de rol en verantwoordelijkheid van online platforms in de digitale strijd tegen namaakproducten?’ (2022) *Computerrecht* 2.1.

it to have knowledge of or control over the stored data.¹¹¹ To do so, however, the online intermediary must quickly delete that data or make access to it impossible as soon as it becomes aware of the unlawful nature of that data.¹¹² This interpretation is codified in Recital 18 DSA:

“The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. ... “

- 53 The European legislator’s decision to use the term “neutrally” rather than “passively” in its wording merits attention. This choice indicates a more cautious approach when evaluating the “active role” criterion, particularly for hosting services like online marketplaces. Recital 21 DSA further underscores this caution, emphasising only conduit and caching and stipulating that for service providers to claim exemptions, they must not be involved with user content. Notably, online hosting services face a somewhat lenient standard; they can interact with such content and potentially claim the safe harbour provision. The crux of determining the service provider’s “active role” and eligibility for liability exemptions lies in the online marketplace’s activity. Thus, complete passivity is optional to qualify for the Article 6 DSA safe harbour.
- 54 Taking voluntary action on one’s initiative to deal with illegal content or to comply with EU or national law is not a ground to be excluded from the Article 6 DSA safe harbour exemption. This “Good Samaritan” clause from Article 7 DSA builds on the potential reluctance of service providers to take an active role and aims to remove a disincentive for such voluntary action.¹¹³ According to Article 7 DSA, this reluctance

is unwarranted, provided an online intermediary acts in good faith and with due care.¹¹⁴ Nevertheless, it cannot be ruled out that online platforms remove more content from their websites to avoid liability. This would contradict one of the DSA’s goals, i.e., to safeguard more protection of fundamental rights online, including freedom of expression.¹¹⁵

3. Due Diligence

- 55 The DSA formulates several *due diligence* obligations the online intermediary must comply with. These obligations mainly focus on the process and design of the service offered rather than the content itself.¹¹⁶ Taking measures to comply with the due diligence obligation is separate from the liability question and, therefore, does not affect the assessment of the active role of the online intermediary.¹¹⁷ However, these different obligations provide a clear picture of what is expected of the online intermediary. The degree of responsibility depends on the extent and social impact of the service. In general, four “layers”

evolution of the DSA’s liability rules in light of the CJEU’s case law’ *Verfassungsblog* (2022) <<https://verfassungsblog.de/dsa-preservation-clarification/>> accessed 23 July 2023. While a platform that actively tracks down information and removes infringing information loses its neutral position, it does not automatically mean that a benevolent platform is directly liable or more quickly liable than a platform that keeps its distance. Indeed, there is still a need to investigate whether there has been unlawful conduct. Nevertheless, an involved host may be more likely to have knowledge or be deemed to know the infringing information, so it may still be liable more quickly than a passive host. See: M.Y. Schaub, *Onlineplattformen - Monografieen Privaatrecht nr. 19* (Wolters Kluwer 2020), nr. 71.

111 C-324/09 *L’Oréal v. eBay* [2011] ECLI:EU:C:2011:474.

112 C-236-238/08 *Google v. Louis Vuitton* [2010] ECLI:EU:C:2010:159. For instance, the Dutch Supreme Court argued that operating a spam filter and providing a search function did not result in the platform NSE having knowledge of or control over the messages stored on that platform. The Supreme Court also held that the platform took the technical measures that could be expected of a diligent economic operator in its situation to credibly and effectively counter copyright infringements on its platform. The fact that the NTD procedure could possibly be improved, and additional measures were conceivable did not detract from this (Dutch Supreme Court, 17 January 2023, 17/01135, ECLI:NL:HR:2023:94 (*Brein v. NSE*), para. 3.6.3.

113 F. Wilman, ‘Between preservation and clarification: The

114 In any case, the diligent economic operator is not acting in good faith if it operates a business model based on promoting infringements by users of the platform. See J. Nordemann, *Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?*, Study prepared for the European Parliament, 2018. Available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_IDA%282017%29614207, pp. 11.

115 A. Kuczerawy, ‘The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act’ (2021) <The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act – *Verfassungsblog*>, accessed 5 September 2023.

116 M. Husovec & I. Roche Laguna, ‘Digital Service Act: A Short Primer’, in *Principles of the Digital Service Act* (Oxford University Press: Forthcoming 2023) 4.

117 Rectical 41 DSA.

of due diligence obligations can be distinguished:¹¹⁸

- 56 *Universal obligations* apply to all providers of intermediary services that may qualify for the liability exemptions.¹¹⁹ These obligations include assigning a single point of contact for authorities and users.¹²⁰ In addition, the provider must explain the moderation of third-party content and the use of automation.¹²¹ Medium-sized or more prominent firms¹²² must also publish an annual report containing various aspects that enhance transparency in the market.¹²³
- 57 *Additional obligations* apply to all hosting services.¹²⁴ The DSA defines how the hosting provider must receive notifications of illegal content on the service provided.¹²⁵ Once the provider is notified of the illegal content, it may lose the right to its liability exemption if it does not act against this content.
- 58 *Advanced obligations* apply to medium-sized or bigger hosting service providers with an online platform.¹²⁶ This set of obligations is by far the most comprehensive. Several categories of obligations can be distinguished: Content Moderation, Fair Design of Services, Advertising, Amplification and Transparency. In the Advertising category, the online platform is required to make it clear who paid for the advertisement, the content creator must be enabled to include advertisements in uploaded content, and the advertisement must not be based on profiling using sensitive data as

input.¹²⁷ These advanced obligations also include a set of transparency obligations designed explicitly for online marketplaces.¹²⁸ For instance, a “Know-Your-Business-Customer” obligation is formulated whereby the traceability of merchants must be improved.¹²⁹ The provider of an online marketplace must undertake measures to promote such traceability by, for example, storing ID documents and payment details. If a third party has a legitimate interest in receiving this information, this data should be provided to that third party.

- 59 *Special obligations* apply to VLOPs, online platforms with an average of 45 million active monthly users.¹³⁰ VLOPs are designated as such by the European Commission in the Official EU Journal. VLOPs must identify, analyse, and assess systemic risks from their services’ design, functioning, and use.¹³¹ This risk assessment must be carried out at least once a year and at the expense of the VLOP. The assessment focuses on illegal content, actual or foreseeable adverse effects on all fundamental rights, pre-defined protected issues, and serious negative consequences to users’ physical and mental well-being. In addition, the VLOP should, among other measures, maintain a crisis response mechanism, provide access to data to supervisory authorities and vetted research, and appoint a compliance officer responsible for complying with the DSA obligations. The European Commission is the sole authority in monitoring and enforcing these specific obligations.

III. Implications for Online Intermediaries

- 60 On 23 April 2023, the European Commission designated 17 VLOPs.¹³² These include several online marketplaces like Amazon, Zalando and Alibaba AliExpress. They will have to comply with all obligations outlined by the DSA for VLOPs within four months from the date of notification of the designation. Amazon opposes this designation and asserts that they are a retailer rather than a

118 M. Husovec & I. Roche Laguna, ‘Digital Service Act: A Short Primer’, in: *Principles of the Digital Service Act* (Oxford University Press: Forthcoming 2023) 4.

119 Chapter III, Section 1 DSA.

120 Article 11 and 12 DSA.

121 Article 14 DSA.

122 Small firms are fewer than 50 employees, and turnover and or/annual balance sheet total does not exceed 10 million Euros. However, if the small firm is qualified as VLOP, it remain under the obligation. See: European Commission, ‘Internal Market, Industry, Entrepreneurship and SMEs’ <https://single-market-economy.ec.europa.eu/smes/sme-definition_en> accessed 23 July 2023.

123 Article 15 DSA.

124 Chapter III, Section 2 DSA.

125 Article 16 DSA.

126 Chapter III, Section 3 DSA.

127 Articles 26 and 28 DSA.

128 Chapter III, Section 4 DSA.

129 Article 30 DSA.

130 Chapter III, Section 5 DSA.

131 Article 34 DSA.

132 European Commission, ‘Digital Service Act: Commission designates first set of Very Large Online Platforms and Search Engines’ (2023) <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413> accessed 23 July 2023.

communication platform and, therefore, does not fall under the targeted group of obligations.¹³³ Zalando also resists the designation, asserting that the European Commission significantly overestimated the size of its user base. Amazon further claims that the designation is “based on a discriminatory criterion and disproportionately violates the principle of equal treatment and the applicant’s fundamental rights”.¹³⁴ Whether such arguments will hold in the lawsuits filed remains to be seen.

- 61 As highlighted in Section 3, the scope of online intermediary liability has been expanded by the CJEU. The fact that the perspective of the customarily informed and reasonably observant internet user is now considered an essential factor in assessing whether a given act can be classified as a “commercial communication” could potentially have implications for interpreting some provisions of the ECD and the DSA. This may affect, for example, the interpretation of an active role, which is relevant for possible reliance on Article 6 DSA.¹³⁵ If the perspective of the internet user is taken as a measure when assessing whether an online intermediary has an active role, it could be that this would lower the threshold for assuming the active role.

E. Conclusion

- 62 Online marketplaces are digital platforms where the operators facilitate interactions between (third-party) sellers and buyers (consumers). These operators function as “intermediaries” under the DSA’s classification. As the prevalence of such platforms increases, complex legal issues arise, particularly concerning the extent of these intermediaries’ liabilities. When trademark infringements occur, rights holders decide to pursue legal action against the individual seller or the more prominent online intermediary. Often, the latter is the more appealing target due to various reasons. Yet, evolving European regulations and diverse case

law have muddled the waters. This article addressed a pressing question: How do the EU trademark law and the Digital Services Act define the responsibilities of online marketplaces toward these rights holders?

- 63 Much debate has been about the level of responsibility online intermediaries have to provide trademark owners. Generally, only secondary liability was assumed, as the online intermediary was not held to be able to bear its own “primary” liability for conduct not directly attributable to itself. The analysis of case law reveals that the CJEU has had to rule on this matter often, but each time with the outcome mentioned. The CJEU did emphasise the importance of a responsible online intermediary but did not attach direct liability to it yet. In *Louboutin v. Amazon*, the question arose from two different national courts through preliminary questions on how the concept of use should be interpreted when an online intermediary operating an online marketplace is involved. The Louboutin heels fell victim to counterfeit products on Amazon’s online marketplace. The problem was the lack of clarity on whether Amazon played an active role by placing ads for counterfeit products on its website.

- 64 In its decision, the CJEU frequently references the benchmarks and arguments from the cases of *L’Oréal v. eBay* and *Coty v. Amazon*, suggesting a possible parallel outcome. However, the CJEU introduces a shift in its ruling by articulating a new criterion for defining “commercial communication” to determine an “active role” in infringement. The CJEU posits that this definition should encompass the viewpoint of an informed and discerning internet user. Additionally, the Court outlines various factors that could influence this interpretation. Notably, this approach of integrating the perspective of the informed user is novel in evaluating active behaviour in such cases.

- 65 This perspective becomes increasingly evident that online intermediaries like Amazon may bear primary liability for products infringing on copyrights offered by third parties. The CJEU appears to be recalibrating the balance between parties, tilting it towards enhanced consumer protection. This perspective has been identified as the pivotal factor in this shift.

- 66 European legislative bodies also reflect this inclination. The Digital Services Act (DSA) introduction underscores the heightened responsibility of online intermediaries. The DSA encompasses several obligations, some novel, distinguishing it from its precursor, the E-Commerce Directive (ECD). While these two regulations coexist and are intended to be complementary, it’s pivotal to recognise the DSA’s immediate enforceability upon its enactment. Consequently, specific provisions of the ECD might become obsolete, but interpretations

133 E. Woollacott, ‘Amazon ‘Isn’t A Very Large Online Platform’, *Forbes* (2023) <<https://www.forbes.com/sites/emmawoollacott/2023/07/12/amazon-isnt-a-very-large-online-platform/?sh=2cf812761ab4>> accessed 23 July 2023.

134 E. Woollacott, ‘Amazon ‘Isn’t A Very Large Online Platform’ *Forbes* (2023) <<https://www.forbes.com/sites/emmawoollacott/2023/07/12/amazon-isnt-a-very-large-online-platform/?sh=2cf812761ab4>> accessed 23 July 2023.

135 See also E. Rosati, ‘The Role, Responsibility and Liability of Online Intermediaries under EU IP Law’, in *Routledge Handbook of Fashion Law* (Routledge: Forthcoming 2024), ch. 7, who also indicates an emerging trend towards a greater responsabilisation of online intermediaries.

by entities, including the CJEU, continue to influence the DSA's interpretation. Specifically, the definition of an "active role," critical for invoking the safe harbour provisions, could be impacted by this judgment. Furthermore, the emergence of Very Large Online Platforms (VLOPs) mandates these platforms to adhere to heightened due diligence requirements. VLOPs are now tasked with formulating and upholding policies aligning with the new legislation and prevailing case law.

- 67 The legal position of online intermediaries about trademark owners has seen a notable transformation. This change is primarily attributed to the verdict in *Louboutin v. Amazon* and the introduction of the DSA and its subsequent obligations. These developments imply an augmented responsibility for online platforms, positioning them at potential direct liability for infringing products listed on their sites. Consequently, with a valid trademark, trademark owners now possess a substantial legal advantage. Considering this, it is plausible that, in the future, trademark owners will primarily target online marketplace operators when infringements occur on their platforms. This revised legal position has evoked strong reactions from numerous online platforms. As with many evolving legal landscapes, these changes present many unresolved questions. Thus, the definitive resolution on this issue still needs to be discovered.

Devaluing SEPs: Hold-up bias and side effects of the European Draft Regulation

by **Oscar Borgogno and Giuseppe Colangelo** *

Abstract: The EU Commission's recent proposal for a regulation on standard essential patents (SEPs) envisages a radical overhaul of the current framework, introducing an essentiality check system, a conciliation process for fair, reasonable and non-discriminatory (FRAND) terms, and a mechanism to determine a reasonable aggregate royalty. However, both the economic justification and the approach endorsed by the proposal are questionable. Indeed, on one hand, there is no evidence of a market failure to justify the initiative and, in addition, the

provisions appear to be one-sided, apparently being aimed only at addressing a hold-up problem and pursuing a value-distribution goal from SEP owners to implementers. Accordingly, this paper views the proposal critically, arguing that it departs from the well-established meaning and rationale of FRAND commitments by disregarding hold-out problems, and it jeopardises the suitability of SEPs to serve as valuable financial collateral, thereby endangering future investments in innovation.

Keywords: Standard Essential Patents; FRAND Royalty; Hold-Up; Hold-Out; Royalty Stacking; Intangible Asset Finance; Collateral

© 2024 Oscar Borgogno and Giuseppe Colangelo

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Oscar Borgogno and Giuseppe Colangelo, Devaluing SEPs: Hold-up bias and side effects of the European Draft Regulation, 15 (2024) JIPITEC 74 para 1

A. Introduction

- 1 After almost a decade of communications and studies commissioned on the functioning of standard essential patents (SEPs) licensing markets¹, some

* Oscar Borgogno: TOELI Research Fellow; PhD (University of Turin); MSc (Oxon); <https://orcid.org/0000-0003-0721-4442>; oscar.borgogno@unito.it. Giuseppe Colangelo: Jean Monnet Professor of EU Innovation Policy and Associate Professor of Law and Economics, University of Basilicata; TTLF Fellow, Stanford University and University of Vienna; <https://orcid.org/0000-0002-0089-3545>; giuseppe.colangelo@unibas.it. The authors gratefully acknowledge the financial support of the Research Network for Digital Ecosystem, Economic Policy and Innovation (Deep-In).

1 See, e.g., Justus Baron, Pere Arque-Castells, Amandine Leonard, Tim Pohlmann, and Eric Sergheraert, 'Empirical

Assessment of Potential Challenges in SEP Licensing', (2023) <https://www.iplytics.com/wp-content/uploads/2023/04/Empirical-Assessment-of-Potential-Challenges-in-SEP-Licensing.pdf>; Group of Experts on Licensing and Valuation of Standard Essential Patents, 'Contribution to the Debate on SEPs' (2021) <https://ec.europa.eu/docsroom/documents/45217>; Rudi Bekkers, Joachim Henkel, Elena M. Tur, Tommy van der Vorst, Menno Driesse, Byeongwoo Kang, Arianna Martinelli, Wim Maas, Bram Nijhof, Emilio Raiteri, and Lisa Teubner, 'Pilot Study for Essentiality Assessment of Standard Essential Patents', (2020) <https://publications.jrc.ec.europa.eu/repository/handle/JRC119894>; European Commission, 'Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience', COM(2020) 760 final; European Commission, 'Setting out the EU approach to Standard Essential Patents', COM(2017) 712 final; IPlytics, 'Landscaping study on Standard Essential Patents (SEPs)', (2017) <https://www.iplytics.com/wp-content/uploads/2017/05/Landscaping-Study-on-Standard-Essential-Patents-SEPs.pdf>.

months ago the European Commission decided to intervene, delivering a proposal for a regulation (Draft Regulation).² The Commission's wish list is ambitious, as the initiative aims to address the lack of transparency with regard to SEPs, fair, reasonable and non-discriminatory (FRAND) terms and conditions, licensing in the value chain, and the limited use of dispute resolution procedures for resolving disagreements.³ These are considered to be the causes of an inefficient SEP licensing ecosystem, which is likely to become even more problematic due to the emergence of the Internet of Things (IoT), as new players with few resources and little licensing experience (i.e. start-ups and SMEs) are entering the market for connectivity.⁴

- 2 As a result, the Commission is not aiming to maintain the system as it stands but is instead envisaging its overhaul by introducing an essentiality check system, a conciliation process for the FRAND determination, and a mechanism to determine a reasonable aggregate royalty.

content/uploads/2017/04/Pohlmann_IPlytics_2017_EU-report_landscaping-SEPs.pdf; European Commission, 'ICT Standardisation Priorities for the Digital Single Market', COM(2016) 176 final; Charles River Associates, 'Transparency, Predictability, and Efficiency of SSO-based Standardization and SEP Licensing', (2016) <https://ec.europa.eu/docsroom/documents/48794>.

- 2 European Commission, Proposal for a Regulation of the European Parliament and of the Council on Standard Essential Patents and Amending Regulation (EU) 2017/1001, COM(2023)232.
- 3 Ibid., Recital 2.
- 4 European Commission, 'Intellectual property – new framework for standard-essential patents', (2022) Call for evidence for an impact assessment, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13109-Intellectual-property-new-framework-for-standard-essential-patents_en. See also European Commission, 'Impact Assessment Report Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on Standard Essential Patents and Amending Regulation (EU) 2017/1001', SWD(2023) 124 final, 10, arguing that, as result of the IoT the landscape of SEP licensing is shifting since today "(i) some companies incorporate standards into their products while not owning SEPs covering such standards, (ii) others own and license SEPs without using them in any products, and (iii) major SEP holders have significantly reduced their product businesses and focus more on licensing their SEPs." Therefore, "[w] hereas over the last two decades most high-stakes SEP disputes have centred around mobile communication devices (i.e. smartphones), we are already witnessing more disputes in the automotive sector and expect other IoT sectors to be similarly affected."

- 3 However, the proposal has been met with much criticism, firstly questioning the existence of any problem to be solved and then warning against the approach adopted, which was thought to be imbalanced. Indeed, from this perspective, empirical evidence does not justify the intervention, as there is no proof of any market failure that needs to be fixed. Furthermore, the main provisions appear to be one-sided, implying that there is a need to redistribute value from SEP owners to implementers, and thus to address a hold-up problem.
- 4 Against this background, this paper investigates whether the Draft Regulation may devalue European SEPs, thus reducing the incentives for patent owners to invest in research and development (R&D). Notably, the paper suggests that, irrespective of the hold-out problems and the imposition of costs and restrictions on patent holders alone, the Commission's proposal departs from the well-established meaning of FRAND commitments and ultimately threatens the financial value of SEPs.
- 5 The paper is structured as follows. Section 2 frames the debate around SEPs licensing by reconstructing the long-standing dispute between hold-up and hold-out theories' supporters. Section 3 provides an overview of the main pillars of the Draft Regulation. Section 4 analyses the side effects of the provisions on essentiality checks, FRAND determination, and aggregate royalties, maintaining that the proposal entirely disregards the perspective of SEP owners in relation to hold-out risks. Section 5 investigates the relationship between patents and finance, illustrating the potential impact of the Draft Regulation on the financial value of SEPs as collateral and, in turn, its implications on innovation incentives. Section 6 concludes.

B. Hold-up or hold-out, that is the question

- 6 From a policy perspective, the entire history of SEPs licensing rules, including the goal of FRAND commitments and the role of competition law enforcement, can be analyzed through the lens of the dispute between hold-up and hold-out as the theory that should guide any initiative.⁵
- 7 At first, most of the scholars contended that the primary goal of Standard Developing Organisations (SDOs) licensing rules should be to alleviate the hold-up problem for implementers by prohibiting

5 See, e.g., Jorge L. Contreras, 'A Brief History of FRAND: Analyzing Current Debates in Standard Setting and Antitrust Through a Historical Lens', (2015) 80 Antitrust Law Journal 39.

SEP holders from imposing excessively high royalties once implementers are locked into a particular standard.⁶ According to this narrative, implementers dedicate a significant amount of resources to adhere to a standard and, once the latter is established, due to the substantial investment made and the impracticality of shifting to a different technology that does not conform to the standard, SEP holders may wield considerable influence and seek royalties that surpass the fair value of their contribution to the standard. In this context, FRAND policies play a crucial role, as negotiations between implementers and SEP holders typically commence only after implementers have already utilized and possibly infringed upon technologies covered by SEPs. Further, this strand of literature claims that such a risk of opportunistic behavior by SEP holders is so severe to require antitrust intervention as the hold-up problem cannot be resolved through private contracts.⁷ Thus, the governance of SDOs should be subject to antitrust scrutiny and compliance with FRAND commitments should be also ensured through antitrust enforcement.

- 8 While the concerns of courts, policymakers, and antitrust authorities have been concentrated on the hold-up issue, a different strand of literature argues that there is no evidence of systematic problems of hold-up in SEPs licensing and that instead the hold-out (or reverse hold-up) may arise as a different and equally worrisome problem.⁸

6 See, e.g., Carl Shapiro, 'Injunctions, Hold-Up, and Patent Royalties', (2010) 12 *American Law and Economics Review* 280; Joseph Farrell, John Hayes, Carl Shapiro, and Theresa Sullivan, 'Standard Setting, Patents, and Hold-Up', (2007) 74 *Antitrust Law Journal* 603; Mark A. Lemley and Carl Shapiro, 'Patent Holdup and Royalty Stacking', (2007) 85 *Texas Law Review* 1991. More recently, see Brian J. Love, Yassine Lefouili, and Christian Helmers, 'Do Standard-Essential Patent Owners Behave Opportunistically? Evidence From U.S. District Court Dockets', (forthcoming) *American Law and Economics Review*; Brian J. Love and Christian Helmers, 'Patent Hold-out and Licensing Frictions: Evidence from Litigation of Standard Essential Patents', (2023) 89 *International Journal of Industrial Organization* 102978; and Thomas F. Cotter, Erik Hovenkamp, and Norman Siebrasse, 'Demystifying Patent Holdup', (2019) 76 *Washington and Lee Law Review* 1501.

7 See, e.g., Carl Shapiro and Mark A. Lemley, 'The Role of Antitrust in Preventing Patent Holdup', (2020) 168 *University of Pennsylvania Law Review* 2019; A. Douglas Melamed and Carl Shapiro, 'How Antitrust Law Can Make FRAND Commitments More Effective', (2018) 127 *The Yale Law Journal* 2110; Stacey L. Dogan and Mark A. Lemley, 'Antitrust Law and Regulatory Gaming', (2009) 87 *Texas Law Review* 685.

8 See, e.g., Richard A. Epstein and Kayvan B. Noroozi, 'Why

- 9 The hold-out happens when potential licensees strategically leverage FRAND commitments to evade royalty payments or negotiate more favorable terms. This objective can be accomplished by intentionally prolonging license negotiations or by getting involved in protracted and expensive legal disputes with SEP holders. Indeed, due to the ambiguity surrounding the FRAND acronym, disagreements often arise between patent holders and licensees regarding what constitutes a FRAND licensing rate. In such cases, licensees may use FRAND commitments as leverage to insist on royalty rates that are below market standards, backed by the threat of litigation. As a consequence, hold-out proponents contend that SEPs licensing should be only addressed by contract law as hold-up risks are the effect of sunk investments already made by implementers on negotiation power, hence they reflect a problem of contract incompleteness at the time of standardization rather than an issue of the competitive process.⁹

- 10 Admittedly, hold-up and hold-out are two sides of the same coin as they both emerge in licensing relationships marked by information asymmetries, agency costs, and legal uncertainties linked to patent enforcement.¹⁰ While hold-up theory accuses patent holders of opportunistic rent-seeking, hold-out theory is primarily focused on the moral hazard of implementers excessively relying on FRAND commitments. Therefore, FRAND pledges build upon a twofold economic rationale as they are intended to

Incentives for "Patent Holdout" Threaten to Dismantle FRAND, and Why it Matters', (2017) 32 *Berkeley Technology Law Journal* 1381; Alexander Galetovic and Stephen Haber, 'The Fallacies of Patent-Holdup Theory', (2017) 13 *Journal of Competition Law & Economics* 1; J. Gregory Sidak, 'The Antitrust Division's Devaluation of Standard-Essential Patents', (2015) 104 *Georgetown Law Journal* 48; Gregor Langus, Vilen Lipatov and Damien Neven, 'Standard-Essential Patents: Who Is Really Holding Up (and When)?', (2013) 9 *Journal of Competition Law & Economics* 253. More recently, see Bowman Heiden and Justus Baron, 'The Economic Impact of Patent Holdout', (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4505268; Gerard Llobet and Jorge Padilla, 'A theory of socially inefficient patent holdout', (2023) 32 *Journal of Economics & Management Strategy* 424. Conversely, against the ongoing debate over the empirical evidence for systemic patent hold-up, considering it a fruitless academic exercise, see Jorge L. Contreras, 'Much Ado About Holdup', (2019) *University of Illinois Law Review* 875.

9 Maureen K. Ohlhausen, 'The Elusive Role of Competition in the Standard-Setting Antitrust Debate', (2017) 20 *Stanford Technology Law Review* 93.

10 Colleen V. Chien, 'Holding Up and Holding Out', (2014) 21 *Michigan Telecommunications & Technology Law Review* 1.

address both of these economic issues at the same time.

- 11 As we will illustrate in the following Sections, instead of striking a fair balance between the interests of both patent owners and implementers, the Commission's proposal merely embraces the hold-up theory and disregards the opposite risk of hold-out.¹¹

C. Brief overview of the Draft Regulation: Essentiality checks, FRAND determination, and reasonable aggregate royalties

- 12 By introducing provisions that, albeit not binding, would establish an essentiality check system, a FRAND determination procedure, and a mechanism for determining reasonable aggregate royalties for a standard, the Draft Regulation would overhaul the entire SEP licensing system, affecting the core of governance of SDOs, namely both disclosure and licensing rules usually adopted to ensure that the process functions efficiently and to reduce the risks of opportunistic behaviours by participants.
- 13 Indeed, by requiring firms taking part in a standardisation initiative to disclose the existence of any intellectual property right that might cover a technology considered to be implemented into the standard, SDOs aim to reduce the risk of any investment in the preparation, adoption, and application of standards being wasted as a result of the unavailability of a patent that is essential for a standard.¹² In this regard, disclosure rules may play

a significant role in alleviating risks of under- and over-declaration of patents that might be essential for practising an industry standard. The former may result in patent ambush, namely the non-disclosure of patents or patent applications that become essential to the adopted standard, perhaps enabling a patent holder to avoid a FRAND commitment and demand supra-FRAND royalties to license its patents. For these reasons, by failing to disclose SEPs, patent holders could be open to antitrust liability.¹³ However, over-disclosure may also originate from the possible benefit for patent holders in inflating the numbers of their patents disclosed as being potentially essential to a standard. In this regard, as some studies suggest that many patents disclosed as essential are not actually essential¹⁴, the request for a reform stems from the argument that SDOs are not under any obligation to perform any essentiality check.¹⁵

- 14 Furthermore, according to SDO licensing rules, SEP holders are required to license their patents implemented into the standard on FRAND terms. Notwithstanding the time spent by courts, policy makers, and academics, the economic and legal meanings of the FRAND commitment are still controversial. While it has been suggested that this commitment is mainly designed to avoid hold-up risks, courts have also (correctly) interpreted it as a tool for addressing hold-out problems. Indeed, in an attempt to tackle both hold-up and hold-out opportunistic behaviour and to strike a fair balance between the different interests involved, in the landmark ruling *Huawei v. ZTE* the European Court of Justice (CJEU) developed the so-called willing licensee test, stating that the exercise of

11 For a different point of view, see Jorge L. Contreras, 'Comments submitted to the European Commission', (2023) <https://ssrn.com/abstract=4534516>, which overall considers the Proposal "a logical and promising response" to increasing international jurisdictional conflict, private litigation and continuing uncertainty regarding the terms on which SEPs subject to FRAND commitments should be licensed. See also Josef Drexler, Dietmar Harhoff, Beatriz Conde Gallego, and Peter R. Slowinski, 'Position Statement of the Max Planck Institute for Innovation and Competition of 6 February 2024 on the Commission's Proposal for a Regulation on Standard Essential Patents', (2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4719023, which support the rationale of the Commission's initiative, complaining however that the proposal does not sufficiently consider how the specificities of the IoT influence the legal framing of SEP licensing, thus arguing that the Commission both overestimates the effect of the measures proposed and underestimates the difficulties involved in their practical implementation.

12 See, e.g., ETSI, 'Intellectual Property Rights Policy', (2022)

\$1.1, <https://www.etsi.org/images/files/ipr/etsi-guide-on-ipr.pdf>.

13 See, e.g., European Commission, 9 December 2009, Case COMP/38636, *Rambus*; U.S. Federal Trade Commission, *In the Matter of Rambus*, File no. 011-0017 (2002); U.S. Federal Trade Commission, *In the Matter of Dell Computer*, File No. 931-0097 (1996).

14 See, e.g., Rudi Bekkers, Christian Catalini, Arianna Martinelli, Cesare Righi, and Timothy Simcoe, 'Disclosure rules and declared essential patents', (2023) 52 *Research Policy* 104618; Robin Stitzing, Pekka Sääskilahti, Jimmy Royer, and Marc Van Audenrode, 'Over-Declaration of Standard Essential Patents and the Determinants of Essentiality', (2018) <https://ssrn.com/abstract=2951617>; IPlytics (n 1) Charles River Associates (n 1); Josh Lerner and Jean Tirole, 'Standard-Essential Patents', (2015) 123 *Journal of Political Economy* 547.

15 Mark A. Lemley and Timothy Simcoe, 'How Essential are Standard-Essential Patents?', (2019) 104 *Cornell Law Review* 607, 610.

remedies to protect intellectual property rights may be considered unlawful for the purposes of competition law only in exceptional circumstances, and subordinated any limitation of injunctions to the demonstration of the licensee's willingness to sign a FRAND deal.¹⁶

15 Admittedly, the need to enhance transparency, predictability, and efficiency of SEP licensing is not new to the EU policy agenda. In 2016, the Commission committed to working in collaboration with stakeholders on the identification of possible measures to increase the “transparency and quality of [SEPs] declarations” as well as to clarify core elements of an “equitable, effective and enforceable licensing methodology” around FRAND principles, and to facilitate the “efficient and balanced settlement” of disputes.¹⁷ One year later, the Commission called for a “clear, balanced and reasonable policy” for SEPs with the aim of contributing to the development of the IoT.¹⁸ In the 2020 IP Action Plan, the Commission reiterated its willingness to consider reforms to further clarify and improve the framework governing the declaration, licensing, and enforcement of SEPs.¹⁹ The Commission also appointed two expert groups aimed at investigating licensing and valuation practices of SEPs²⁰ as well as the technical and institutional feasibility of a system that ensures better essentiality scrutiny²¹, respectively.

16 The Impact Assessment accompanying the Draft Regulation confirmed that the overarching problems are represented by uncertainty and high transaction costs, which affect differently the behavior of SEP implementers and owners, in particular when these two groups are completely distinct, as it happens in the IoT.²² Notably, as result of the hold-up and hold-out risks, while implementers would be unable to both assess their SEP exposure and incorporate SEP

cost into product price, owners would be exposed to uncertain and delayed SEP revenue. The main drivers of such issues would be the insufficient transparency on SEP ownership and essentiality, the lack of information about FRAND royalties, and a dispute settlement system not adapted for FRAND determination.²³

17 Against this background, the Draft Regulation envisages an intrusive intervention, entrusting to a competence centre established under the purview of the European Union Intellectual Property Office (EUIPO) the main tasks regarding SEP licensing and litigation.²⁴

18 Firstly, in order to conduct essentiality checks, the competence centre would create and manage a register in which SEP owners seeking to license their SEPs in the EU must specify which patents they consider to be essential to a particular standard.²⁵ The registration is mandatory for enforcement purposes: if an SEP is not registered, the owner would not be able to assert it in court and would not be able to collect royalties or pre-existing damages for any use of the SEP prior to the registration date. Essentiality checks would be conducted randomly by independent evaluators on a sample from SEP portfolios, based on a methodology to be developed by the Commission so as to ensure that the sample is capable of producing statistically valid results.²⁶ Only one SEP from the same patent family would be checked. SEP owners may designate up to 100 registered SEPs for essentiality checks and may submit a claim chart for each SEP that is checked, including for the peer evaluation process. The results of the essentiality checks are not legally binding;

16 CJEU, 16 July 2015, Case C-170/13, *Huawei Technologies Co Ltd v. ZTE Corp*, ECLI:EU:C:2015:477.

17 European Commission, ‘ICT Standardisation Priorities for the Digital Single Market’ (n 1) 14.

18 European Commission, ‘Setting out the EU approach to Standard Essential Patents’ (n 1) 2.

19 European Commission, ‘Making the most of the EU’s innovative potential’ (n 1) 13.

20 Group of Experts on Licensing and Valuation of Standard Essential Patents (n 1).

21 Bekkers, Henkel, Tur, van der Vorst, Driesse, Kang, Martinelli, Maas, Nijhof, Raiteri, and Teubner (n 1).

22 Impact Assessment (n 4) 11.

23 Ibid. 17.

24 See, e.g., the concerns expressed by the President of the European Patent Office (EPO) in a letter sent to the European Parliament’s Committee on Legal Affairs: Antonio Campinos, ‘Re: Proposal for a Regulation of the European Parliament and of the Council on Standard Essential Patents’, (2023) <https://files.lbr.cloud/public/2023-10/EPO%20Letter%20IAM.pdf?VersionId=Xk2GKKPZ.qRisb5bU4BFaeiLe44oIuGB>.

25 Draft Regulation (n 2) Articles 19-25. The European Commission has been inspired by the Japanese *hantei* system, which represents the only attempt so far at introducing an essentiality review of SEPs by a patent office: see Japan Patent Office, ‘Manual of Hantei for Essentiality Check’ (2018) https://www.jpo.go.jp/e/system/trial_appeal/hantei_hyojun.html. However, because of stringent admission criteria and a narrowly defined test, this procedure has not yet been invoked by market parties. The *hantei* system has been recently revised to tackle some of these limits.

26 Draft Regulation (n 2) Articles 28-33.

therefore, any disputes in relation to essentiality would have to be decided by the courts.

- 19 Furthermore, in order to speed up negotiations concerning FRAND terms and to reduce costs, the Draft Regulation introduces a mandatory conciliation process, which is also a precondition for accessing the competent court of the Member States.²⁷ The obligation to initiate FRAND determination is without prejudice to the possibility for either party to ask the competent court of a Member State, pending the FRAND determination, to issue a provisional injunction of financial nature against the alleged infringer. However, the provisional injunction would exclude the seizure of the property of the alleged infringer and the seizure or delivery up of the products suspected of infringing an SEP.
- 20 Although it would be mandatory to start the conciliation before bringing a court action, the parties would be free to decide on their own level of engagement and would not be prevented from leaving the process at any time. The FRAND determination could even take place with the participation of just one party. The process would be completed within nine months and, upon its conclusion, the conciliator would make a proposal recommending a FRAND rate.²⁸ If the parties do not settle and/or do not accept that proposal, the conciliator would draft a report of the FRAND determination, including a confidential and a non-confidential version. The latter would contain the proposal for FRAND terms and conditions and the methodology used and would be provided to the competence centre for publication in order to inform any subsequent FRAND determination between the parties and other stakeholders involved in similar negotiations.
- 21 Moreover, to facilitate SEP licensing further and to reduce its cost, the Draft Regulation includes the determination of aggregate royalties for SEPs covering a standard, enabling holders of FRAND-encumbered SEPs to agree jointly upon it and notify the competence centre.²⁹ If there is no agreement between the SEP holders, those representing at least 20% of all SEPs of a standard may ask the competence centre to appoint a conciliator to

mediate discussions for the joint submission of an aggregate royalty. In this case, the conciliator's role would be to facilitate the decision-making by the participating SEP holders without making any recommendation of an aggregate royalty. However, SEP holders and/or implementers would also be able to ask the competence centre for a non-binding expert opinion on a global aggregate royalty. The opinion would contain a non-confidential analysis of the expected impact of the aggregate royalty on SEP holders and stakeholders in the value chain.

- 22 The provisions concerning the aggregate royalty aim to address the risk of royalty stacking, which is a phenomenon related to hold-up. Essentially, it means that even if the royalty rates, taken separately, are fair and reasonable, when large numbers of patents are involved, this may result in supra-competitive total rates due to double marginalisation.³⁰ Notably, the total royalty burden on a standardised product can become so high that the overall price paid exceeds the value of the corresponding contributions, with the aggregate royalties obtained for the various features of a product outweighing the value of the product itself.³¹
- 23 Both the aggregate royalty determination and the compulsory FRAND determination prior to litigation would be not required for SEPs covering those cases of the use of standards for which the Commission establishes, by means of a delegated act, that there is sufficient evidence that SEP licensing negotiations on FRAND terms do not give rise to significant difficulties or inefficiencies.³²

D. Biases versus empirical evidence: the (absent) economic justification of the Draft Regulation

- 24 Each of the illustrated regulatory proposals has

30 Lemley and Shapiro (n 6). See also *Ericsson, Inc. v. D-Link Systems, Inc.*, 773 F.3d 1201, 1209 (Fed. Cir. 2014), arguing that, when a standard implicates numerous patents, “[i]f companies are forced to pay royalties to all SEP holders, the royalties will ‘stack’ on top of each other and may become excessive in the aggregate.”

31 Draft Regulation (n 2) Recital 15, contending that knowledge of the potential total royalty for all SEPs covering a standard applicable to the implementations of that standard is important for the assessment of the royalty amount for a product, which plays a significant role for the manufacturer's cost determinations, and it also helps SEP holder to plan expected return on investment.

32 Ibid., Article 1(3-4).

27 Ibid., Article 34.

28 Ibid., Articles 37 and 50-58.

29 Ibid., Articles 15-18. This solution seems supported by the analysis commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs in 2019: see Luke McDonagh and Enrico Bonadio, 'Standard Essential Patents and the Internet of Things', (2019) <https://www.europarl.europa.eu/committees/en/supporting-analyses/sa-highlights>.

been harshly criticised for being detached from reality and unsupported by empirical evidence and economic justification.

- 25 With regard to essentiality checks, some scholars have questioned the results of essential patent landscaping studies, raising doubts about their accuracy and reliability, such as with regard to the actual number of non-essential patents disclosed.³³ Furthermore, some over-declaration is - to a certain extent - inevitable as it reflects the natural process of standard development.³⁴ Moreover, it has been argued that the challenge for policy makers is to select an efficient and effective essentiality test mechanism as, due to the number of technical specifications and patents involved, essentiality checks are a costly and time-consuming activity; the accuracy of the different potential methods is also strongly debated.³⁵ As a result, while it is uncertain

whether the EU solution could enhance the *status quo*, essentiality checks may provide implementers with a strategic opportunity for hold-out by delaying or even avoiding royalty payments.³⁶ Concerns that some implementers may misuse such a process in an attempt to delay negotiations or to avoid paying royalties are further exacerbated by the fact that, under the Draft Regulation, the results of the essentiality checks would be not legally binding and any disputes in relation to them would need to be decided by the courts.³⁷

- 26 Similar concerns have been raised about the pre-trial mandatory FRAND determination. Indeed, by endorsing an anti-injunction approach, the Draft Regulation marks a significant departure from the bargaining framework developed by the CJEU in *Huawei*.³⁸ While the CJEU's willing licensee test aims to strike a fair balance between the different interests involved, compulsory conciliation would determine an uneven bargaining position between licensors and licence seekers by reducing the scope of injunctions beyond *Huawei*. Implementers would be free to challenge SEPs requesting determinations of invalidity, and declarations of non-infringement and non-essentiality, but patent owners would be restricted from bringing an infringement suit prior to initiating a FRAND determination, regardless of the implementers' willingness.³⁹ Therefore, rather than being focused on tackling both hold-up and

33 See Keith Mallinson, 'Essentiality checks might foster SEP licensing, but they won't stop over-declarations from inflating patent counts and making them unreliable measures', (2022) <https://ssrn.com/abstract=4278639>; Igor Nikolic, 'Estimating 5G Patent Leadership: The Importance of Credible Reports', (2022) <https://ssrn.com/abstract=4109222>; Haris Tsilikas, 'Patent Landscaping Studies and Essentiality Checks: Rigorous (and Less Rigorous) Approaches', (2022) 53 *les Nouvelles*.

34 See *Unwired Planet v. Huawei Technologies*, [2020] UKSC 37, para. 44, arguing that "problem of over-declaration is in part the result of the IPR Policy process which requires patent owners to declare SEPs in a timely manner when a standard is being prepared, as it encourages patent owners to err on the safe side by making a declaration. In part, there are difficulties in interpreting both the patents and the standards. In part also, patent claims are amended over time; different national patents within a patent family will vary in scope around the world; and standards themselves will vary over time." See also Bekkers, Henkel, Tur, van der Vorst, Driesse, Kang, Martinelli, Maas, Nijhof, Raiteri, and Teubner (n 1) 112, noting that actual essentiality can only be determined once the standard's document in question is final and once the patent in question is granted. Therefore, because disclosures are typically made before these processes are concluded, some inaccuracies in the disclosure process are inevitable even if companies act in good faith.

35 See Giuseppe Colangelo, 'Finding an efficiency-oriented approach to scrutinize the essentiality of SEPs: a survey', (2023) 18 *Journal of Intellectual Property Law and Practice* 502, providing a review of the literature on different mechanisms that have been proposed to determine the essentiality of a patent. For an estimation of the cost of essentiality checks, see Bekkers, Henkel, Tur, van der Vorst, Driesse, Kang, Martinelli, Maas, Nijhof, Raiteri, and Teubner (n 1); IPlytics (n 1) 51-52; Charles River Associates (n 1) 58-59.

36 Charles River Associates (n 1) 32. For a different view, see Drexler, Harhoff, Conde Gallego, and Slowinski (n 11).

37 See Cody M. Akins, 'Overdeclaration of Standard-Essential Patents', (2020) 98 *Texas Law Review* 579, suggesting introducing a presumption of infringement by standard-compliant products once patents are deemed essential by the patent office in order to make these procedures more effective. See also Group of Experts on Licensing and Valuation of Standard Essential Patents (n 1) 68, advocating the adoption of measures to prevent the challenging of independent essentiality confirmations for all or a substantial number of SEPs of one SEP holder as part of licensing negotiations and delay tactics.

38 Giuseppe Colangelo, 'FRAND determination under the European SEP Regulation Proposal: discarding the *Huawei* framework?', (forthcoming) *European Competition Journal*. A different view is provided by Drexler, Harhoff, Conde Gallego, and Slowinski (n 11) 10, which argue that structured negotiations and court proceedings alone do not suffice to eliminate the systemic lack of transparency affecting SEP licensing negotiations.

39 Draft Regulation (n 2) Article 56(4), stating that the enforcement before a national court is also precluded when the determination of FRAND terms and conditions is raised in abuse of dominance cases, namely in the national application of the *Huawei* framework.

hold-out opportunistic behaviour, the Commission appears to be concerned solely with the former. Furthermore, as the FRAND determination under the Draft Regulation and the *Huawei* bargaining framework are intended to coexist⁴⁰, the European proposal is likely to cause confusion, thus leading to licensing disputes, rather than supporting balanced and successful SEP licensing negotiations.⁴¹

- 27 Finally, the proposed mechanism for determining reasonable aggregate royalties has been questioned due to the lack of empirical evidence to support the royalty stacking theory.⁴² Furthermore, it has been highlighted that antitrust risks may arise from the participation of implementers in the process of providing an expert opinion on global aggregate rates, as they may exploit such an opportunity to coordinate their submissions with the aim of devaluing FRAND royalty rates.⁴³
- 28 By and large, the main criticism made against the Draft Regulation concerns its economic justification, notably the fact that there is no discernible evidence of a market failure that needs to be addressed.⁴⁴

40 See Impact Assessment (n 4) 43 and 58, arguing that the mandatory conciliation will complement the *Huawei* process.

41 Colangelo (n 38).

42 For a summary of the empirical evidence on royalty stacking, see Justus A. Baron, 'The Commission's Draft SEP Regulation – Focus on Proposed Mechanisms for the Determination of "Reasonable Aggregate Royalties"', (2023) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4537591, arguing that aggregate royalty burdens on implementers are well below the levels predicted by such a theory, thus encouraging EU institutions to delete Articles 15-18 of the Draft Regulation.

43 Igor Nikolic, 'Some practical and competition concerns with the proposed Regulation on Standard Essential Patents', (2023) <https://www.4ipcouncil.com/research/some-practical-and-competition-concerns-proposed-regulation-standard-essential-patents>. In a similar way, Drexler, Harhoff, Conde Gallego, and Slowinski (n 11).

44 See, e.g., Centre for a Digital Society of the European University Institute, 'Feedback to EU Commission's public consultation', (2023) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13109-Intellectual-property-new-framework-for-standard-essential-patents/F3432699_en; Christine A. Varney, Makan Delrahim, David J. Kappos, Andrei Iancu, Walter G. Copan, and Noah Joshua Phillips, 'Comments on European Commission's Draft "Proposal for Regulation of the European Parliament and of the Council Establishing a Framework for Transparent Licensing of Standard Essential Patents"', (2023) <https://ipwatchdog.com/wp-content/uploads/2023/04/Comments-on-European-Commission->

Indeed, the empirical evidence informing the Commission's initiative reveals that there is no SEP litigation failure in Europe.⁴⁵ According to the study used as the main input for the Commission's Impact Assessment, existing empirical evidence on the causal effects of current SEP licensing conditions is "largely inconclusive".⁴⁶ In particular, there is no evidence that FRAND licensing frictions are causing SEP owners to contribute less to standard development or are inducing implementers to opt for alternative standards (i.e. without FRAND licensing); there is also no indication that current SEP licensing conditions systematically suppress or delay standard implementation.⁴⁷ For these reasons, the European regulatory intervention appears unnecessary.

- 29 In addition, the Draft Regulation seems to be imbalanced and one-sided, essentially being driven by a hold-up bias. Although it is a well-established principle, acknowledged by the courts⁴⁸ and the European Commission⁴⁹, that hold-up and hold-out are two sides of the same coin - and thus that FRAND pledges are intended to address both of these opportunistic behaviours at the same time - the hold-out problem is completely disregarded by the Draft Regulation.

- 30 Indeed, the EU proposal completely ignores the perspective of SEP owners. As reported by the Impact Assessment, in order to participate in standard creation, prospective SEP holders have to invest considerable time and resources in R&D activities firstly to develop new technology and then to patent it worldwide⁵⁰: "All that is done without guarantee

Draft-SEP-Regulation-by-Former-US-Officials-1.pdf; Robin Jacob and Igor Nikolic, 'ICLÉ Feedback to EU Commission's public consultation', (2023) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13109-Intellectual-property-new-framework-for-standard-essential-patents/F3433917_en.

45 Baron, Arque-Castells, Leonard, Pohlmann, and Sergheraert (n 1).

46 Ibid., 185.

47 Ibid., 164.

48 See, e.g., *Huawei* (n 16) paras. 65-67; *Unwired Planet* (n 34) paras. 10, 61 and 167.

49 See European Commission (n 4) 2, stating that the inefficient SEP licensing that the Draft Regulation aims at addressing includes hold-up and hold-out; European Commission, 'Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements', (2023) OJ C 259/1, para. 444.

50 Impact Assessment (n 4) 11-15, mentioning Raphaël De

that first, the inventor's patents will be used by the standard, and second, that the standard will be accepted by the market."⁵¹ Given that, even if a standard is accepted, it takes time before it is widely used, while an invention is protected for a limited amount of years, SEP holders have limited time to generate a return for their R&D investments through royalties for the use of their patents.⁵² Furthermore, in contrast to other patents, SEP holders are bound by the FRAND commitment. Therefore, in the public consultation, SEP owners stated that their main challenges included facing lengthy negotiations and the high cost of licensing due to the various means used by implementers to delay the obtaining of a licence.⁵³

- 31 Against this backdrop, the Draft Regulation disregards the problems raised by SEP owners in the public consultation and highlighted by the Impact Assessment. Furthermore, the costs of such a regulation would be borne by the SEP holders alone, whereas the implementers would reap all the benefits. This emerges clearly from the comparison between the expected costs and benefits envisaged by the Impact Assessment.⁵⁴ While it imposes costs and restrictions on patent holders, the Draft Regulation gives implementers a free-ride, allowing them to undertake delaying tactics and to pursue efficient infringements. As a result, the Draft Regulation is apparently motivated by the aim of redistributing value from SEP owners to implementers.⁵⁵ Moreover, given that, according to the findings of the Impact Assessment, less than 10% of implementers are based in Europe, the Draft Regulation would have the effect

of subsidising non-EU implementers.⁵⁶

- 32 The immediate effect of such an approach would be to devalue European SEPs, endangering future investments in innovation. The consequences of a potential devaluation of SEPs should be particularly worrisome for EU policy makers as the landscape illustrated in the Impact Assessment reveals that, while one-third of all SEPs are owned by Chinese companies, which have doubled their share in seven years, EU shares in SEPs have decreased from 22% to 15% in the same period.⁵⁷
- 33 In brief, the Draft Regulation is not only providing solutions for a problem that does not exist, as there is no evidence of market failure, but it is also pursuing an unjustified goal of value redistribution by embracing a hold-up bias that is at odds with the rationale of FRAND commitments and threatens the financial value of SEPs.

E. Patents and finance

- 34 As patents are central to corporate financing and innovation, it is crucial to assess the potential impact of the Draft Regulation on a significant aspect of SEPs, namely their role as financial collateral, which is both promising and sensitive from a regulatory perspective. Before moving into the details of the issue, it is worth making a note of caution as to the perimeter of the discussion.
- 35 While a rich debate has emerged in the literature regarding the potential unconstitutional character of legislative redesigning specific IP frameworks, we do not engage with this issue.⁵⁸ The purpose of our analysis is to highlight the potential of SEPs to serve as financial collateral and the associated risk of undermining this economic feature by diluting SEP-related rights. We do not aim at discussing whether the conditional unavailability of a remedy violates the essence of rights or excessively limits the right

Coninck, Christoph von Muellern, Samuel Zimmermann, and Kilian Mueller, 'SEP Royalties, Investment Incentives and Total Welfare', (2022) <https://fair-standards.org/wp-content/uploads/2023/04/SEP-Royalties-Investment-Incentives-and-Total-Welfare.pdf>, which estimate R&D amounts of between USD 2 and 9 billion annually for standards used in a smartphone.

51 Impact Assessment (n 4) 12.

52 Ibid., reporting that, in order to be able to better assess the value that their technology brings to the standard implementations, a SEP holder would wait around 2 to 4 years until the standard is implemented in the market and then approach companies in specific markets to offer them licences. This is followed by negotiations, which take on average 3 years and potentially litigation in case parties cannot reach an agreement (adding another 1 to 2.5 years).

53 Ibid., 13-14.

54 Ibid., 58.

55 Jacob and Nikolic (n 44).

56 Ibid.

57 Impact Assessment (n 4) 8.

58 See, e.g., the different views expressed by Martin Husovec, 'The Fundamental Right to Property and the Protection of Investment: How Difficult Is It to Repeal New Intellectual Property Rights', in *Research Handbook on Intellectual Property and Investment Law* (ed. C. Geiger), Edward Elgar, 2020, 385; and Mohammad Ataul Karim, 'The Proposed EU SEP Regulation: Checking Balancing Incentives, and compatibility with EU Fundamental Rights, and the TRIPS Regime', (2023). https://www.4ipcouncil.com/application/files/9816/8847/8735/2023.07.04_final_Draft_SEP_Regulation_paper_.pdf.

to property.

36 Financial intermediaries typically require collateral to mitigate information imbalances and moral hazard risks, since borrowers with lower credit ratings may be less inclined to pledge assets as a means of demonstrating their creditworthiness.⁵⁹ Admittedly, intangible assets pose unique challenges when seeking external financing. Indeed, the valuation of intangibles is more volatile than that of tangible assets, and asset transferability might not be optimal due to several sector-specific areas of friction.⁶⁰ Consequently, intangible assets are more challenging to redeploy and hold a lower liquidation value, limiting any recovery for creditors in the event of default.

37 When focusing on the case of patents, it is imperative to gain some insight into access by companies to bank debt financing and the degree to which regulatory obstacles can hinder their ability to pledge patents as collateral. Banks have been playing a significant role in funding innovative ventures, ultimately shaping corporate innovation policies.⁶¹ Therefore, the use of patent portfolios as collateral within financing strategies is progressively gaining prominence for both market participants and policymakers.⁶²

59 Hans Degryse, Artashes Karapetyan, and Sudipto Karmakar, 'To ask or not to ask? Bank capital requirements and loan collateralization', (2021) 142 *Journal of Financial Economics* 239-260.

60 Guido Franco and Lilas Demmou, 'Mind the Financing Gap: Enhancing the Contribution of Intangible Assets to Productivity', (2021) OECD Economics Department Working Papers No. 1681, https://www.oecd-ilibrary.org/economics/mind-the-financing-gap-enhancing-the-contribution-of-intangible-assets-to-productivity_7aefd0d9-en.

61 See, e.g., Anna Geddes and Tobias S. Schmidt, 'Integrating finance into the multi-level perspective: Technology niche finance regime interactions and financial policy interventions', (2020) 49 *Research Policy* 103985; Ramana Nanda and William Kerr, 'Financing innovation', (2015) 7 *Annual Review of Financial Economics* 445; Shane A. Johnson, 'An empirical analysis of the determinants of corporate debt ownership structure', (1997) 32 *Journal of Financial and Quantitative Analysis* 47; Joel Houston and Christopher James, 'Bank information monopolies and the mix of private and public debt claims', (1996) 51 *Journal of Finance* 1863.

62 See, e.g., the World Intellectual Property Organization (WIPO) launching in 2022 a High-level Conversation on Unlocking Intangible Asset Finance, https://www.wipo.int/sme/en/news/2022/news_0018.html; and OECD, 'Bridging the gap in the financing of intangibles to support productivity: Background paper', (2021) <https://www.oecd.org/global-forum-productivity/events/Bridging-the-gap->

38 For instance, numerous countries have initiated policies to facilitate patent-backed loans for innovative firms. In the US, private investment banks, unbridled by the strict prudential regulations to which commercial banks must adhere, have driven the growth of IP-backed financing. These loans secured by intangible assets rose from 11% to 24% between 1997 and 2005.⁶³ France has implemented a legal framework that offers lenders a high level of legal certainty; this framework grants lenders the right to acquire non-possessory interests in the intellectual property assets of debtors and hinges on a centralised registry for various IP assets.⁶⁴ In addition, Bpifrance, a French public sector investment bank, offers uncollateralised loans to SMEs for digitalisation, while Germany's Bavaria Digital initiative provides favourable loans to digital SMEs with streamlined applications.⁶⁵ In China, the active market for IP-backed financing relies on massive government support, involving, in particular, the State Intellectual Property Office (SIPO) and the Ministry of Finance.⁶⁶ South Korea's Development Bank plays a key role through its Techno Banking initiative, including IP purchase loans and support for distressed IPs.⁶⁷ Singapore's IP Financing Scheme, established in 2014, certifies

in-the-financing-of-intangibles-to-support-productivity-background-paper.pdf.

63 Maria Loumrioti, 'The Use of Intangible Assets as Loan Collateral', (2012) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1748675.

64 Laurie Ciaramella, David Heller, and Leo Leitzinger, 'Intellectual Property as Loan Collateral' (2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4260877; Michel Sejean and Nicolas Binctin, 'Security rights in intellectual property in France', in *Security Rights in Intellectual Property* (ed. E.-M. Kieninger), Springer, 2020, 373.

65 Bpifrance, 'The Digital Transformation Of French Companies With The France Num Guarantee', (2022) Press Release, <https://www.bpifrance.com/2022/04/20/bpifrance-supports-the-digital-transformation-of-french-companies-with-the-france-num-guarantee/>. See also Bavarian Ministry of Economic Affairs, 'Funding and financing options for investors', (2023) https://cms.invest-in-bavaria.com/fileadmin/media/documents/Flyer_broschures/210527_RZ_IIB_Foerdermittelbroschuere_ENG_2021_Web-PDF_1_.pdf.

66 Martin Brassell and Kris Boschmans, 'Fostering the Use of Intangibles to Strengthen SME Access to Finance', (2019) OECD SME and Entrepreneurship Papers No. 12, <https://www.oecd-ilibrary.org/deliver/729bf864-en.pdf?itemId=%2Fcontent%2Fpaper%2F729bf864-en&mimeType=pdf>.

67 Franco and Demmou (n 59), 35.

patent values and shares risk with lender banks, partially underwritten by the Government.⁶⁸

- 39 Given such an increasing policy interest in IP finance, the issue of patent pledgeability must be carefully considered when developing adjacent regulation constraining SEP holders. After reviewing the literature on patents as financial collateral, this section highlights the distinctive characteristics that make SEPs particularly appealing from a financial perspective and also as tools to incentivise innovation.

I. Literature review

- 40 The practice of using patents as financial collateral has evolved over time, driven by the need for capital access and risk mitigation. A substantial body of economic literature addressing this issue has been developed over the last decade.
- 41 Amable et al., as well as Grilli et al., theorised the suitability of patents as collateral by contemplating the potential implications of a widespread increase in patent use and the leverage effect that this collateral could have on innovation-driven growth.⁶⁹ Loumioti found evidence that loans secured by intangibles perform no worse than other secured loans.⁷⁰ Mann and Hochberg et al. reported that patents are often used as collateral and that innovative firms obtain loans more frequently.⁷¹ On a similar note, Brassell and King provided evidence that innovative firms use cash flow streams deriving from licensing

or royalties to secure loans.⁷² Furthermore, as demonstrated by Francis et al., patents function as a signalling mechanism for small and nascent enterprises, showcasing the calibre of the firm's management and its technological acumen, thereby enjoying fewer collateral requirements and lower bank loan spreads.⁷³ On a related note, Robb and Robinson provided causal evidence to suggest that a substantial source for start-up capital stems from bank financing.⁷⁴

- 42 Farre-Mensa et al. consolidated the argument by documenting that, due to randomly assigned lenient patent examiners, small firms which obtain patent protection are set to benefit beyond the value of the technical solution itself in terms of increased post-patent funding.⁷⁵ Similarly, Chava et al. demonstrated that cheaper loans result from an exogenous enhancement in the value of borrowers' patents, either through creditor rights over collateral or greater patent protection.⁷⁶ Plumlee et al. found that borrowers with forthcoming patents are charged a lower spread by banks.⁷⁷ Dai et al. found that increased patent pledgeability encourages corporations to shift from secrecy-based innovation to patent-based innovation, rather than solely alleviating financial constraints.⁷⁸ This

68 Asia-Pacific Economic Cooperation, 'Best Practices on Intellectual Property (IP) Valuation and Financing in APEC', (2018) Report by the Committee on Trade and Investment (CTI), Intellectual Property Rights Experts Group, <https://www.apec.org/publications/2018/04/best-practices-on-ip-valuation-and-financing-in-apec>.

69 Bruno Amable, Jean-Bernard Chatelain, and Kirsten Ralf, 'Patents as collateral', (2010) 34 *Journal of Economic Dynamics & Control* 1092; Luca Grilli, Marianna Mazzucato, Michele Meoli, and Giuseppe Scellato, 'Sowing the seeds of the future: Policies for financing tomorrow's innovations', (2018) 127 *Technological Forecasting and Social Change* 1.

70 Loumioti (n 63).

71 William Mann, 'Creditor rights and innovation: Evidence from patent collateral', (2018) 130 *Journal of Financial Economics* 25; Yael V. Hochberg, Carlos J. Serrano, and Rosemarie H. Ziedonis, 'Patent collateral, investor commitment, and the market for venture lending', (2018) 130 *Journal of Financial Economics* 74.

72 Martin Brassell and Kelvin King, 'Banking on IP?: The Role of Intellectual Property and Intangible Assets in Facilitating Business Finance' (2013) The Intellectual Property Office of the United Kingdom, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/312008/ipresearch-bankingip.pdf.

73 Bill Francis, Iftexhar Hasan, Ying Huang, and Zenu Sharma, 'Do Banks Value Innovation? Evidence from US Firms', (2021) 41 *Financial Management* 159.

74 Alicia M. Robb and David Robinson, 'The capital structure decisions of new firms', (2014) 27 *Review of Financial Studies* 153.

75 Joan Farre-Mensa, Deepak Hegde, and Alexander Ljungqvist, 'What is a patent worth? Evidence from the US patent "lottery"', (2020) 75 *The Journal of Finance* 639.

76 Sudheer Chava, Vikram Nanda, and Steven Chong Xiao, 'Lending to innovative firms', (2017) 6 *The Review of Corporate Finance Studies* 234.

77 Marlene A. Plumlee, Yuan Xie, Meng Yan, and Jeff Jiwei Yu, 'Bank loan spread and private information: Pending approval patents' (2015) *Review of Accounting Studies* 20(2): 593–638.

78 Yanke Dai, Ting Du, Huasheng Gao, and Yan Gu, 'Patent Pledgeability, Trade Secrecy, and Corporate Patenting', (2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4132148.

evidence aligns with the perception of patents as viable collateral and indicators of technological achievement, thereby enhancing future profitability prospects.

- 43 Additionally, Hsu et al. showed that bond premiums are negatively correlated with the impact, originality, generality, and quantity of a company's patent portfolio.⁷⁹ Concerningly, Ayerbe et al. brought to light the potential adverse consequence of patents used as collateral for loans, whereby technology companies may be tempted to veer away from pursuing long-term innovation in favour of short-term strategies centred around patent monetisation and litigation.⁸⁰
- 44 Another strand of literature emphasises the economic challenges associated with financing innovative activities in a perfectly competitive market due to the idiosyncratic nature of innovation, which gives rise to significant information gaps between those with insider knowledge and the capital markets.⁸¹ Given this background, critics of debt financing argue that equity is a better tool for addressing the substantial uncertainty inherent in genuine innovation and the challenges associated with patent rights.⁸² Conversely, debt financing advocates argue that financial institutions can better regulate firms through contract design.⁸³ In particular, Ma et al. emphasised that banks should design debt contracts that facilitate idea generation yet provide stronger incentives to implement patented solutions in an

effective and efficient way.⁸⁴

II. SEPs as financial collateral

- 45 Within the realm of patents, SEPs stand out as a specific class of IP assets with exceptional attributes, making them a tremendous candidate to serve as valuable financial collateral and to sustain R&D investments. In essence, while traditional patents are suitable to guarantee loan schemes, SEPs are better placed to safeguard lenders' interests as they generate less economic friction to debt financing. Due to their essential role in implementing standards across various industry sectors, SEPs possess distinctive attributes which render them highly appealing as financial collateral for several compelling reasons.
- 46 Firstly, SEPs have a relatively high nominal worth, which eliminates the need for banks to engage in overly complex examinations to assess the significance of the assets involved as collateral. In essence, lenders can rely on SEPs, treating them like any other asset with a solid return on investment and less volatile valuation, thereby minimising any information asymmetry and the risks associated with innovative projects.⁸⁵ As demonstrated by Lerner, Tirole, and Stojwas, higher quality patents are more likely to be included in a patent pool functional to cooperative standards.⁸⁶ At the same time, Rysman and Simcoe found that patents disclosed in the standard-setting process receive roughly twice as many citations as a set of controls from the same technology class and application year.⁸⁷ While it is widely acknowledged that SEPs are likely to cover the most influential technologies⁸⁸, Layne-Farrar and

79 Po-Hsuan Hsu, Hsiao-Hui Lee, Alfred Zhu Liu, and Zhipeng Zhang, 'Corporate innovation, default risk, and bond pricing', (2015) 35 *Journal of Corporate Finance* 329.

80 Cécile Ayerbe, Jamal Azzam, Selma Boussetta, and Julien Pénin, 'Revisiting the consequences of loans secured by patents on technological firms' intellectual property and innovation strategies', (2023) 52 *Research Policy* 104824.

81 For a thorough review of the issue, see Jonathan Haskel and Stian Westlake, *Capitalism without Capital: The Rise of the Intangible Economy*, (2018) Princeton University Press; Bronwyn Hall and Josh Lerner, 'The Financing of R&D and Innovation', (2010) 1 *Handbook of the Economics of Innovation* 609; Robert E. Carpenter and Bruce C. Petersen, 'Capital market imperfections, high-tech investment, and new equity financing', (2002) 112 *Economic Journal* 54.

82 James R. Brown, Steven M. Fazzari, and Bruce C. Petersen, 'Financing innovation and growth: Cash flow, external equity, and the 1990s R&D boom', (2019) 64 *Journal of Finance* 151.

83 Yuqi Gu, Connie X. Mao, and Xuan Tian, 'Banks' interventions and firms' innovation: Evidence from debt covenant violations', (2017) 60 *Journal of Law and Economics* 637.

84 Zhiming Ma, Kirill E. Novoselov, Derrald Stice, and Yue Zhang, 'Firm innovation and covenant tightness', (2022) *Review of Accounting Studies*.

85 Mary E. Barth, Ron Kasznik, and Maureen F. McNichols, 'Analyst Coverage and Intangible Assets', (2001) 39 *Journal of Accounting Research* 1.

86 Josh Lerner, Jean Tirole and Marcin Stojwas, 'Cooperative Marketing Agreements Between Competitors: Evidence from Patent Pools', (2003) NBER Working Paper No. 9680, <https://www.nber.org/papers/w9680>.

87 Marc Rysman and Timothy Simcoe, 'Patents and the Performance of Voluntary Standard-Setting Organizations', (2008) 54 *Management Science* 1920.

88 Rudi Bekkers, Geert Duysters, and Bart Verspagen, 'Intellectual property rights, strategic technology agreements and market structure: The case of GSM', (2002) 31 *Research Policy* 141.

Padilla clarified that the inherent positive effects on patent value from being included in a standard depend on a wide range of idiosyncrasies across industries, technologies, standards, patent offices, and SDOs.⁸⁹

- 47 Secondly, licensing an SEP does not involve any further transfer of the related know-how and technical information to enable the licensee to use the technology. As argued by Bourreau et al., it simply requires manufacturers to pay for implementing the standard.⁹⁰ Indeed, the essential technology is needed to implement a specific standard across the industry regardless of the patent owner. As they benefit from high transferability, SEPs are easy to redeploy and retain a significantly higher liquidation value, increasing the share creditors can recoup in the case of default as opposed to other types of intangible assets.⁹¹
- 48 Thirdly, by definition, SEPs generate a consistent cash flow due to the continuous need by industry to implement a standard. As argued by Brassell and King, such a steady financial stream deriving from licensing is well-suited to securing loans.⁹² Once a standard gains broad market recognition, the earning generated by the underpinning SEPs is likely to retain a solid market value. Furthermore, as SEPs are subject to FRAND commitments, lenders have room to assess in advance the amount of the cash flow by relying on the pricing mechanisms used in the industry to determine the FRAND licences. This element increases the financial predictability of the intrinsic value of SEPs.
- 49 Fourthly, SEPs function as a positive market signal for lenders, as the financial performance of companies active in technology-related markets is not only connected to their innovative capabilities and resources, but also depends on the strategic positioning of their patent portfolio. Notably, the results obtained by Pohlmann et al. showed a curvilinear (inverse U-shaped) relationship of owning SEPs and financial performance and

particularly the return on assets.⁹³

- 50 Therefore, SEPs not only qualify as the most suitable IP asset class to serve as financial collateral, but they also make a strong case in favour of privileged prudential treatment. So far, prudential regulation has obstructed the development of loans secured against intangibles. As loans backed by intangibles are considered riskier than physical assets (e.g. real estate), they are not included in the calculation of banks' regulatory capital. As documented by Dell'Araccia et al., over the last decade, banks have had lower incentives to engage in IP financing and the cost of capital for intangible-intensive firms has increased, leading to a reallocation of banks' portfolios from commercial loans to real estate lending.⁹⁴ Crouzet and Eberly have provided evidence that the simultaneous rise in investment allocated to intangible assets and the relatively limited portion of it funded through bank loans is likely to undermine the effectiveness of monetary policy transmission channels.⁹⁵ This is because investments tend to be less sensitive to shifts in interest rates under these circumstances.
- 51 Against this backdrop, the potential of SEPs to guarantee higher and more consistent cash flows, as well as their strong transferability, allow individual institutions to demonstrate the performance and the rates of recovery of SEP asset classes in downside scenarios when assets need to be liquidated independently of the business. Moreover, the prospect, investigated by Brassell and King, of facilitating banks and insurance companies to sustain IP-backed loans is likely to benefit first and foremost SEPs which present a more manageable risk profile than other IP asset classes.⁹⁶
- 52 In essence, SEPs can be regarded as crucial financial assets, providing vital funding for innovation in technology-centric sectors, benefiting both established firms and emerging players. Thus, it is important to alert policymakers about the potential

89 Anne Layne-Farrar and Jorge Padilla, 'Assessing the Link Between Standards and Patents', (2011) 9 *International Journal of IT Standards and Standardization Research* 19.

90 Marc Bourreau, Yann Ménière, and Tim Pohlmann, 'The Market for Standard Essential Patents', (2015) Working Papers HAL-01261024, <https://www.parisschoolofeconomics.eu/IMG/pdf/market-for-standard-essential-patents-menieres-workshop-pse-june2015.pdf>.

91 Hall and Lerner (n 81).

92 Brassell and King (n 72).

93 Tim Pohlmann, Peter Neuhäusler, and Knut Blind, 'Standard essential patents to boost financial returns', (2016) 46 *R&D Management* 612.

94 Giovanni Dell'Araccia, Dalida Kadyrzhanova, Camelia Minoiu, and Lev Ratnovski, 'Bank Lending in the Knowledge Economy', (2017) IMF Working Paper No. 2017/234, <https://www.imf.org/en/Publications/WP/Issues/2017/11/07/Bank-Lending-in-the-Knowledge-Economy-45343>.

95 Nicolas Crouzet and Janice C. Eberly, 'Understanding Weak Capital Investment: the Role of Market Concentration and Intangibles', (2019) NBER Working Paper No. 25869, <https://www.nber.org/papers/w25869>.

96 Brassell and King (n 72).

unintended consequences of regulatory proposals which could threaten the intricate economic framework supporting the financial ability of SEPs to serve as financial collaterals. To be clear, this is not to suggest that new provisions should refrain from influencing companies' strategies or expected profits,⁹⁷ but rather to emphasize their effects on how innovation could be financed in a specific context.

F. Concluding remarks

- 53 The comparison between the purported goals and envisaged solutions of the Draft Regulation provides a clear, yet surprising, picture of the EU SEP landscape. Spurred on by concerns over the emergence of the IoT across several industries, the European Commission has portrayed SEP holders as a hindrance to innovation and growth due to an apparently inefficient licensing ecosystem. The main remedies put forward in the Draft Regulation are to introduce significant costs and restrictions on SEP holders, ostensibly in pursuit of a value-redistribution agenda designed to favour implementers. The assumption underlying the proposal is that patent hold-up issues are the primary cause of inefficiencies in the European SEP market.
- 54 However, this worrisome narrative does not reflect reality. The very same study commissioned to support the regulatory intervention reveals no evidence of a SEP litigation failure in Europe, arguing that there is no indication that current SEP licensing conditions systematically suppress or delay standard implementation or that FRAND licensing friction is causing SEP owners to contribute less to standard development or is inducing implementers to opt for alternative standards.
- 55 While these findings call into question the justification of the overhaul proposed by the Commission in the first place, the potential side effects of the Draft Regulation are further amplified by the endorsed hold-up approach. Indeed, by suggesting solutions to a problem that apparently does not exist, the Commission is devaluing European SEPs and granting implementers leeway to engage in opportunistic behaviours and to reap all the benefits of the standardisation process.
- 56 This paper scrutinises the Commission's proposed remedies, maintaining that such a profound restructuring of SEP licensing dynamics is likely to trigger a surge in opportunistic behaviours among market participants. Consequently, SEP owners may

face mounting transaction costs associated with licensing negotiations and strong risks of failing to recover their investments. By the same token, the Draft Regulation could inadvertently undermine its own objectives by dissuading collaborative standardisation efforts in favour of proprietary solutions. Indeed, as acknowledged by the European Commission in the Impact Assessment, standard creation is a resource-intensive R&D activity, and lengthy negotiations and the high cost of licensing may reduce the incentives for SEP owners to participate in the development of new standards.

- 57 Finally, we argue that the Draft Regulation has failed to consider the financial dimension of technological innovation, namely the potential of SEPs to function as valuable financial assets. By reviewing the relevant theoretical and empirical literature, the paper demonstrates that SEPs are one of the most promising IP asset classes to be used as financial collateral and they receive more favourable prudential treatment than other intangibles. Indeed, SEPs present all the features to sustain R&D and financial investments in technological innovation. In fact, it is essential for a modern standardisation framework to provide incentives for carrying out R&D investments in the first place.
- 58 By undermining the economic value of SEPs in terms of enforcement and monetisation, the Draft Regulation is watering down their potential to serve as valuable financial collateral and therefore to help innovators access debt financing. Disregarding the fundamental links between patents and finance may have serious consequences on innovation and competitiveness.

⁹⁷ Martin Husovec, 'A Human Right to Ever-Stronger Protection?', (2023) 54 IIC 1483.

Trademark protection for faces?

A comprehensive analysis on the benefits and drawbacks of trademarks and the right to facial image

by **Barna Arnold Keserű** *

Abstract: The purpose of this paper is to present a comprehensive framework for the possibility of trademark protection for human faces. In the case law of the European Union Intellectual Property Office there are a few examples of trademarks, which consist of only photorealistic human faces. Private law protects the use of images; however, the trends of recent years demonstrate that trademarks could also have a role in such protection. The author aims to analyze the similarities and differences between trademark protection and personality rights in order to determine whether trademarks for faces are necessary or not. The over-

arching analysis compares twelve aspects of the two ways in which the legal systems protect facial imagery, highlighting their various advantages and drawbacks. The comparison includes the following attributes: function of protection, scope of protection, territorial dimensions of protection, temporal dimensions of protection, conditions of protection, content of protection, limitations and exceptions, transferability of rights, enforcement of rights, requirement of use, termination of rights and costs.

Keywords: Trademark, Right to Image, Individual Rights, Intellectual Property

© 2024 Barna Arnold Keserű

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Barna Arnold Keserű, Trademark protection for faces? A comprehensive analysis on the benefits and drawbacks of trademarks and the right to facial image, 15 (2024) JIPITEC 88 para 1

A. Introduction

1 In the global economy, competitiveness is key to the long-term success of companies. Competitiveness has a number of core elements, one of which is the intellectual property right. In the so-called II. HAG decision the European Court of Justice held that trademark rights are an essential element in the system of undistorted competition.¹ As Luszcz noted, trademarks are lighthouses among the numerous

goods and services of varying quality, providing commercial information for the consumers.²

2 Trademarks are usually words or logos; however, any kind of sign may be subject to protection if it is capable of distinguishing goods or services. In recent years the Board of Appeal of the European Union Intellectual Property Office (hereinafter referred to as EUIPO) has recognized that photographs of human faces are eligible for trademark protection. This evolving case law has not as yet received considerable critical attention; nevertheless, it raises many practical and theoretical questions. This study

* Associate professor, Head of Civil Law and Civil Procedural Law Department, Széchenyi István University. Attorney at law. ORCID: 0000-0002-6789-5246.

1 C-10/89. SA CNL-Sucal NV. v. Hag GF AG (1990), European Court of Justice.

2 Luszcz Viktor, 'A védjegy és a versenyjogi szabályozás összeegyeztetése az Európai Közösségben' [2001] Magyar Jog, 121.

focuses on the fundamental question: compared to personality rights, is trademark protection a legitimate alternative? Does trademark protection have more benefits than the right to facial image?

- 3 The findings of this research should make an important contribution to the marketing and advertising industry, and especially for fashion models. This could prove useful, not only for European market actors and intellectual property offices, but also for non-Europeans since the investigated issues affect the core elements of trademark law, which are the same globally.
- 4 There is a limited amount of qualitative analysis on this topic, especially in academic literature. Terpstra (2021) briefly analyzed a few Dutch examples of portrait trademarks, and argued that there are some essential objections against that phenomenon, and even if they may be overruled, not everyone would see any added value of portrait trademarks.³ Troutt (2005) investigated the application of trademark protection to actual persons from a theoretical perspective (including racism and slavery), stating that “critical theoretical interpretation of Lanham Act boundaries and culture of mass marketing suggest that the day may not be far off when a human persona may prove sufficiently distinctive in interstate commerce to qualify as a protectable signifier”.⁴ That day has already come to pass, as will be illustrated. Troutt also provides insight into a trademark infringement case related to the golf legend Tiger Woods.⁵ Woods’ portrait was used without permission, thus he sued for trademark infringement. The court denied the lawsuit on all grounds, arguing that Tiger Woods cannot be a walking, talking trademark. Images and likenesses of Woods are not protectable as a trademark because they do not fulfil the trademark function of designation. Dogan and Lemley (2006) argued from a moral perspective that the people who claim ownership rights over their personalities are willing, in many cases, to sell their dignity for a fairly low price. It is a form of paternalism where individuals are protected against their own commodification.⁶

3 Syb Terpstra, ‘Famous faces: the portrait as a trademark’ (2021, <https://bureaubrandeis.com/famous-faces-the-portrait-as-a-trademark/?lang=en>.)

4 David Dante Troutt, ‘A Portrait of the Trademark as a Black Man: Intellectual Property, Commodification, and Redescription’ (2005) 38 U.C. Davis Law Review, 1141 (p. 1142.)

5 ETW Corp. v. Jireh Publ’g., Inc. 332F.3d 915 (6th Cir. 2003).

6 Stacey L. Dogan & Mark A. Lemley, ‘What the Right of Publicity Can Learn from Trademark Law’ (2006) 58 Stanford Law Review 1161 (p. 1182.).

- 5 A further study will examine the landmark decisions of the EUIPO in cases involving the protectability of faces and the trademark law issues arising from them. For the purposes of this study, it is sufficient to point out, that in the first instance the EUIPO has refused the application on the basis of lack of distinctiveness, but the Board of Appeal (hereinafter referred as BoA) has repealed the decisions and ordered the trademark applications to be published in accordance with the general registration procedure. The first indicator of the new case law concerns the Dutch model Maartje Robin Elke Verhoef, who has applied for trademark protection on her face on 14 October 2015. It was initially rejected, but in November 2017 the BoA held that the portrait photo met the criteria for protection.⁷ Rozanne Verduin and Yasmin Wijnaldum has also filed their portrait photo on 16 October 2017, and 11 September 2018. According to the same script, the BoA has annulled the refusal decisions and ordered to continue both registration procedures in May 2021.⁸ In recent months two additional cases have been concluded with the same result. The portrait of Jill Kortleve, filed on 18th of January 2022 was supported by the BoA in December 2023,⁹ and the portrait of Puck Schrover applied on 19 April 2023 was approved by the BoA in January of 2024.¹⁰

B. METHODOLOGY AND THE SOURCE OF DATA

- 6 The subject of the investigation are portrait trademarks. This is not an existing category in trademark classifications. Throughout the paper, the term portrait trademark refers to trademarks, which only contain photorealistic representation of human faces, either of real persons or computer-generated persons, and the trademark does not include any other distinctive elements such as names, titles or logos. Non distinctive frames or backgrounds are allowed. The signs may be colored or black and white as well.

7 EUIPO, Decision of the Fourth Board of Appeal in the case R 2063/2016-4 (EUTM 014679351)

8 EUIPO, Decision of the Fourth Board of Appeal in the case R 468/2021-4 (EUTM 017953534), EUIPO, Decision of the Fourth Board of Appeal in the case R 378/2021-4 (EUTM 017358458).

9 EUIPO, Decision of the Fourth Board of Appeal in the case R 1704/2023-4 (EUTM 018640603)

10 EUIPO, Decision of the Fourth Board of Appeal in the case R 2173/2023-4 (EUTM 018864324)

- 7 From a practical point of view, searching for portrait trademarks in the EUIPO eSearch plus database is not an easy task. At present, there is no separate administrative category for portrait trademarks; in most cases they are registered as figurative trademarks and less frequently as 3D trademarks. The Vienna Classification (from January 1, 2023 the 9th edition is in force) provides an opportunity to search for human faces among figurative trademarks (2.1.1. class for men, 2.3.1. for women, 2.5.1. for children). However, it has no allowance for the type of visualization, so in this way a uniquely drawn figurative face is in the same Vienna class as the photorealistic portraits. It shall be noted that the Vienna classification of EU trademarks are not completely consistent; e.g., the 011552321 trademark with the photo of the Hungarian Judit Stahl is classified as just a picture (22.05.01.), not a human face. However, in this class there are only 539 EU trademarks, which makes it easy to find realistic photos among them.
- 8 Irrespective of the actual status, among the circa 3400 EU trademarks with female faces, 50 trademarks and trademark applications can be listed according to the eSearch plus, which are photorealistic photos without any distinctive element (like names or logos). From the 50 listed trademarks, 38 have been filed since 2015, and 21 since 2021. Using the same selection method, among the approximately 8800 EU trademarks with male faces there are 67 photorealistic photos, or computer-rendered faces. More than half of these trademarks have been filed since 2021. It should be noted that a trademark application filed in 2022 consists of a female face although it is categorized as a male face in the EUIPO database, so the presented data is corrected accordingly. Only 4 trademark applications were filed for children's faces, three of them for boys, and one for a family photo with boys and girls.
- 9 In the Annex the application number for the collected trademarks can be found. The following table summarizes these data:
- 10 Despite the fact that the absolute number of portrait trademarks is still low, there has been a progression in the last years in the number of new applications. The author deduces from the data gathered that the increasing number of portrait trademarks justifies the comprehensive research of this topic. Among the female trademarks, the majority of signs are photos of fashion models, while among males the earliest trademarks refer to sportsmen, like Michael Schumacher or John Cena and other wrestlers. In the last years, mainly Dutch applicants started to exploit the trademark protection, and a new trend is the application of AI-generated realistic faces; 46 such applications were filed by Trend Development BV., and all of them have already been registered. It should be noted that the high number of applications relating to only one applicant distorts the objectivity of trends.
- 11 The study is based on the qualitative assessment of trademark law and private law. During the comparison of trademark protection and personality rights, the detailed assessment of personality rights will be carried out according to Hungarian law, as there isn't unified private law in the European Union. However, the aspects examined are the same in each country, so the structure of comparison can be applied to any legal system. The main contribution of this paper is to provide the necessary comparative framework for further evaluations. In the paper the term of the right to facial images is used as a synonym for the right to personal portrayal and the right to likeness.
- 12 On the side of trademark law the rules of Regulation (EU) 2017/1001 of the European Parliament and of the Council on the European Union trade mark (hereinafter referred to as EUTMR), and the Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast) (hereinafter referred to as Trademark Directive) provide the basis for the comparison.
- 13 The analysis is carried out according to twelve dimensions which may be important for strategic decisions. In the conclusion the results of the comparison are illustrated in a point-scale based spreadsheet.

According to EUIPO database	Male portrait	Female portrait	Children portrait
Total number of applications	67	50	4
Currently under protection	57	23	3
Currently under examination	1	10	0
Before Board of Appeal after the refusal	0	4	0
Filed after 2015	48	38	2
Filed after 2021	38	21	0

1. Table on the portrait trademark applications at the EUIPO until 26th November, 2023. Compiled by the author.

C. TRADEMARK PROTECTION VS. PERSONALITY RIGHTS FOR HUMAN PORTRAITS

I. Function

14 It is generally accepted that the function of trademarks is to identify the goods or services of the owner and to distinguish them from the other competitors' goods and services. This function can be detected in the ancient times as well, where the signs used by the producers served as the indication of source of origin.¹¹ However, the value of modern trademarks lies in their selling power, because – as Schechter argued – the primary function of trademarks shall be the creation and retention of custom.¹² The traditional approach is supported by the recital (11) of the EUTMR and recital (16) of the Trademark Directive. This function shall be considered within the scope of trade. Article 10. of Trademark Directive provides exclusive rights to the owners, entitling them to prevent all third parties from using the trademark without consent in the course of trade, in relation to the goods and services. Thus, the scope of trademark protection covers only the commercial activities, which is clearly a serious limitation. Non-commercial activities, such as private use, political use, and use by civil organizations are beyond the scope of trademark law if they lack commercial elements. This is in harmony with Article 16. of the TRIPS Agreement which also limits protection to trade.

15 Trademark is a form of intellectual property. In fact, it is a special form because, unlike other types of intellectual property, it does not necessarily require creative activity. Creativity is at the heart of patent or copyright, but not for the commercial signs of origin, at least not at first sight. However, in order to avoid the grounds for refusal, the given sign shall have something new, uncommon, and original. It is not prescribed by the law directly, although through the system of grounds for refusal it is obvious that a commercial sign which is merely descriptive, or generally used in the course of trade, or, indeed, just the mere copy of an existing trademark, is not acknowledged by the law, and can be excluded from protection, either ex officio or upon request. These requirements can be deemed as the manifestation of creativity. From this perspective a serious concern arises: how can we classify a human face as a form of intellectual property? Natural faces – which are not

designed by a surgeon – are the “products” of nature. They were not created by anybody, they evolved by the laws of nature and evolution. The author argues that the basic philosophy of intellectual property rights is to protect human creativity, even in the trademark law as well, despite the fact that is not immediately obvious. The protection of human faces expands the theoretical foundation of intellectual property.

16 In the majority of trademarks collected, the owner is not the subject of the sign but a legal entity, such as advertising and model agencies. This leads us to a very important question: who is the owner of the face? The de facto owner is, of course, the individual who “wears” that face; however, if the trademark owner is another person, then the legal owner will be different from the natural bearer of that sign. It is a philosophical contradiction of trademark law: how can somebody own exclusive rights to a sign, if the sign inseparably belongs to a human, who cannot be forced to cease the wearing of it. Immanuel Kant shall be quoted at this point: *“Man cannot dispose over himself because he is not a thing; he is not his own property; to say that he is would be self-contradictory; for in so far as he is a person he is a Subject in whom the ownership of things can be vested, and if he were his own property, he would be a thing over which he could have ownership. But a person cannot be a property and so cannot be a thing which can be owned, for it is impossible to be a person and a thing, the proprietor and the property.”*¹³ This citation clearly depicts the immanent contradiction raised by portrait trademarks: the exclusive economic rights provide economic power over a “property”, which cannot be separated by the human subject, since it is an immanent characteristic of the individual. Whereas the evolution of civil rights, especially human dignity and legal equality, led to the fundamental principle that no person shall be regarded as the property of others,¹⁴ trademark protection for portraits reopens the way for economic slavery of humans through the exclusive control of their bodies.

17 Civil law provides personality rights to protect various aspects of an individual, such as the right to bear a name, the right to reputation, the right to privacy, and the right to a facial image. According to the Hungarian Civil Code (hereinafter referred to as Civil Code), the consent of the individual affected shall be required for producing or using their likeness or recorded voice.¹⁵ The function of personality rights is to provide legal protection for the immanent

11 Vida Sándor & Kováts Borbála, 'Árjelzők az ókorban' [2020] Iparjogvédelmi és Szerzői Jogi Szemle 78-79.

12 Frank Isaac Schechter, 'The Rational Basis of Trademark Protection' (1927) 40 Harvard Law Review 813 (p. 813-814).

13 Troutt, *ibid.* 1142, citing Margaret Jane Radin, 'Market Inalienability' (1849) 100 Harvard Law Review.

14 Article 4. of Universal Declaration of Human Rights.

15 Article 2:48(1) of Civil Code

slices of personality. Unlike trademarks, personality rights offer protection, not only in the course of trade, but generally, without any restriction. This way a privately taken photograph of an individual infringes the right to a facial image in the absence of consent. It is a major difference between trademark protection and the right to a facial likeness in favor of the latter.

which leads to the same effect as personality rights.¹⁹ However, while this range of protection is the basic characteristic of the right to personal portrayal, in the case of trademarks, only the trademarks with reputation may obtain the same legal consequences.

III. Territoriality of rights

II. Scope of protection

18 In theory, the essential function of the trademarks can be achieved through the exclusive rights granted to the owner. Since the adoption of the Paris Convention, it has been a widely accepted feature of trademark law that the owner may exclude any third party from using the sign in respect of identical or similar goods or services.¹⁶ This exclusive right is twofold: First, it refers to the fact that the trademark owner is entitled to use the sign, and second, everybody else is prohibited from such a use. The use of own sign does not require any legal procedure, while the possibility of excluding others from that use is the result of the trademark registration (not to mention some cases of unfair competition, which, compared to trademark law, require more conditions to prohibit the use by others).¹⁷ The list of goods or services is a necessary element of trademark application, which shall be structured according to the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks. Therefore, a portrait trademark confers exclusive rights only in respect of the list of goods and services, and not in general. In contrast, the right to a facial image has no such limitation; it exists independently from any types of goods or services. The rightsholder can enforce the right to a facial image against any unlawful act in any field. This is a major advantage on the side of personality rights.

19 The Paris Convention recognizes well-known trademarks, and both the Trademark Directive and EUTMR recognizes the protection of trademarks with reputation.¹⁸ Such trademarks enjoy a wide range of protection, irrespective of the list of goods and services. In the case of famous persons their portrait trademark may acquire such broad protection,

20 Intellectual property rights are territorial by nature. Territoriality is one of the main features of intellectual property rights.²⁰ It is a clear consequence of the territorially varying legal systems. The Paris Convention introduced the right of priority based on earlier trademarks, the purpose of which is to reduce the drawbacks of territoriality during the spatial expansion of the owner. Similarly, personality rights are also territorial, as they are the part of the civil law of the country concerned. Intellectual property rights are far more internationally harmonized than civil law. The Paris Convention of 1883 and Berne Convention of 1886 initiated the international harmonization of this area, and it is still ongoing. At that time, only a few countries had already adopted a civil code; for instance, Hungary's first civil code was adopted only in 1959.

21 Nowadays, traditional civil law (including personality rights, law of property, law of inheritance, law of obligations and so on) is not harmonized at an international level, and only to a small extent harmonized at an EU level, which mainly focuses on consumer protection aspects.²¹ Deeper harmonization – especially in the field of personality rights – is not necessary at all, since every EU member state has its unique legal tradition, and the social order and social values may differ country by country. However, since intellectual property rights are considered primarily as an economic tool,²² the

16 Article 6bis of Paris Convention.

17 Beck Salamon, *Magyar védjegyjog* (Kertész József Könyvnyomdája, 1934) 159-160.

18 Article 9. (2)c) of EUTMR and Article 10 (2)c) of Trademark Directive.

19 Munkácsi Péter, 'A közismert és jó hírű védjegyek az Európai Bíróság „General Motors Corporation v. Yplon SA („Chevy”)” döntése tükrében' [2000] Iparjogvédelmi és Szerzői Jogi Szemle 22.

20 Bobrovsky Jenő, 'Az enyém, a tied és a miénk a szellemi tulajdonban. Áttekintés a közkinccs és a szellemi magántulajdon egyes összefüggéseiről az Internet tükrében' (p. 13.) <http://www.mie.org.hu/pdf/Public_domain-Mie.pdf>

21 Fazekas Judit, *Fogyasztóvédelmi jog 2.0* (Gondolat Kiadó, 2022) 17-27.

22 Szalai Péter, 'A védjegyjogtalom sajátos problematikája a szellemi tulajdonjogban' in Keserű Barna Arnold – Kőhidi Ákos (eds.), *Tanulmányok a 65 éves Lenkovics Barnabás tiszteletére* (SZE-DFK – Eötvös József Könyv-és Lapkiadó Bt.,

European Union provides a geographically unitary set of rights for the single market.²³ An excellent instance is the European trademark system, which ensures a unitary character for EU trademarks. It means that it has equal effect throughout the Union in respect of any status issues, such as registration, transfer, surrender or cancellation.²⁴

- 22 For the European market, the unitary EU trademark offers an advantage over the right to facial images, because trademark law provides the same content on the same legal basis for the trademark owner throughout the European Union, while the general civil law rules, and the extent of the right to image may vary from one member state to another. Outside of the European Union this advantage diminishes in the absence of regional territoriality.

IV. Temporal validity of rights

- 23 With regards to the term of protection, there are significant differences between intellectual property rights. The general theory behind copyrights and patents is that the owners and their successors have the possibility to exploit the economic potential of their creation for a limited period of time, after which the works and inventions will belong to the public domain. From this perspective, intellectual property rights are temporary, while the public domain is permanent and infinite. This thesis is supported by the historical development of intellectual property rights and expressed by the Article 8.²⁵ of the Constitution of United States of America.²⁶ However, trademark law follows a different logic. According to Adler, trademarks provide exclusivity for indefinite time.²⁷ There is no such public domain-driven reason for limited protection as in the case of copyright and patent. The term of protection and the requirement for renewal is a purely rational feature of trademark law, as it

can lead to the termination of formally registered but unused, unnecessary trademarks. It serves as a filter to purge the register of obsolete trademarks.²⁸ The TRIPS Agreement requires the member states to register the trademarks for a minimum of 7 years, and unlimited number of renewals shall be provided by the law.²⁹ In contrast, the vast majority of the countries offer 10-year terms for registered trademarks. According to the data gathered by World Intellectual Property Organization a decade ago, 10 years is the most common duration, whereas Bangladesh registers trademarks perpetually and Zambia applies the 7-year rule of TRIPS.³⁰ The Trademark Directive requires the registration of trademarks for a period of 10 years from the date of filing the application, and those may be renewed for further 10-year periods without limitation. The EUTMR applies the same rule for EU trademarks.³¹ Consequently, trademarks may be maintained forever, even after the death of the portrait model.

- 24 By contrast, personality rights may exist only during the life of the person. After death, in the absence of legal capacity, personality rights would be meaningless. Some personality rights – like the right to prevent the use of a facial portrait – may transform after death to the right in memoriam.³² The Civil Code prescribes that in the case of any violation of the memory of a deceased individual, the relative and/or the person named heir apparent in the will of the deceased shall be entitled to bring court action.³³ It shall be noted, that the rightsholder of the right in memoriam is the relative or the heir of the deceased individual, since the dead, of course, cannot obtain any rights. This right has a narrower reach than the right to facial image because the relatives or the heir may enforce it only in the case of violation of memory; however, not every use of image harms a memory. Such acts may be prevented by the living individual according to the right of likeness. The temporal limitation of personality rights and the unique transformation for right in memoriam is a

2015), 414 (p. 425-427).

23 *Study on the Overall Functioning of the European Trade Mark System*, (Max Planck Institute, 2011) (p. 145-146.)

24 Article 1.(1) of EUTMR.

25 „The Congress shall have Power To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries”

26 Bobrovsky, *ibid.* 19-20.

27 Emmanuel Adler, 'System des Österreichischen Markenrechtes' (Manzsche Verlags- und Universitätsbuchhandlung, 1909), cited by Beck, *ibid.* 96.

28 Beck, *ibid.* 96.

29 Article 18. of the TRIPS Agreement.

30 WIPO/STrad/INF/1 Rev. 1. Standing Committee on The Law of Trademarks, Industrial Designs and Geographical Indications, 2010, World Intellectual Property Organization, 182-185.

31 Article 52 of EUTMR and Article 48 of Trademark Directive.

32 Görög Márta, *A kegyeleti jog és a nem vagyoni kártérítés* (Pólay Elemér Alapítvány, 2008).

33 Article 2:50 of Civil Code, Görög Márta, 'A kegyeleti jog gyakorlásának jogosultjairól és az érvényesíthetőség időbeli korlátairól' [2005] Polgári Jogi Kodifikáció 15 (p. 15-19).

drawback as compared to the practically unlimited validity of trademarks.

V. Conditions of protection

- 25 There is a significant difference between trademarks and the right to facial image in terms of the conditions for protection. Registered trademarks require a procedure before the competent intellectual property authority. The registration procedure has been a fundamental element of trademark laws since the adoption of Paris Convention. The relevant legal sources assume that trademarks are created by registration, and the structure of the legislation follows this procedural logic. It shall be noted, that some countries which provide protection for a limited extent for unregistered trademarks, while others recognize only the registered form of trademarks, and have civil law, competition law and criminal law provisions for other commercial signs which are not trademarks.³⁴
- 26 To acquire protection, the sign shall satisfy the positive requirements: essentially it must have a distinctive character and it must be capable of being represented in a manner which enables the competent authorities and the public to determine the clear and precise subject matter of the protection.³⁵ On the other hand, the sign shall avoid the grounds for refusal (both absolute and relative grounds) as those are the negative requirements of protectability. Besides, the application shall pass more examination phases during the registration process in order to have grant of protection, which may take a considerable amount of time.
- 27 Personality rights are different from trademarks in the way they are created. Personality rights exist *ex lege*; persons are entitled to personality rights by the force of law. There is no need for administrative procedure; nobody makes a decision to grant personality rights. They are provided for every person (including legal entities where the given personality right does not inherently pertain solely to human beings)³⁶ only by the fact that every human has the right to dignity, and personality rights stems from dignity.³⁷ In this sense, personality rights are the projection of legal capacity and every person

34 Verena von Bomhard & Artur Geier, 'Unregistered Trademarks in EU Trademark Law' (2017) 107 Trademark Rep 686-698.

35 Article 4. of EUTMR and Article 3. of Trademark Directive.

36 Article 3:1. of Civil Code.

37 Article 2:42. Civil Code.

automatically possesses these rights from the beginning of their legal capacity. Consequently, the right to facial image has a striking advantage over trademarks, since no action and time is required by individuals to obtain this right.

VI. Content of protection

- 28 There are a few similarities in respect of the content of protection between trademark and the right to facial images; however, there are also a number of important differences. The primary function of both rights is to grant exclusive rights to the owner. By exclusivity every third party may be prevented from the use of the subject of protection. However, as described above, exclusive rights on trademarks can be enforced only in the course of trade and in respect of the list of goods and services (excluding trademarks with reputation). The concept of use may cover a wide range of activities. The Trademark Directive and EUTMR simultaneously presents instances of use, such as affixing the sign to the goods or to the packaging, offering or putting the goods on the market, or stocking the goods for those purposes, importing and exporting the goods under the sign, using the sign as a trade or company name, and using the sign on business papers and in advertising.³⁸
- 29 In contrast, the content of the right to facial image may vary from country to country. According to the Civil Code, it provides protection against the unauthorized production or use of images. Prior to 2014, the previous Civil Code only prohibited unauthorized use, whereas the current law has extended the scope of protection to production as well.³⁹ This constitutes a wide range of enforcement as it is not limited to any type of goods or services, nor to commercial activities.

VII. Limitations and exceptions

- 30 As legal systems have historically evolved, the number of limitations of rights has risen. Just as rights do not exist without limits, the protection of trademarks and the right to facial image also have their own legal limitations. Article 17. of the TRIPS Agreement allows the member states to introduce exceptions for trademark protection. The Trademark Directive under Article 14. lists certain

38 Article 10 of Trademark Directive and Article 9 of EUTMR.

39 Szeghalmi Veronika, 'A képmás polgári jogi védelme és a hazai szabályozás alapvonalainak áttekintése európai példákon át' [2014] Médiautató 53 (p. 55).

limitations of trademarks, where the owner is not entitled to prohibit a third party from using the sign. However, the exhaustion of the rights conferred by a trademark is regulated in a different article, it is undoubtedly one of the limitations of the exclusive rights of use. The EUTMR applies the same set of limitations and exceptions for European Union trademarks.

- 31 The limits of rights to personal portrayal vary country by country. In Hungary, there is a general clause for personality rights which defines the aims of these rights, but simultaneously sets general limits to them. According to the Civil Code, each individual is entitled to freely exercise their personality rights, but only within the framework of the law and within the rights of others. This means that the exercising of personality rights cannot result in the violation of law or harm another persons' rights.⁴⁰ Besides, the right to a facial image has specific limitations as well. A recording may be produced and used without the authorization of the individual if the recording is created in a crowd, or it is connected to activities in a public event. According to Hungarian case law, the courts apply the crowd as an exception if the visual recording aims to catch individuals as an uncountable mass of people, and to demonstrate the crowd effect. Even if the individuals can be recognized, for the sake of illustration at important events, the crowd can be recorded. The other element of the restrictions relates to such public events motivated by public interest;⁴¹ namely, political summits, publicly held speeches, riots, or events organized by public bodies. The common feature of these events is that they are part of public affairs.

VIII. Transferability of rights and in rem attributes

- 32 As explained earlier, the commercial exploitation of trademarks is a crucial point of protection. There are numerous methods of exploitation, one of which is the partial or entire transfer of ownership. Trademarks may be transferable, as Article 21. of the TRIPS Agreement requires the member states to provide the transferability of trademarks, either with or without transfer of the business to which the trademark belongs. Previously, the Paris Convention also recognized the transferability of trademarks. The version of the text in force at the

time of its adoption did not contain any guidelines on transfer. The Convention was amended in 1937 at the London Conference to include rules on assignment. Reflecting the contemporary conflicting trends in trademark law at the time, the amendment was intended to maintain the status quo, but not to force the member states to adopt new rules.⁴² It is clear from the current wording that the primary concern was to respect the trademark laws of the Member States and to preserve their independence. In particular, the Paris Convention was amended to take account of the interests of the United States, which left it to the discretion of the Member States to recognize the validity of a transfer that is made only with the undertaking or the business (goodwill).

- 33 Section 4. of EUTMR bears the title of EU trademarks as objects of property, which clearly refers to the economical consideration of trademarks. Section 5. of Trademark Directive also has the same title. Both recognize the assignment in gross, which means that the transfer may be carried out without the transfer of any other business assets, such as the undertaking partially or totally, or trade secrets.⁴³
- 34 The commercialization of personality rights varies on a wide scale among the different legal systems. As a general rule, in continental civil law countries the transfer of personality rights is not possible, or just to a limited extent, or only in respect of certain personality rights.⁴⁴ Hungarian Civil Code does not contain a specific provision on the prohibition of the transfer of personality rights. However, from the jurisprudence it is a well-established doctrine that personality rights are the derivatives of human dignity and thus non-transferable.⁴⁵ In recent years some scholars have argued in favor of new economic theories of personality rights which include the possibility of transfer by the fact that in the current socio-economic era some rights – like the right to

40 Article 2:42. of Civil Code. Fézer Tamás, 'Harmadik rész. Személyiségi jogok', in Osztovits András (ed.), *A Polgári Törvénykönyvről szóló 2013. évi V. törvény és a kapcsolódó jogszabályok nagykommentárja*, Vol. 1. (Opten, 2014) 249 (p. 255-258.)

41 Győr Regional Court of Appeal, ÍH2018.131.

42 Irene Calboli, 'Trademark assignment „with goodwill”: a concept whose time has gone' [2005] *Florida Law Review* 772 (p. 817).

43 Keserű Barna Arnold, 'A magyar védjegyek átruházására vonatkozó szabályok összehasonlítása a közösségi védjegyvitalom átruházásának szabályaival, különös tekintettel a szellemi tulajdon elméleteire' [2011] *Iparjogvédelmi és Szerzői Jogi Szemle* 42 (p. 67).

44 Horst-Peter Götting, *Persönlichkeitsrechte als Vermögensrechte* (Paul Siebeck, 1995).

45 Görög Márta, 'A képmáshoz és hangfelvételhez való jog védelmének fejlődéstörténete és a jogosultat megillető „rendelkezési jog” gyökere', in Görög Márta – Menyhárd Attila – Koltay András (eds.), *A személyiség és védelme. Az Alaptörvény VI. cikkelyének érvényesülése a magyar jogrendszeren belül* (ELTE-ÁJK, 2017), 253 (p. 264).

a name or right to facial image – obviously have monetized value.⁴⁶

- 35 In order to exploit the potential economic value of facial images, trademark protection offers the full range of property rights, so it may be transferred or licensed, levied in execution, be given as security or be the subject of other rights in rem. On the contrary, the right to facial image as one of the personality rights is strongly linked to the individual; thus, economic exploitation is extremely limited by assignments.

IX. Enforcement of rights

- 36 *Lex imperfecta* in Roman law is such a norm which forbids something to be done and, if this has been done, neither voids it nor imposes a penalty on the person who has violated the law.⁴⁷ *Lex imperfecta* is a rule without consequences, thus unenforceable. Efficient legal protection requires the possibility of enforcement (*lex perfecta* norms), since the real value of a right is determined by the effective, quick, and inevitable enforcement. Enforcement of intellectual property rights is exceptionally harmonized at international levels compared to other areas of private law, in particular, personality rights. Before the TRIPS Agreement, the provisions dealing with enforcement of rights were basically general obligations to provide legal remedies and, in certain cases, for the seizure of infringing goods. At that time the enforcement was left primarily to national legislation. However, the enforcement section of the TRIPS Agreement was one of the most impactful achievements of the diplomatic conference.⁴⁸ The European Union has also taken steps to harmonize the enforcement of intellectual property rights across the EU, with the European Parliament and the Council adopting the Directive on the enforcement of intellectual property rights on 29 April, 2004. Although the detailed rules may

differ within the EU and the TRIPS member states, the trademark owners may generally foresee the applicable measures, procedures and remedies if their rights are infringed.

- 37 In respect of personality rights, neither procedural nor substantive harmonization exists for enforcement. This is clearly a weak point for the right to facial image. In Hungary, the Civil Code provides basically the same civil law remedies against infringements of personality rights as for intellectual property rights, although not to the full extent. Apart from the obvious remedies like declaration of infringement, discontinuation of infringement, restoration of the previous state, seizure of goods or depriving the infringing goods from unlawful nature, the most remarkable sanction is that the person may claim from the violating party the financial advantage acquired by the infringement according to the principle of unjust enrichment. This is independent from attributability; only the fact of infringement is necessary to apply this measure. The minimum financial advantage for unlawful use of facial images is the sum of the license fee which shall be paid at market value for the use of image. A specific remedy, which is available only in intellectual property cases, is to demand information on the identity of persons who were involved in the production or distribution of the infringing goods.

- 38 In Hungary there is a special remedy for personality rights, the so-called grievance fee, which is a monetary claim for violation of personality rights. The rules of liability for damages shall apply to this claim; however, no damages shall be proved.⁴⁹ The aim of the grievance fee is not to remedy the undesirable shifts in pecuniary relations like the purpose of tort law, but to compensate the aggrieved party for any immaterial, non-pecuniary disadvantages and inconveniences. The secondary function of the grievance fee is to punish the infringing party. The punishment is manifested in the amount of the fee, which is determined by the court, considering the degree of responsibility, the number or duration of the infringement, the severity of the infringement and its impact upon the aggrieved party and their environment.⁵⁰

- 39 While the civil law remedies and injunctions for trademarks and right to facial images are fairly similar and balanced, the degree of protection by criminal law significantly differs. According to the provisions of Article 61. of the TRIPS Agreement, the member states shall provide for criminal procedures

46 Schultz Márton, *A személyiségi jog vagyoni értékminőségének elvi és dogmatikai alapjai, különös tekintettel a névjogra* (PhD dissertation, 2019., Menyhárd Attila, 'Forgalomképes személyiség?' in Menyhárd Attila – Gárdos-Orosz Fruzsina (eds.), *Személy és személyiség a jogban* (Wolters Kluwer, 2016) 65, Harkai István, 'A képmáshoz való jog és pénzben kifejezhető értéke a számítógépi programalkotásokban' in Báró-Farkas Margit Chiara – Kemény Zsanett (eds.), *A pénzügyi világ kihívásai a 21. században* (Pro Talentis Universitatis Alapítvány, 2018).

47 Thomas A. McGinn, 'The Expressive Function of Law and the Lex Imperfecta' (2015) 11 Roman Legal Trad, 28.

48 Daniel Gervais, *The TRIPS Agreement: Drafting History and Analysis*, (Sweet & Maxwell, 2008), (p. 440).

49 Sándor István, 'A képmáshoz való jog és a sérelemdíj bírósági gyakorlatának tendenciái' [2020] Belügyi Szemle 53 (p. 63). DOI: 10.38146/BSZ.2020.4.2

50 Article 2:52. of Civil Code.

and sanctions to be applied at least in cases of willful trademark counterfeiting or copyright piracy on a commercial scale. The Hungarian Criminal Code consists of more crimes against intellectual property rights, including counterfeiting and trademark infringement as well.⁵¹ Conversely, the protection of the right to a facial image by criminal law is highly limited. While the right to facial image basically belongs to the field of civil law, criminal law only prohibits the production or publication of fake images that harm the honor of the injured party. This way, many of the unlawful, commercial use of facial images are beyond the scope of criminal law, unless those images are not protected as trademarks either.

X. Requirement of use

- 40 Trademarks as an economic monopoly right are designed to provide exclusivity, but in return this exclusive right shall be used. Trademarks in modern trademark laws cannot be registered just to permanently block the market; this is prevented by the requirement of genuine use.⁵² Although Article 19. of TRIPS does not require an obligation to use the trademarks, it recognizes that such national requirements with the provision of use are required to maintain a registration. This registration may be cancelled only after an uninterrupted period of at least three years of non-use, unless valid reasons based on the existence of obstacles to such use are shown by the trademark owner. The two main components of this rule are the minimum of years of non-use to apply detrimental consequences, and the possibility of exemption with valid reasons.⁵³
- 41 European law extends the period for lack of genuine use to an uninterrupted five years from the date of registration or later at any time during the protection, and if this period expires, the trademark

shall be subject to negative sanctions.⁵⁴ The lack of genuine use dismantles the power of exclusivity, since an opposition or a cancellation request based on non-used trademark will be rejected, a non-used trademark cannot be enforced against trademark infringement, and finally, anyone can submit a request for a non-used trademark to be revoked.

- 42 This requirement of genuine use and all the negative effects resulting from its absence are justified by the economic function of trademarks. To the contrary, personality rights stem from constitutional human rights; in fact the recognition of personality rights is one form of the protection of human rights. This origin makes it clear that genuine use cannot be required in the case of personality rights. The right to facial images shall not be exercised obligatorily in order to maintain the protection, and the individual will never lose the possibility of enforcement in case of non-use. The right to a facial image is granted by the law without any further conditions.

XI. Termination of rights

- 43 There is a considerable difference between trademarks and personality rights in respect of termination, determined by their legal nature. Trademark protection may cease to exist on more legal grounds. The most common case of termination is the lack of renewal, as described above; the trademark owner shall periodically file an application for renewal and pay the fee in order to maintain protection. Chapter VI. of EUTMR provides provisions for surrender, revocation and invalidity as different reasons for termination. As a trademark is granted by an application, it may be surrendered by the request of owner, either in respect of some or all of the goods or services. Revocation procedures refers to cases where maintaining the protection will be detrimental to the general purposes of trademarks. As explained above, the requirement of use is a basic principle of trademark law by economic nature of trademarks; hence, non-use or the lack of genuine use is the most frequently cited ground for revocation. Another ground for revocation is the loss of distinctiveness. If a trademark is extremely widespread and leads to a nearly monopolistic situation on the market, the sign may become the common name in the trade for the product or service for which it was registered. This way the trademark loses its most essential attribute, which makes it impossible to maintain its protection. The third ground for revocation in the EUTMR relates to the informational function of trademarks, as a trademark shall be declared to be revoked if it is liable to mislead the public, in particular as to the

51 Chapter XXXVII. of Act C. of 2012 on Criminal Code.

52 This requirement is relatively new, most of the EU member states adopted this rule only in the second half of the 20th century. For example, the Hungarian Salamon Beck noted in 1934 that the use of a trademark is not generally obligatory, which allowed to register trademarks only for defensive purposes. However, the Ministry of Trade could prescribe mandatory use of trademarks for certain products, such as straw cutters or sugar. See Vida Sándor, 'A védjegy "tényleges használata" az Európai Bíróság gyakorlatában' [2007] Iparjogvédelmi és Szerzői Jogi Szemle 45., Beck, ibid. 169-172.

53 See Vida Sándor, 'A védjegy "tényleges használata" az Európai Bíróság gyakorlatában' [2011] Iparjogvédelmi és Szerzői Jogi Szemle 91.

54 Article 16. of Trademark Directive and Article 18. of EUTMR.

nature, quality or geographical origin of those goods or services.⁵⁵

- 44 The grounds for invalidity primarily refer to cases where the trademark should not have been registered in the first place. Thus, the absolute and relative grounds for refusal are transformed into absolute and relative grounds for invalidity, which provide the post-grant assessment of these grounds. Article 60 (2) of EUTMR consists of such relative grounds for invalidity which are not mentioned among the grounds for refusal. In this way these grounds can only be invoked within a post-grant invalidity procedure instead of an opposition during the registration procedure. This group includes the right to a name, the right to personal portrayal, copyright, and industrial property rights.
- 45 While trademark protection can be terminated in more ways, the right to a facial image is an inalienable right of the individual, provided ex lege by the law; consequently, it cannot be terminated. As long as the person is alive, they are entitled to the right to a facial image, and nobody can claim the invalidity or revocation of such right. This is a considerable advantage in defense of such rights.

XII. Costs

- 46 Costs are a relevant aspect of acquiring exclusive rights. As trademarks are registered by the competent authorities, an application fee is paid for the procedure. For a European Union trademark, the lowest application fee is 850 EUR which covers one class, according to the Nice classification. The same fee be paid at the time of renewal. By and large, this is a relatively low price for an exclusive right in the entire territory of the European Union, especially in comparison with national application fees in European countries. Furthermore, it is recommended to give mandate to an attorney-at-law, especially in cases where the possibility of refusal may be high. Obviously, this entails higher costs. In contrast, personality rights are free by their nature, and are granted by law without any procedure that may involve payment. The costs of law enforcement have many variables, but it cannot be assumed that there would be significant additional costs on either side.

D. CONCLUSION

- 47 In the previous chapter, trademark protection and the right to facial image were critically compared according to twelve different aspects in order to

discover whether it is worthwhile to file trademark applications for human faces or not. The unlawful use of faces can be prohibited in both ways; however, the most important strategic question is whether the right to facial image provides sufficient protection and enforcement options, or should it be supplemented by trademark?

- 48 The following table summarizes the results of the comparison. A (+) mark indicates a considerable advantage, and (++) indicates an enormous advantage for the corresponding protection. If there is a (+) mark in both columns, it means that there is no significant difference in the examined element. It should be emphasized once more that the right to facial image is governed by national laws, hence the analysis may lead to different results in different countries based on the same evaluation criteria.

Aspects of comparison	EU Trademark	Right to facial image
Function		+
Scope of protection		+
Territoriality	+	
Temporal validity	+	
Conditions of protection		++
Content of protection		+
Limitations and exceptions	+	+
Transferability	++	
Enforcement	+	
Requirement of use		+
Termination		++
Costs		+
Total	6 +	10 +

2. Table Summarizing table of comparison. Compiled by the author.

- 49 Each type of protection has advantages and disadvantages. As can be seen in the comparison results more benefits can be identified for the right to facial image, outweighing the drawbacks, as opposed to trademark protection for portrait photographs. If the given individual has to choose between trademark and personality right to protect their image, the right to facial image seems an adequate solution. Trademark protection for faces is not essential; however, it may be complementary and the owner may benefit from the advantages of trademark protection. Primarily the economic flexibilities of licensing and transferring could be tempting, and the unlimited number of renewals could support business purposes after the death of an individual. Further study will examine how specific trademark law rules can be applied for portrait photos.

⁵⁵ Article 58. of EUTMR.

Annex: List of selected EU portrait trademarks & trademark applications

Male	Female	Children			
000554428	18640603	005305032	018585938	018935420	
000753483	W01087379	013112404	018585925		
000887190	W00900614	013960216	018585913		
001034032	002112738	015726491	018585918		
W01277883	003803591		018585895		
001257328	003930104		018585908		
001332659	004079851		018585924		
001643675	005035548		018585922		
002550036	009013558		018585910		
009086364	009213687		018585899		
010004901	010245231		018585906		
010004919	012695565		018603544		
010004927	014679351		018603548		
010004935	014657449		018603551		
010004943	016503492		018603559		
010004951	017358458		018603554		
011118767	017355066		018603569		
011775335	017393125		018603571		
012225793	017901626		018603556		
014711907	017903677 ²				
014908602	017899480				
014908628	017953534				
014908677	017958820				
015165558	017987149				
015165434	018101943				
018100216	018098887				
018100202	018192360				
018277607	018318511				
018364862	018364871				
018406449	018452841				
018406450	018585935				
018594683	018585916				
018585960	018585956				
018585968	018603131				
018585966	018603550				
018585958	018603564				
018585967	018603546				
018585955	018603561				
018585944	018603567				
018585947	018603563				
018585965	018603568				
018585934	018608409				
018585940	018864324				
018585953	018935347				
018585951	018935419				
018585942	018935414				
018585937	018935324				
018585929	018935418				

