

An Evaluation of the EU Regulatory Framework for Hosting Information Society Service Providers' liability for Copyright and Trade Mark Infringements: Criticisms, Challenges and Recommendations

PhD in Law

School of Law

Zoi Krokida

January 2020

Contents

Abstract	ix
Acknowledgements.....	xi
Chapter 1: Introduction	1
I. Background	1
II. The need for this thesis	6
A. Article 14 of the E-Commerce Directive 2000/31/EC (ECD) adopts an outdated approach with regard to Hosting Information Society Service Providers' (hosting ISSPs) liability	6
B. Article 17 of the Copyright in the Digital Single Market Directive 2019/790 (DSMD): a controversial approach with regard to Online Content Sharing Service Providers' (OCSSPs) liability and a problematic intersection with Article 14 of the E-Commerce Directive (ECD)	7
C. Overview of academic scholarship: lack of scholarly contributions that discuss the creation of a responsibility framework for Hosting Information Society Service Providers (hosting ISSPs) based on a co-regulatory approach	8
III. Research Question and aims	12
IV. Scope of the thesis	14
A. Copyright and trade mark infringements	14
B. Hosting Information Society Service Providers (hosting ISSPs) and Online Content Sharing Service Providers (OCSSPs)	17
C. Primary and secondary liability in tort	22
V. Research Methodology	25
VI. Originality of the thesis	27
VII. Structure of the thesis.....	28
Part I: The current EU legislative tools that regulate hosting ISSPs' liability for copyright and trade mark infringements within their networks.....	31

Chapter 2: The Hosting Information Society Service Providers' (hosting ISSPs) liability framework under Article 14 of the E-Commerce Directive (ECD): an outdated approach

33

I.	Introduction	33
II.	Holding hosting ISSPs liable: theoretical and policy considerations	36
A.	Theoretical justifications of imposing a liability framework for hosting ISPPs in the form of secondary liability	36
i.	Moral Theory.....	36
ii.	Utilitarian Theory	40
a.	Gatekeepers as a source of deterrence	41
b.	Gatekeepers as control points that identify the wrongdoings at a reasonable cost.....	43
B.	Policy and practical considerations for imposing a liability framework on hosting ISPPs in the form of secondary liability	45
III.	The concept of secondary liability for copyright and trademark infringements	49
IV.	Hosting ISSPs' liability as a form of secondary liability: Article 14 of the ECD and legal traditions of EU Member States.....	53
A.	Article 14 of the ECD: Concept of hosting ISPPs' liability	53
B.	Hosting ISPPs' liability under the national implementation of Article 14 of the ECD into three selected EU member states: UK, Germany and France	56
i.	UK: E-Commerce Regulations 2002/2013.....	61
ii.	Germany: Telemediengesetz	64
iii.	France: Act on Confidence in Digital Economy	68
C.	Hosting ISPPs' liability under the legal traditions of three EU member states: UK, Germany and France.....	72
i.	UK	72
ii.	Germany	77

iii.	France	85
V.	Conclusion	91
Chapter 3: The regulatory framework of Online Content Sharing Service Providers (OCSSPs) under Article 17 of the Copyright in the Digital Single Market Directive (DSMD): a controversial approach..... 93		
I.	Introduction	93
II.	Historical account of Article 17 of the DSMD	97
A.	EU Commission’s Proposal for the Copyright in the Digital Single Market Directive (DSMD).....	97
B.	European Council’s text for the Copyright in the Digital Single Market Directive (DSMD).....	105
C.	EU Parliament’s compromised text for the Copyright in the Digital Single Market Directive	108
III.	Article 17 of the DSMD: Problematic features	110
A.	The new definition of Online Content-Sharing Service Providers (OCSSPs).....	111
B.	The introduction of primary liability rules.....	114
C.	The possibility for OCSSPs to conclude a license	120
D.	The possibility for OCSSPs to demonstrate the best efforts.....	122
E.	No general monitoring: a void provision	131
F.	Redress mechanisms and out of court mechanisms: non legitimate without safeguards?.....	133
IV.	Problematic intersection between Article 17 of the DSMD and Article 14 of the ECD	135
V.	Conclusion	138
VI.	Concluding remarks for PART I: Critical evaluation of the implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD.....	142
A.	Implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD on hosting ISSPs and OCSSPs.....	142

B.	Implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD on internet users' rights.....	147
C.	Implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD on the rights of right holders	149
Part II:	Recommendations	153
Chapter 4:	Towards a responsibility framework for hosting ISSPs based on co-regulatory approach.....	155
I.	Introduction	155
II.	Normative justifications for establishing a responsibility framework for hosting ISSPs based on co-regulatory approach.....	156
A.	Hosting ISSPs as information gatekeepers	157
B.	Hosting ISSPs as policymakers	158
C.	Hosting ISSPs as enforcers of intellectual property rights online	160
D.	Hosting ISSPs as architects of e-commerce infrastructure.....	163
E.	Hosting ISSPs as inducers of illicit activity online.....	164
III.	Theoretical underpinnings of the responsibility framework for hosting ISSPs: internet co-regulatory theories	166
A.	Reidenberg's Lex Informatica theory	166
B.	Lessig's theory.....	168
IV.	How to construe a responsibility framework based on co-regulation for hosting ISSPs?	170
A.	A duty of care for hosting ISSPs at legislative and policy level	170
B.	Criticism and counter-arguments for imposing a duty of care for hosting ISSPs	173
i.	Duty of care vs notice and take-down mechanism and notice and notice mechanism	173
ii.	From neutral to active hosting ISSPs	175
iii.	Duty of care vs general monitoring: lack of clash	180
C.	How should a proposed duty of care for hosting ISSPs be shaped?	186

i.	A duty of care as a matter of outcome or as a matter of principle	186
ii.	The scope of a duty of care	191
a.	Trends in case law	191
b.	How to prevent the dissemination of unlawful content or counterfeit goods online.....	194
D.	Limitations upon a proposed duty of care.....	199
i.	Hosting ISSPs’ perspective: endorsing a “Good Samaritan clause”	199
ii.	What about internet users’ perspective?	203
V.	Conclusion	204
Chapter 5:	Endorsing a transparency obligation for hosting ISSPs	207
I.	Introduction	207
II.	Current initiatives for a transparency obligation and trends	208
A.	EU initiatives for a transparency obligation.....	209
B.	National initiatives for a transparency obligation.....	211
III.	Normative considerations of a proposed transparency obligation	214
IV.	How should a proposed transparency obligation be shaped?	221
A.	Transparency in algorithmic decision-making process.....	222
B.	Operational transparency.....	232
C.	Transparency reports	236
V.	Conclusion	240
Chapter 6:	Towards a hosting ISSP supervisory authority	243
I.	Introduction	243
II.	Normative considerations for the proposed hosting ISSP supervisory authority	245
III.	Examples of supervisory authorities for copyright and trade mark infringements: not ideal but a good start.....	253

A.	Administrative agency in Greece	253
B.	Administrative agency in Italy.....	255
IV.	Principles of the proposed hosting ISSP supervisory authority	258
A.	Independence	258
B.	Accountability	261
C.	Proportionality	264
D.	Consistency	266
V.	Functions of the proposed hosting ISSP supervisory authority	268
A.	Enforcement duties.....	268
B.	Complaints’ mechanism for internet users and online consumers .	272
C.	Promoting user-consumer awareness.....	279
VI.	Conclusion	283
Chapter 7:	Conclusion.....	285
I.	Introduction	285
II.	Research Findings.....	286
III.	Recommendations	292
IV.	Epilogue	298
A.	Note for Brexit.....	298
B.	Note for the DSMD	298
Appendix	299	
I.	European Commission’s Proposal for a Copyright in the Digital Single Market Directive on the 14 th September 2016	299
II.	EU Council text 25 May 2018	299
III.	EU Parliament text 26 June 2018	302
IV.	EU Parliament text 12 September 2018	304
V.	Compromised Text after the trialogues’ negotiations 20 February 2019 ..	306

VI. Final text of the Copyright in the Digital Single Market Directive as voted by the EU Parliament on the 26 th of March 2019	309
--	-----

Bibliography 313

I. Primary sources.....	313
A. EU Legislation.....	313
B. European Court of Human Rights Case Law	321
C. Court of Justice of the European Union Case Law	321
D. UK Case Law	323
E. Irish Case Law.....	324
F. US Case Law	324
G. Belgian Case Law	324
H. Spanish Case Law	324
I. Italian Case Law.....	325
J. French Case Law	325
K. Swedish Case Law.....	325
L. German Case Law.....	326
M. Greek Case Law	326
II. Secondary sources	327
A. Books and book chapters.....	327
B. Articles in journals and conferences and reports	334
C. Websites and Blogs	356

Abstract

Hosting information society service providers (hosting ISSPs) have facilitated the exchange of content between users and the purchase of goods online, enabling copyright holders and brand owners to attract a greater audience for their works and goods. However, those services have attracted a high number of copyright and trade mark violations.

Seeing their rights to be infringed, copyright holders and brand owners seek redress against hosting ISSPs requesting either monetary damages or injunctive relief. The main legislative tools that regulate hosting ISSPs' liability towards copyright and trade mark infringements that accrue within their networks are the E-Commerce Directive (EC) 2000/31/EC (ECD) and the Copyright in the Digital Single Market Directive (EU) 2019/790 (DSMD). Yet, both legislative tools fail to accommodate the interests of the parties involved. In particular, Article 14 of the ECD addresses the liability of hosting ISSPs for infringements that are committed by their users. However, it provides defences for hosting ISSPs to escape from liability and thus refrains from defining hosting ISSPs' liability. For this reason, the national courts within the EU use their national tortious secondary doctrines in order to ascribe liability to hosting ISSPs for infringements within their networks. Yet, given that secondary liability is not harmonized at European level, secondary tortious law doctrines are heterogenous and therefore fail to offer a uniform and solid response to the hosting ISSPs' liability conundrum. As a corollary, the fundamental rights of intellectual property holders, hosting ISSPs and internet users are subordinated.

On the other hand, Article 17 of DSMD is relatively new but a number of problematic aspects have already been identified. Article 17 of the DSMD addresses the liability of a new type of hosting ISSPs, the online content sharing service providers (OCSSPs). It introduces a primary liability regime which conflicts with the rationale of a secondary liability regime as set forth in Article 14 of the ECD. It endorses a licensing system for the OCSSPs and a notice and stay down mechanism. As corollary, Article 17 of the DSMD might give rise to tantamount concerns with regard to protection of different interests at stake, namely the rights of internet users and hosting ISSPs.

In the midst of the uncertainty that is created by the existing legislative tools that address hosting ISSPs' liability and OCSSPs' liability, this thesis offers an array of novel suggestions

with regard to the EU regulatory framework of hosting ISSPs with regard to copyright and trade mark infringements within their networks. Based on a thorough examination of normative and theoretical considerations along with a bedrock of court rulings and policies across the EU borders, this thesis recommends the ascription of a number of responsibilities to hosting ISSPs through which they should be accountable to a hosting ISSP supervisory authority. The proposed regulatory framework takes into consideration to a great extent the different interests at stake and thus safeguard fundamental rights, as they are explicitly included in the EU Charter of Fundamental Rights, namely the right of hosting ISSPs to operate their business, the right of internet users to freedom of information and expression and the right of intellectual property holders to achieve protection for their rights.

Acknowledgements

First and foremost, I would like to thank my supervisor Professor Stavroula Karapapa. Her guidance and expertise have enabled me to shape the scope of my research while her constructive feedback has given me the opportunity to develop my research skills and overcome any difficulties I faced. I am immensely indebted to her being always there when I needed her and providing me with support in difficult stances of my PhD journey (especially the time when the Copyright in the Digital Single Market Directive has been finalized); encouraging me to continue and complete it. Her academic entity would act as a role model for the academic I would like to turn into.

I would also like to thank my co-supervisor Associate Professor Anne Thies who stepped in the third year of my PhD studies for her insightful comments as well as Professor Alina Tryfonidou who acted as my second supervisor in the first and second year of my PhD studies. Her constructive comments on my drafts were valuable for my research.

Many thanks to Professor Therese Callus and Dr. Andrea Miglionico, who were in my monitoring panel and whose comments have been of ultimate importance for my thesis.

I also like to thank Malcolm Langley who allowed me to use the facilities of the Queen Mary University Archive for IP law during my PhD studies and who ordered all the books that I requested for my PhD thesis.

Further, I would like to express my gratitude to my colleagues in Law School at the University of Reading. In particular, special thanks to Patsy Kirkwood with whom we have started the PhD journey together. Our fruitful conversations in the course of our PhD studies and our research activities (participating to conferences, attending courses at the Graduate School, having coffee at Henley Business School and discussing the progress of our thesis) would be one of the most memorable moments of my PhD studies. Many thanks to Dr. Adnan Farook who always reminded to relax and enjoy the redrafting of my chapters and who always invited to me to watch any new Avengers film with him. Many thanks to Dr. Athanassios Skourtis with whom I had many fruitful discussions about the progress of our research projects and any difficulties we faced.

Last but not least, I would like to thank and dedicate this thesis to my family. To my sister Maria and my brother-in-law Miltos who offered me a shelter in London during the

difficult times of my PhD journey. Their encouragement and support have helped to continue. To my parents, my mother Asimina and my father Theodoros who emotionally and financially supported me from the very beginning of my PhD studies until their completion. Σας ευχαριστώ πολύ!!!!!!!!!!!!!!

Leicester, 3 January 2020

Chapter 1: Introduction

I. Background

Information Society Service Providers (ISSPs) are described as the “backbone of internet infrastructure.”¹ They do not only serve as a communication tool among Internet users, but they also offer a multitude of services.² There are different types of ISSPs such as the internet access ISSPs, cache ISSPs and hosting ISSPs.³ The latter type of ISSPs, namely the hosting ISSPs are relevant for this research. Their services vary from enabling users to exchange videos online to offering goods for sale. The EU Commission Communication entitled “towards a modern, more European copyright framework” remarks that 49% of European citizens have accessed music and films online.⁴ In similar fashion, 88% of the respondents in the public consultation on the future of electronic commerce in the Internal Market have accessed online marketplaces in order to purchase goods.⁵ A study conducted by the Digital News Oxford’s Reuters Institute in 2019 indicates that 52% of the respondents between 25-34 years old reported that Facebook is the main source of information while at the same time 32% of the respondents between 18-24 years old rely on YouTube for their news.⁶ These are examples of services that hosting ISSPs offer to their users, and their popularity has skyrocketed in recent times. As of January 2019, Facebook was considered the most popular online platform.⁷ At the same time, YouTube’s

¹ I. Revolidis, “Internet intermediaries and copyright enforcement in the EU: In search of a balanced approach” in M. Corrales, M. Fenwick and N. Forgo (eds.), *New Technology, Big Data and the Law* (Springer 2017) 224; A Costa Rican judgement considers internet access as fundamental right, see in A. Guadamuz, “Text of the Costa Rican ruling declaring Internet as a fundamental right” (Technollama, 23 April 2012) is available at <<https://www.technollama.co.uk/text-of-the-costa-rican-ruling-declaring-internet-as-a-fundamental-right>> last accessed 16 October 2019; C. Beaumont, “Finland makes broadband a legal right” (The Telegraph, 15 October 2009) is available at <<https://www.telegraph.co.uk/technology/broadband/6337698/Finland-makes-fast-broadband-a-legal-right.html>> last accessed 25 December 2019

² OECD, “The economic and social role of internet intermediaries” (2010) 9 is available at <<https://www.oecd.org/internet/ieconomy/44949023.pdf>> last accessed 25 April 2019.

³ Article 12 of the E-Commerce Directive- mere conduit ISSPs, Article 13 of the E-Commerce Directive- cache ISSPs, Article 14 of the E-Commerce Directive- hosting ISSPs; As per Article 12 of the ECD, mere conduit ISSPs are those whose services “consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.” As per Article 13 of the ECD, cache providers offer “the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request.” Finally, pursuant to Article 14 of the ECD, hosting ISSPs are those ISSPs whose services offer “the storage of information provided by a recipient.”

⁴ EU Commission, “Towards a modern, more European copyright framework” COM (2015) 626 final 2.

⁵ EU Commission, “Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce” (2000) 1.

⁶ Reuters Institute for the Study of Journalism, “Reuters Institute Digital News Report” (2019) 56.

⁷ J. Clement, “Most famous social network sites worldwide as of April 2019, ranked by number of active users (in millions)” (Statista, 27 May 2019) is available at <<https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>> last accessed 3 January 2020.

dominance in respect of younger generations has been confirmed, with 91% of its users being between 19-28 years old.⁸ The main activities for YouTube's users range from having their own channel on YouTube⁹ to sharing music videos Internet.¹⁰ In similar fashion, online market places have given a tremendous boost to the e-commerce services, with companies such as eBay and Amazon being the leaders in the market. The enormous success of online retail services has resulted in Amazon's CEO becoming the richest man worldwide.¹¹

However, whereas hosting ISSPs have offered an array of services to users and enabled right holders to reach a broader audience,¹² their activities seem to attract a large amount of copyright and trade mark infringements. According to the summary responses to the public consultation on the modernization of the enforcement of intellectual property rights, that was launched by the EU Commission in September 2016, the emergence of new hosting ISSPs has led to the increase of online piracy.¹³ Likewise, the Global online piracy study¹⁴ reveals that in 2017 a high percentage of internet users across the EU member states have accessed music via illegal sources, with Spanish internet users being the pioneers- 35% of the Spanish population. At the same time, content owners see their work being circulated without their permission on video exchange platforms and social networks and witness very high annual losses.¹⁵ For instance, at European level, the

⁸ M. Hills, "Survey: YouTube Is America's Most Popular Social Media Platform" (Forbes, 23 March 2018) is available at <<https://www.forbes.com/sites/meganhills1/2018/03/23/social-media-demographics/#59f74a57783a>> last accessed 25 December 2019.

⁹ B. Murphy, "This 6-Year-Old Makes \$11 Million a Year on YouTube. Here's What His Parents Figured Out" (Inc.) is available at <<https://www.inc.com/bill-murphy-jr/this-6-year-old-makes-11-million-a-year-on-youtube-heres-what-his-parents-figured-out.html>> last accessed 9 July 2019.

¹⁰ H. Yu, L. Xie and S. Sanner "The Lifecycle of a Youtube Video: Phases, Content and Popularity" (2015) Proceedings of the Ninth International AAAI Conference on Web and Social Media 533.

¹¹ R. Frank, "Jeff Bezos is now the richest man in modern history" (cnbc, 16 July 2018) is available at <<https://www.cnbc.com/2018/07/16/jeff-bezos-is-now-the-richest-man-in-modern-history.html>> last accessed 26 December 2019.

¹² A. Bridy and D. Keller, "U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry" (31 March 2016) 14-15.

¹³ EU Commission, "Public Consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights: Summary of responses" (2016) 8.

¹⁴ Poort J and Quintais J P, "Global online piracy study" (2018) University of Amsterdam 50, 51.

¹⁵ OECD, "The Economic Impact of Counterfeiting and Piracy" (2008) is available at <<http://www.oecd.org/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm>> last accessed 27 December 2019; UNODC, "The Globalization of Crime: A Transnational Organized Crime Threat Assessment" (2010) is available at <https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment.html/TOCTA_Report_2010_low_res.pdf> last accessed on 27 December 2019; EU Commission Staff Working Paper, "Counterfeit and Piracy Watch List" SWD (2018) 492 final is available at <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf> last accessed 24 December 2019; "YouTube law fight 'threatens net" (bbc news, 27 May 2008) is available at <<http://news.bbc.co.uk/1/hi/technology/7420955.stm>> last accessed 27 December 2019.

average user consumed unlawful content 9.7 times monthly in 2018¹⁶ while in the UK, the creative sector has faced annual losses of 9 billion pounds due to copyright infringements over the Internet.¹⁷

Against this background, feeling the deck to tilt beneath them, content owners and brand owners have turned against hosting ISSPs to seek compensation for the violation of their rights. Instead of turning against primary infringers, they are bringing proceedings against hosting ISSPs.¹⁸ Basing their legal claims on the provisions enshrined in the E-Commerce Directive (ECD),¹⁹ they are either asking for monetary or injunctive relief against hosting ISSPs.

However, the existing legal framework under the ECD that regulates hosting ISSPs' activities appears to be outdated.²⁰ This is mainly because Article 14 of the ECD refrains from providing a definition of liability of hosting ISSPs and leaves it to the discretion of European national jurisdictions. The result is a patchwork of miscellaneous tort law doctrines that either impose secondary liability rules to hosting ISSPs or are difficult to apply within the online context. As a corollary, the rights of intellectual property holders might not be safeguarded while the right of hosting ISSPs to conduct business as per Article 16 of the EU Charter of Fundamental Rights might be restricted.²¹

¹⁶ European Intellectual Property Office, "Online copyright infringement in the European Union: music, films and TV (2017-2018), trends and drivers (November 2019) 22 is available at <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf> last accessed 30 December 2019

¹⁷ Intellectual Property Office, "IP Crime and Enforcement Report 2018-2019" (2019) 54 is available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/842351/IP-Crime-Report-2019.pdf> last accessed 30 December; Oxford Economics, "The economic impact of the UK film industry" (June 2010) is available at <<https://www.bfi.org.uk/sites/bfi.org.uk/files/downloads/economic-impact-of-the-uk-film-industry-2010-06.pdf>> last accessed 27 December 2019; Due to the expeditious increase of intellectual property infringements online, China has established specific online courts that deal with online disputes, see White Paper, "Chinese courts and internet judiciary" (2019) 66 is available at <http://wlf.court.gov.cn/upload/file/2019/12/03/11/40/20191203114024_87277.pdf> last accessed 27 December 2019.

¹⁸ B. Kleinschmidt, "An International Comparison of ISP's Liabilities for Unlawful Third-Party Content" (2010) 18 International Journal of Law and Information Technology 332; C. Waelde and L. Edwards, "Online Intermediaries and Liability for Copyright Infringement" (WIPO Workshop Keynote Paper, Geneva 2005) 3; J.L. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) 107.

¹⁹ Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] O.J. L 178.

²⁰ As I critically examine in chapter 2 of this thesis.

²¹ Analysis of the regulatory framework of hosting ISSPs under the ECD in chapter 2.

This outdated framework has been aggravated by the introduction of the Copyright in the Digital Single Market Directive²² (DSMD) which is in force in parallel with the ECD. While the DSMD has not been tested yet, since it was only finalized on the 17th of April 2019 and thus relatively new, there appear to be several problematic issues to be addressed.²³ After two years of intensive negotiations, this much anticipated directive provides a definition of the liability of hosting ISSPs but marks a seismic shift with regard to the kind of liability that is ascribed to hosting ISSPs. Refraining from the secondary liability regime that exists under the ECD, the DSMD endorses a primary liability regime for hosting ISSPs. This means that when an infringement takes place within the online network, the hosting ISSP is liable for the infringement. Although this understanding might offer a higher degree of protection for the rights of intellectual property holders, it might have a detrimental effect for the rights of hosting ISSPs and internet users.

The ascription of primary liability rules to a hosting ISSP under Article 17 of the DSMD establishes a new era of liability regime for those hosting ISSPs whose services aim at “enabling users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit from that activity.”²⁴ This is because the introduction of primary liability to ISSPs seems to go against the main rationale of tortious secondary liability rules that were imposed by European policymakers in the ECD back in 2000. According to the secondary liability regime, hosting ISSPs can be held liable if they have knowledge of the infringing content and they did not remove it upon being notified by the intellectual property holders. So, it is this defence of knowledge that has been widely used by hosting ISSPs to be exonerated from liability and which has allowed them to continue without disrupting the operation of their business model.

By contrast to secondary liability rules, primary liability rules do not require the element of knowledge. For instance, without the defence of knowledge, new players would be hesitant to enter the Digital Single Market, and existing hosting ISSPs would be forced to develop or license highly advanced technology in order to prevent the emergence of online infringements in the first place. This might pose serious threats on innovation and competitiveness within the Digital Single Market and be in conflict with the main aims of

²² The Copyright in the Digital Single Market Directive (hereinafter DSMD).

²³ As I critically examine in chapter 3 of this thesis.

²⁴ Recital 62 of 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 O.J.L 130.

the Digital Single Market Strategy that outlined the need to “maximize the growth potential of the Digital Economy.”²⁵

What is more, the imposition of primary liability rules to hosting ISSPs might have a side effect on internet users’ rights. Under the threat of being held primarily liable for the infringements of their users, hosting ISSPs might ‘over-remove’ content without investigating further its illegality. This understanding has been exemplified in a number of studies that demonstrate that hosting ISSPs are in favour of taking down content without a detailed examination of the notifications that they receive.²⁶ However, as these studies reveal, the content that has been removed by hosting ISSPs upon notice is not always unlawful. For instance, it might be a parody or a work that belongs to public domain. In this way, the removal of legitimate content by hosting ISSPs might amount to users’ speech censorship and be in violation with Article 11 of the EU Charter of Fundamental Rights that guarantees the freedom of expression of individuals.

On the basis of the above, it appears that the existing legal framework for ISSPs’ activities under Article 14 of the ECD and Article 17 of the DSMD either does not safeguard right holders, users and ISSPs or favours right holders’ rights, and undermining users and hosting ISSPs’ interests. For this reason, it is evident that a more robust legal framework is needed.

In this light, this chapter sets out the background of this thesis, the importance of this thesis along with an overview of the existing academic scholarship. Further, the research question, the aims, the scope of this research as well as the appropriate research methodology in order to answer the research question will be discussed. Finally, this chapter outlines the originality of this thesis and presents an outline of the chapters.

²⁵ EU Commission, “A Digital Single Market Strategy for Europe” COM (2015) 192 final 13-14.

²⁶ Lecture by Sjoera Nas, Bits of Freedom, “The Multatuli Project ISP Notice & take down” (2004) is available at <<https://www-old.bof.nl/docs/researchpaperSANE.pdf>> last accessed 1 March 2019; C. Ahlert, C. Marsden and C. Yung, “How ‘Liberty’ Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation” (2014) is available at <<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>> last accessed 1 March 2019; D Kiat Boon Seng, “The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices” (2014) 18 Va. J. L. & Tech. 369 37; D. Keller, “DMCA classic, DMCA turbo: major new empirical research on notice and takedown operations” (The Center for Internet and Society, 20 April 2016) is available at <<http://cyberlaw.stanford.edu/blog/2016/04/dmca-classic-dmca-turbo-major-new-empirical-research-notice-and-takedown-operations>> last accessed on 16 March 2019.

II. The need for this thesis

A. *Article 14 of the E-Commerce Directive 2000/31/EC (ECD) adopts an outdated approach with regard to Hosting Information Society Service Providers' (hosting ISSPs) liability*

Firstly, the need for this project is warranted in light of the outdated legal framework for hosting ISSPs under the ECD. This outdated framework, as my findings indicate in chapter 2, does not offer adequate protection for intellectual property holders' rights while at the same time subordinates internet users' interests and hosting ISSPs' business operations.

Article 14 of the ECD states that a hosting ISSP can escape from liability if “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 legal systems, of requiring the service provider to terminate or the information.” However, it does not define hosting ISSPs' liability. As a result, national courts turn to their national tortious legal doctrines in order to ascribe liability to hosting ISSPs. Given that secondary liability is not harmonized at EU level, heterogenous tortious secondary liability doctrines have been applied by national courts with conflicting outcomes. Further, the disappointment towards the regulatory framework for hosting ISSPs' activities as enshrined in Article 14 of the ECD is mirrored in a handful of policy documents at European level. In these policy documents, different stakeholders, such as right holders, civil society organizations and online platforms associations, have expressed their dissatisfaction. More specifically, pursuant to the public consultation on the role of hosting ISSPs in 2015,²⁷ 49.50% of 599 respondents admitted that the “liability regime introduced in Section IV of the ECD (Articles 12-15) has proven not fit for purpose or has negatively affected market level playing field.”²⁸ At the same time, in a public consultation on the ECD in 2011,²⁹

²⁷ EU Commission, “Study on the role of intermediaries - Summary of the public consultation” (25 May 2016) is available at <<https://ec.europa.eu/digital-single-market/en/news/study-role-intermediaries-summary-public-consultation>> last accessed 27 December 2019.

²⁸ M. Husovec and R. Leenes, “Study on the role of online intermediaries Summary of the public consultation, a study prepared for the European Commission DG Communications Networks, Content & Technology” (2016) is available at <<https://ec.europa.eu/digital-single-market/en/news/study-role-intermediaries-summary-public-consultation>> last accessed 27 December 2019.

²⁹ EU Commission Staff Working Paper, “Online Services, Including E-Commerce, in the Single Market” SEC (2011) 1641 final 33-34. <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011SC1641&from=EN>> last accessed 27 December 2019; EU

stakeholders criticized the current legal framework under the ECD. This is mainly due to the lack of guidance on the concept of 'knowledge' and the term 'expeditious', which are included in Article 14 of the ECD that dictates that a hosting ISSP that provides hosting services to its users can be exonerated from liability if it does not have any knowledge of the allegedly infringing material and if upon receiving notification of the infringing material, the hosting ISSP expeditiously removes the material.

B. Article 17 of the Copyright in the Digital Single Market Directive 2019/790 (DSMD): a controversial approach with regard to Online Content Sharing Service Providers' (OCSSPs) liability and a problematic intersection with Article 14 of the E-Commerce Directive (ECD)

The second need for this project is also justified in view of the controversial legislative attempts to amend and reconstruct the existing legal framework for hosting ISSPs at European level with the introduction of the DSMD on the 17th of April 2019. The DSMD was endorsed in the aftermath of the impact assessment on the enforcement of copyright rules in the digital ecosystem, where rights holders expressed concerns about fair remuneration and control of the circulation of their works.³⁰ Although the DSMD has not yet been tested, a cluster of problematic issues have already been identified.³¹ To name a few, Article 17 of the DSMD, which is relevant to this research, addresses the liability of a new type of hosting ISSPs, the online content sharing service providers (OCSSPs). It

Commission, "Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce: Summary of response" (2010) is available at <http://ec.europa.eu/information_society/newsroom/image/document/2017-4/consultation_summary_report_en_2010_42070.pdf> last accessed 27 December 2019.

³⁰ EU Commission Staff Working document, "Executive summary of the impact assessment on the modernisation of EU copyright rules" SWD/2016/0302 final.

³¹ J. Quintais and others, "Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics" (November 2019); M. Husovec and J. Quintais, "How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms" (1 October 2019) is available <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011&download=yes> last accessed 16 October 2019; G. Frosio and S. Mendis, "Monitoring and filtering: European reform or Global trend?" (2019) Center for International Intellectual Property Studies Research Paper 21; C. Angelopoulos and J. Quintais, "Fixing copyright reform: a better solution to online infringement" (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 153; M. Vermeulen, "Online content: to regulate or not to regulate- is that the question?" (2019) Association for progressive communications 10-11; Communia, "Guidelines for the implementation of Article 17 of the DSMD" is available at <<https://www.notion.so/Article-17-Use-of-copyrighted-content-by-online-platforms-8e9ab9aaa4ce42c2a6f35cb7415b8b83>> last accessed 24 December 2019; K. Grisse, "After the storm—examining the final version of Article 17 of the new Directive (EU) 2019/790" (2019) 14 Journal of Intellectual Property Law & Practice 887.

introduces a primary liability regime which conflicts with the rationale of a secondary liability regime as set forth in Article 14 of the ECD. It endorses a licensing system for the OCSSPs and a notice and stay down mechanism. As corollary, Article 17 of the DSMD might give rise to tantamount concerns with regard to protection of different interests at stake, namely the rights of intellectual property holders, internet users and hosting ISSPs. For this reason, this research will engage in a comprehensive analysis of the implications of the DSMD for OCSSPs', intellectual property holders' and internet users' rights. This analysis forms chapter 3 of this thesis.

What is more, the DSMD does not only entail problematic features itself. Rather, it also presents a problematic intersection with the ECD since both legislative tools exist in parallel. As discussed in chapter 3, Article 17 of the DSMD is a *lex specialis* to Article 14 of the ECD. While Article 14 of the ECD endorses a secondary liability regime, Article 17 of the DSMD introduces a primary liability framework for OCSSPs. This dual liability regime might trigger a fragmented framework of copyright law, split the existing case law at the European level, impede innovation within the Digital Single Market as well as force the creation of a monopolistic market within the OCSSPs. A detailed analysis of this problematic intersection is presented in chapter 3 of this thesis.

C. Overview of academic scholarship: lack of scholarly contributions that discuss the creation of a responsibility framework for Hosting Information Society Service Providers (hosting ISSPs) based on a co-regulatory approach

The third need for this thesis is justified in light of the existing academic scholarship for the EU regulatory framework of ISSPs. This is because existing contributions mainly concentrate on the harmonisation of tortious secondary liability rules, the appropriateness of issuing injunctions against non-liable hosting ISSPs, how to preserve the right of hosting ISSPs to operate business under the ECD regime as well as who should be liable for the infringing material that is circulated within the online platforms, and the approaches and challenges in attributing liability rules to hosting ISSPs for third party content.

Examples of these scholarly contributions include Angelopoulos' work on *European intermediary liability in copyright: a tort-based analysis* has explored the harmonisation

of liability of ISSPs (mere conduit, cache and hosting) through the lens of tort law.³² Through a comparative approach, she manages to identify similarities and discrepancies among three selected jurisdictions and to recommend how ISSPs' liability can be harmonized at European level. However, the work is limited to copyright infringements and does not discuss the liability of ISSPs with regard to trade mark infringements online.

Another scholar that explores the conundrum of ISSPs' liability is Riordan's work entitled *The liability of internet intermediaries*.³³ This book informs this thesis since it covers the liability of ISSPs (mere conduit, cache and hosting) through a whole spectrum of violations in copyright, trademark, defamation, confidentiality and privacy, as well as data protection law.³⁴ However, it mainly addresses thorny issues of ISSPs' liability in the UK jurisdiction and covers a broad range of violations from different fields of law. Henceforth, a more detailed analysis of ISSPs' liability framework from a European perspective, as well as a focus on copyright and trade mark violations, is required.

Marsoof's work entitled *Internet Intermediaries and trade mark rights* discusses the regulatory framework of mere conduit and hosting ISSPs with regard to trade mark infringements.³⁵ Although the author mainly adopts a UK perspective, he also looks at cases of hosting ISSPs' liability at the European level. Yet, those cases of hosting ISSPs at the European level are discussed very briefly.

Another book that discusses the regulatory framework of hosting ISSPs is entitled *Regulating Hosting ISPs' responsibilities for copyright infringement: The freedom to operate in the US, EU and China*, by Wang. The book offers a comparative analysis of the three main legal jurisdictions, namely United States, Europe and China, which includes a critical evaluation of the safe harbour provisions as enshrined in the relevant legal instruments, the notice and take down mechanisms, and the requirements for ordering identity disclosures.³⁶ His research question seeks how to construe the responsibilities of hosting ISSPs with the aim to give to them "their maximum freedom to operate." However, this book critically evaluates the regulatory framework of hosting ISSPs only

³² C. Angelopoulos, *European intermediary liability in copyright: a tort-based analysis* (Kluwer Law International 2016) 13.

³³ J. Riordan, *The liability of internet intermediaries* (Oxford University Press 2016) 2.

³⁴ *Ibid.*

³⁵ A. Marsoof, *Internet intermediaries and trade mark rights* (Routledge 2019) 1.

³⁶ J. Wang, *Regulating Hosting ISPs' responsibilities for copyright infringement: The freedom to operate in the US, EU and China* (Springer 2018) 12.

from the hosting ISSPs' perspective without taking into consideration the interests of Intellectual property holders and internet users. For this reason, the recommended solutions lean in favour of hosting ISSPs and avoid looking at the bigger picture, which is to accommodate the interests of the other parties at stake.

Moreover, another book that is relevant to this thesis is *Secondary Liability of Internet service providers* edited by Dinwoodie.³⁷ This book adopts a comparative approach, including a number of scholarly contributions that elaborate on the problematic issues of the regulatory framework of ISSPs including hosting ISSPs at national and transnational level. For this reason, it is extremely useful for my research.

Furthermore, another book that is relevant for my research is Husovec's book titled *Injunctions Against Intermediaries in the European Union: Accountable but not liable*. This book focuses on the appropriateness of issuing injunctions against non-liable ISSPs or, as the author refers to them, accountable ISSPs. As he notes, such injunctions "against innocent third parties want to achieve better enforcement by seeking a help of intermediaries who can do more, but do not have to, as they did all the law required from them in order to avoid liability in tort."³⁸ In this sense, he explores the filtering or blocking-based obligations through injunctions against accountable ISSPs, defining the conditions to issue such injunctions, their legal basis and their scope, along with any limitations. Finally, he explores deeper into common and civil law jurisdictions in order to identify the theoretical roots upon which such injunctions might rely. However, this book focuses on cases that deal with injunctive relief redress and does not look at pecuniary claims of intellectual property holders against ISSPs.

It is important to mention that the above-mentioned academic contributions deal with the regulatory framework of hosting ISSPs under the ECD and its national implementation in selected national jurisdictions. With regard to the new developments in terms of the legislative regime of hosting ISSPs for copyright infringements, only three main academic contributions look at the DSMD, which was finalized on the 17th of April 2019.

³⁷ G. Dinwoodie (ed.), *Secondary liability of internet service providers* (Springer 2017) 1.

³⁸ M. Husovec, *Injunctions Against Intermediaries in the European Union: Accountable but not liable* (Cambridge University Press 2017) 12.

The first contribution is the book entitled *Intermediary liability and freedom of expression in the EU: from concepts to safeguards* by Kuczerawy.³⁹ This book offers a comprehensive analysis of the regulatory framework of hosting ISSPs under the ECD but provides a limited analysis of the new legislative reform on copyright law in the Digital Single Market. It only touches upon the Proposal of the EU Commission for the DSMD as it was introduced in September 2016. Therefore, a critical evaluation of the final draft of the DSMD is not addressed.

The second scholarly contribution is Berrak's thesis titled "Reconsidering the law of contributory liability on the internet: analysis on the trade mark issues, challenges and the remedy."⁴⁰ This thesis discusses the regulatory framework of ISSPs including hosting ISSPs for trade mark violations that take place within their networks, including an assessment of the new legislative reform with the DSMD. However, given that the thesis reflects the law as of 12 September 2018, it includes the compromise drafts on the DSMD of the EU Council and EU Parliament. Therefore, the evaluation of the implications of the final draft of the DSMD, as voted by the EU Parliament in March 2019, is not discussed.

The third contribution is the book entitled *Internet Intermediaries and Copyright Law: EU and US perspectives* by Kulk.⁴¹ This book addresses the liability of a range of ISSPs from a comparative angle, namely from the EU and US perspective. Although it discusses the tricky provisions of the final draft of the DSMD,⁴² the author refrains from examining the problematic intersection between Article 17 of the DSMD and Article 14 of the ECD and therefore its potential implications for the parties at stake.

Therefore, it appears that the need for this project is warranted. The outdated legal framework under Article 14 of the ECD along with the problematic features of Article 17 of the DSMD and the lack of scholarly contributions that thoroughly deal with the new regulatory framework of OCSSPs seem to offer solid justifications in order to undertake this research.

³⁹ A. Kuczerawy, *Intermediary Liability and Freedom of expression in the EU: from Concepts to Safeguards* (Intersentia 2018) 17.

⁴⁰ G. Berrak, "Reconsidering the law of contributory liability on the internet: analysis on the trade mark issues, challenges and the remedy" (Unpublished PhD thesis April 2018) 186.

⁴¹ S. Kulk, *Internet Intermediaries and Copyright Law: EU and US perspective* (Kluwer Law International 2019) 3-4.

⁴² Article 15 of the DSMD- the press publisher's right, Article 17 of the DSMD- liability of OCSSPs.

III. Research Question and aims

In light of the issues discussed in the previous section, this thesis addresses the following question:

How should the EU legal framework of hosting ISSPs' liability be shaped in order to safeguard intellectual property right holders' rights as well as the interests of internet users/ consumers and hosting ISSPs?

This means that the aim of this thesis' is twofold. Firstly, it critically assesses the current legal framework that regulates the activities of hosting ISSPs at a normative level and then suggests an array of recommendations that address how the regulatory framework of hosting ISSPs should be shaped. It is important to mention that the proposed legal framework takes into consideration all the different interests of the parties at stake. On the one hand, the rights of intellectual property owners shall be protected. This understanding has been reinforced in a number of EU legislative tools. Indeed, Article 17 (2) of the EU Charter of Fundamental Rights states that "Intellectual property law shall be protected". Likewise, Article 27 (2) of the Universal Declaration of Human Rights states that "Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author." On the other hand, in *Scarlet v Sabam*, CJEU has concluded that intellectual property rights are not inviolable and therefore their protection of intellectual property rights is not absolute.⁴³ As the CJEU outlined, intellectual property rights shall not be prioritized against other fundamental rights at stake.⁴⁴ Such fundamental rights include the rights of internet users and the rights of ISSPs. Users' rights are safeguarded under Article 11 (1) of EU Charter of Fundamental Rights that states "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers." In similar fashion, Article 19 (2) of the International Covenant on Civil and Political Rights states that "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media

⁴³ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 43.

⁴⁴ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 44.

of his choice.” Hosting ISSPs’ fundamental right to conduct business is protected under Article 16 of the EU Charter of Fundamental Rights which notes that “the freedom to conduct a business in accordance with Community law and national laws and practices is recognised.”

Therefore, an equilibrium between the interests of the parties involved shall be achieved. This equilibrium has been reinforced by a bedrock of case law at European level. As the Court of Justice of the European Union (CJEU) noted in the in *Scarlet v Sabam*, it has been concluded that “national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.”⁴⁵ In addition, in *Promusicae* case, “Member States must [...] take care to rely on an interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order.”⁴⁶

Further, in order to answer the research question, a number of sub-questions are addressed:

- i. How does the current legal framework under the ECD regulate the liability of hosting ISSPs?⁴⁷
- ii. How does the Copyright in the Digital Single Market Directive regulate liability of OCSSPs?⁴⁸
- iii. What is the impact of the current legal framework on internet users’, right holders’ and hosting ISSPs’ rights?⁴⁹
- iv. Would a responsibility framework based on a co-regulatory approach for hosting ISSPs have merits?⁵⁰
- v. What kind of responsibilities should be ascribed to hosting ISSPs?⁵¹

⁴⁵ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 45.

⁴⁶ Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, para. 70.

⁴⁷ This sub-question is addressed in chapter 2.

⁴⁸ OCSSPs are a new sub-type of hosting ISSPs and are enshrined in the DSMD. An analysis of this new type of hosting ISSPs is presented in chapter 3.

⁴⁹ This sub-question is addressed in the Concluding remarks of Part I of this thesis.

⁵⁰ A thorough analysis of the theoretical and normative considerations is presented in chapter 4. In a nutshell, a responsibility framework based on a co-regulatory approach lies on the ascription of a set of responsibilities to hosting ISSPs through which they would be accountable to a hosting ISSP supervisory authority.

⁵¹ This sub-question is discussed in chapters 4 and 5.

- vi. What safeguards should be introduced in order to preserve hosting ISSPs' right to operate their businesses, as well as internet users' right to free speech? ⁵²
- vii. Would the establishment of a hosting ISSP supervisory authority have merits for hosting ISSPs, right holders and internet users? ⁵³

IV. Scope of the thesis

The scope of this thesis addresses copyright and trade mark infringements online, a specific type of information society service providers, namely the hosting ISSP and the different types of liability that hosting ISSPs might be ascribed for copyright and trade mark infringements that accrue within their networks.

A. *Copyright and trade mark infringements*

Although there is a vast array of different kinds of violation in the digital ecosystem, the focus of this thesis is limited to copyright and trade mark violations online. This is because, within the online context, the kinds of intellectual property infringements that mostly occur rest in the field of copyright and trade mark law.⁵⁴ Previous literature has identified that, with digitization and the internet, copyright holders, internet users and hosting ISSPs have entered into the arena of the so-called copyright wars. Copyright has become one of the most affected legal disciplines on the internet, due to the ease and speed through which materials can be circulated online.

This understanding has been exemplified in an increasing litigation as indicated by a bedrock of EU case law that was issued just over the last decade. Representative examples are *the Scarlet v Sabam*,⁵⁵ *Netlog v Sabam*,⁵⁶ *UPC Telekabel*,⁵⁷ *Svensson case*,⁵⁸ *GS Media*⁵⁹ and *Brein v Ziggo*⁶⁰ rulings, to name but a few. All the above cases are about the ascription of liability rules to hosting ISSPs for unauthorized copyright content uploaded by their

⁵² This sub-question is addressed in chapters 4 and 5.

⁵³ This sub-question is discussed in chapter 6.

⁵⁴ A joint project between the European Patent Office and the European Union Intellectual Property Office, "IPR-intensive industries and economic performance in the European Union" (2019) 26.

⁵⁵ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

⁵⁶ Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85.

⁵⁷ Case C-314/12, *UPC Telekabel Wien* (2014) ECLI:EU:C:2014:192.

⁵⁸ Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB* (2014) EU:C:2014:76.

⁵⁹ Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644.

⁶⁰ Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456.

users or for linking to material offered in third party websites without the right holders' permission.

Furthermore, the negative implications of digitization on copyright has been mirrored in several policy documents where intellectual property holders have expressed their disappointment and concerns about the current legal framework, as depicted in the ECD.⁶¹ More specifically, in the public consultation for the modernization of the enforcement of intellectual property rights, almost fifty percent of the respondents outlined that the current legal framework was no longer fit⁶² while the majority of the respondents viewed "commercial scale IPR infringements as a global business."⁶³ Along similar lines, the outcomes of the public consultation on the future of electronic commerce in the Internal Market indicated "the failure to respect copyright and the size of the illegal market."⁶⁴

Finally, the need to examine copyright infringements online is also warranted in light of the controversy that revolved around the DSMD, which was the result of intensive lobbying of publishers and content industries. It took 2 years and 6 months to finalize this controversial legislative instrument, which has generated severe criticism by civil society associations, politicians, internet activists and individuals, and whose implications are yet to be seen since there is a timeframe of two years for its implementation on national member states.⁶⁵ The main aim of the DSMD is to address the value gap between the creators of works and the economic benefits of disseminating content within the networks of information society service providers. The term value gap is understood as the non- fair remuneration of creators from the dissemination of their content in the digital ecosystem.⁶⁶ For instance, a report conducted by the International Federation of the Phonographic Industry outlines that whereas paid-online music platforms return to

⁶¹ See also H. Bosher, *The human element in online infringement* (Routledge 2020) 6 where Boscher notes that "at every advent of a new technology a fear rises in stakeholders that copyright is under threat; copyright law is claimed to be out of date and if immediate action is not taken, copyright will become obsolete."

⁶² EU Commission, "Summary of responses to the public consultation on the role of online intermediaries" (2016) 11.

⁶³ EU Commission, "Public Consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights: Summary of responses" (2016) 6.

⁶⁴ EU Commission, "Summary of the results of the public consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce" (2016) 6.

⁶⁵ EU member states must implement the DSMD into their national laws by 7 June 2021.

⁶⁶ See Explanatory Memorandum to the DSM Proposal "It is therefore necessary to guarantee that authors and rightholders receive a fair share of the value that is generated by the use of their works and other subject-matter."; see also N. Elkin-Koren, Y. Nahmias and M. Perel, "Is It Time to Abolish Safe Harbor? When Rhetoric Clouds Policy Goals" (2020) 31 *Stanford Law & Policy Review*, Forthcoming 24.

the creators per user 20 USD, the return to authors per users from free online music platforms is limited to one dollar.⁶⁷ However, as many commentators argue, it seems that the DSMD might override this aim and may pose serious risks for the interests of OCSSPs and internet users.⁶⁸

Apart from copyright law, trade mark law has been affected by the rapid increase of e-commerce services. There are emergent trends indicating that e-commerce has enabled infringements of registered trade marks, either through the unauthorized sale of counterfeit goods or via the use of unlicensed Adwords. Indeed, a bedrock of court rulings indicate the high level of online piracy. Consider, for instance, the unauthorized sale of fake products. Examples at European level, such as landmark decisions in the cases *L’Oreal v eBay*⁶⁹ and *Google Adwords*⁷⁰ have placed trade mark infringements at the forefront. At the same time, court rulings that impose liability are not rare at all. Indeed, national courts in France, Germany, Greece and Spain have attempted to impose liability on hosting ISSPs for trade mark violations within their networks.⁷¹

What is more, the negative implications of e-commerce services for brand owners have been illustrated in the joint study of OECD and EUIPO.⁷² More specifically, this study demonstrated that in 2016 counterfeit goods in international trade reached up to €460 billion and the imports of fake products in Europe represent 6.8% of all European imports.⁷³ Along similar lines, the EU Commission’s public consultation on the modernization of intellectual property rights’ enforcement rules concluded that “more than three quarters of respondents experiences an increasing intellectual property infringements over the last 10 years” while at the same time it has been noted that

⁶⁷ IFPI, “Global Music Report 2018: annual state of the industry” (2018) is available at <<https://www.ifpi.org/downloads/GMR2018.pdf>> last accessed 16 October 2019.

⁶⁸ G. Frosio and S. Mendis, “Monitoring and filtering: European reform or Global trend?” (2019) Center for International Intellectual Property Studies Research Paper 21.

⁶⁹ Case C-324/09, *L’Oreal SA V eBay Int’l AG* [2011] E.C.R. I-6011.

⁷⁰ Case C- 236/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (2010) ECR I-02417.

⁷¹ T. Verbiest, G. Spindler, G. Riccio and A. Van der Perre, “Study on the Liability of Internet Intermediaries” (MARKT/2006/09/E).

⁷² EU Commission, “Trends in trade in counterfeit and pirated goods: the updated picture” (19 March 2019) is available at <https://ec.europa.eu/growth/content/trends-trade-counterfeit-and-pirated-goods-updated-picture_en> last accessed 27 December 2019.

⁷³ OECD and EUIPO study, “Trends in Trade in Counterfeit and Pirated Goods” (2019) is available at <https://read.oecd-ilibrary.org/trade/trends-in-trade-in-counterfeit-and-pirated-goods_g2g9f533-en#page13> last accessed 27 December 2019.

“fighting IPR infringements in the online environment was becoming a regulatory and enforcement challenge.”⁷⁴

However, the policy initiatives to curb online piracy are limited to a certain extent. For instance, in September 2016 the EU Commission announced the ‘follow the money’ approach that aimed at curbing the circulation of fake goods online by blocking the revenue streams to websites that host such material.⁷⁵ However, since the date of writing this thesis, further guidance on the consistent implementation of this policy at European level has not been published. Likewise, a certain number of luxury brands have signed with specific online marketplaces a Memorandum of Understanding for counterfeit goods.⁷⁶ As per this Memorandum, online marketplaces are expected to verify the identity of the sellers that display their goods online as well as undertake preventive measures when right holders notify them about trademark infringements within their platforms. Yet, although this Memorandum might be a good start, its impact is limited since it only involves a certain number of brand owners and online marketplaces.

In light of the above developments, the legal problem addressed in this thesis focuses mainly on copyright and trade mark infringements taking place in the online environment. Given that this thesis examines the regulatory framework of hosting ISSPs for copyright and trade mark infringements within their networks, the following section presents the specific type of hosting ISSPs which this thesis assesses, in the context of copyright and trade mark violations, along with the reasons that justify this choice.

B. Hosting Information Society Service Providers (hosting ISSPs) and Online Content Sharing Service Providers (OCSSPs)

In the online world, ISSPs are those entities that “bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index

⁷⁴ EU Commission, “Public Consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights: Summary of responses” (2016) 8.

⁷⁵ EU Commission, “Commission one step closer to restricting revenues of websites that breach intellectual property rights” (25 October 2016) is available at <https://ec.europa.eu/growth/content/commission-one-step-closer-restricting-revenues-websites-breach-intellectual-property-1_en> last accessed 27 December 2019.

⁷⁶ EU Commission staff working document, “Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit goods via the internet” SWD(2017) 430 final 6; EU Commission, “Memorandum of Understanding on the sale of counterfeit goods via the internet” is available at <https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en> last accessed 24 April 2019.

content, products and services originated by third parties on the Internet or provide Internet-based services to third parties.”⁷⁷

Authoritative legal definitions of Information Society Service Providers (ISSPs) are featured in the main legal instruments that regulate ISSPs, namely the ECD and DSMD. The ECD offers a definition of ISSPs in Recital 17 where it notes that information society providers are those providers whose function “covers any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service.”⁷⁸ Different types of ISSPs are set out in Article 12 of the ECD, Article 13 of the ECD and Article 14 of the ECD. As per Article 12 of the ECD, mere conduit ISSPs are those whose services “consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.” As per Article 13 of the ECD, cache providers offer “the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information’s onward transmission to other recipients of the service upon their request.” Finally, pursuant to Article 14 of the ECD, hosting ISSPs are those ISSPs whose services offer “the storage of information provided by a recipient.”

Apart from the ECD, the DSMD adds- what seems to be- a subcategory to those information society service providers that offer hosting services to internet users ⁷⁹ and thus endorses a new authoritative legal definition in Article 17 of the DSMD, namely the definition of an online content sharing service provider. Yet, an explanation of this new authoritative legal definition is found in Article 2 (6) of the DSMD which notes that an online content sharing service provider is “a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes.”⁸⁰ This means that online content sharing providers are those providers that offer services such as online

⁷⁷ OECD, “The economic and social role of internet intermediaries” (2010) 9 is available at < <https://www.oecd.org/internet/ieconomy/44949023.pdf>> last accessed 27 December 2019.

⁷⁸ Council 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 OJ L 178

⁷⁹ Council Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130.

⁸⁰ Ibid.

audio or video streaming. Representative examples are Facebook, Dailymotion, YouTube and Instagram. By contrast, online marketplaces, cloud to cloud business and not for profit online encyclopaedias do not fall into the scope of Article 17 of the DSMD, as explicitly mentioned in Article 2(6) of the DSMD. Representative examples are eBay, Dropbox and Wikipedia. Therefore, these providers' activities are regulated by Article 14 of the ECD, which addresses the liability of hosting ISSPs.⁸¹

In light of the above, I follow the terms that the main legal instruments include, namely the ECD and the DSMD. More specifically, the term hosting information society service provider (hosting ISSP) as interpreted by the ECD is used throughout this thesis. Moreover, given that this thesis also deals with copyright infringements, I also use the term online content sharing provider pursuant to the new legislative framework introduced by the DSMD in April 2019, since it addresses those information society service providers that provide access to a large amount of copyright-protected content and deal with copyright infringements online.

Furthermore, it is important to mention the reasons for which the scope of this thesis is limited to two types of ISSPs, namely hosting ISSPs and their new subcategory, online-content sharing service providers.⁸²

I have chosen to examine the legislative framework of hosting ISSPs under Article 14 of the ECD and OCSSPs under Article 17 of the DSMD due to the proximity of their role to intellectual property infringements. Firstly, with the services they provide to their internet users, they facilitate their users to commit wrongdoings within their networks. For instance, the business model of a video-music platform, which falls under the definition of OCSSPs, concerns the upload of music videos, among which some may be uploaded without right holders' authorisation and be in breach of copyright law. At the same time, online marketplaces, which falls under the definition of hosting ISSPs, may not merely facilitate the use of electronic content but also the sale of goods bearing intellectual property rights without the consent of the relevant right holders. Online marketplaces that enable their users to sell products may be at the risk of liability when users advertise products that may be counterfeit or in breach of trade mark law. Secondly, they can control the material that is disseminated throughout their networks. This understanding

⁸¹ See also G. Frosio and S. Mendis, "Monitoring and filtering: European reform or Global trend?" (2019) Center for International Intellectual Property Studies Research Paper 21.

⁸² Hereinafter OCSSPs.

is reinforced in YouTube's Content ID system.⁸³ Content ID system is a database that comprises files of works that have been sent by their authors. Once an infringing video is uploaded by a user on YouTube's platform, it is automatically removed by Content ID system.

What is more, another reason that justifies the focus of this thesis on hosting ISSPs and OCSSPs is the risk of over-enforcement of intellectual property rights and their negative implications for users' legitimate speech. Indeed, specialists in the field have frequently warned that the imposition of liability rules to hosting ISSPs might interfere with freedom of expression of users.⁸⁴ This is because hosting ISSPs and OCSSPs may be subject to economic risks, by being held liable for intellectual property violations within their networks and thus they are prone to over-remove content online.

This focus on hosting ISSPs and OCSSPs is also motivated by the lack of transparency within their operational business models. Although they have been entrusted with removing unlawful content online and counterfeit goods, it has been argued that there is a lack of transparency with regard to the processes they tend to follow. For instance, hosting ISSPs and OCSSPs tend to use automated decision-making processes with regard to the removal of content online⁸⁵ without providing any safeguard for users whose material has been erroneously removed. Indeed, civil society organizations have heavily criticised the removal of content without any justification and any opportunity for users to appeal the decision for removal.⁸⁶ In the absence of any legal remedy for users, the principles of due process may be threatened and therefore users' right for equal weapons, as explicitly protected in Article 47 of the EU Charter of Fundamental Rights,⁸⁷ may be violated.

⁸³ T. Margoni and M. Perry, "Online intermediary liability and privatised enforcement: the Content ID case" (2016) *The Tenth International Conference on Digital Society and eGovernments* 36.

⁸⁴ M. Husovec, "Why there is no due process online?" (Balkin.com, 7 June 2019) is available at <<https://balkin.blogspot.com/2019/06/why-there-is-no-due-process-online.html>> last accessed 27 December 2019; G. De Gregorio, "From Constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society" (2018) *11 European Journal of Legal Studies* 82; D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 85-87.

⁸⁵ Negative implications of automated decision-making process are presented in chapter 5!

⁸⁶ European Digital Rights (EDRI), "The Slide from "Self-Regulation" to "Corporate Censorship" is available at <https://edri.org/files/EDRI_selfreg_final_20110124> last accessed 27 December 2019.

⁸⁷ Article 47 of the EU Charter of Fundamental Rights: Right to an effective remedy and to a fair trial "Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid

In addition, the investigation into OCSSPs such as eBay and Amazon is justified by the high rates of counterfeit goods within the networks of online marketplaces,⁸⁸ which might pose a serious threat to e-commerce services. Online consumers lose their trust towards online services when they are deceived and purchase fake goods online. In this sense, the cornerstone of e-commerce, which is the trust of online consumers, may be eroded.⁸⁹ This development may have a negative impact for the online world and the consumers' trust on e-commerce platforms and online sales in general.⁹⁰

Finally, it is important to mention that this thesis will not look at the regulatory framework of search engine machines, such as Google⁹¹ or Bing.⁹² This is because there is no common ground as to whether search engines qualify as hosting ISSPs.⁹³ For instance, in the UK in *Designtecnica Corporation v. Google*⁹⁴ Justice Eady concluded that liability immunity provisions do not apply in search engines. Likewise, in France in *SARL Publison System v SARL Google France*⁹⁵ the Court of Appeal of Paris concluded that search engines do not offer hosting services to their users. By contrast, at European level, in *Google France/Inc. v. Louis Vuitton Malletier*⁹⁶ the Advocate General noted that search engines fall into the

shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice”.

⁸⁸ OECD, “The Economic Impact of Counterfeiting and Piracy” (2008) is available at <<http://www.oecd.org/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm>> last accessed 27 December 2019; UNODC, “The Globalization of Crime: A Transnational Organized Crime Threat Assessment” (2010) is available at <https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment.html/TOCTA_Report_2010_low_res.pdf> last accessed 27 December 2019; EU Commission Staff Working Paper, “Counterfeit and Piracy Watch List” SWD (2018) 492 final is available at <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf> last accessed 27 December 2019.

⁸⁹ World Economic Forum report on “The Global Governance of Online Consumer Protection and E-commerce Building Trust” (2019) 4.

⁹⁰ EU Commission, “Online Platforms and the Digital Single Market Opportunities and Challenges for Europe” COM (2016) 0288 final 10 where it has been found that “if consumers are properly informed of the nature of the products that they view or consumer online, this assist the efficient functioning of markets and consumer welfare”; EU Commission, “Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce: Summary of response” (2010).

⁹¹ <https://www.google.com/>

⁹² <https://www.bing.com/?PC=JV01>

⁹³ For the debate on whether search engines qualify as hosting ISSPs see EU Commission, “EU study on the New rules for a new age? Legal analysis of a Single Market for the Information Society, 6. Liability of online intermediaries” (2009) 24.

⁹⁴ *Designtecnica Corporation v. Google* [2009] EWHC 1765 (QB), para. 117 where it has been noted that with regard to liability immunity provisions as enshrined in Article 14 of the ECD “the United Kingdom government has so far taken the view that it is unnecessary or inappropriate to extend protection expressly to search engines.”

⁹⁵ *SARL Publison System v SARL Google France* [2009] (Court of Appeal of Paris)

⁹⁶ Joined Cases C-236/08, C-237/08 and C-238/08 of *Google France/Inc. v. Louis Vuitton Malletier* (2009) ECLI:EU:C:2009:569, para. 134 where the Advocate General Poireres Maduro notes that “In any case, the provision of hyperlink services and search engines falls squarely within the notion of information society

scope of hosting ISSPs as per Article 14 of the ECD. Therefore, the scope of this thesis is limited to the assessment of the regulatory framework of hosting ISSPs and their subcategories, OCSSPs with regard to their users' wrongdoings. Yet, if any court rulings or policy initiatives that are related to search engines are deemed relevant to the analysis and can be equally applied to the context of hosting ISSPs and OCSSPs that host material, they are discussed.

C. *Primary and secondary liability in tort*

As presented above, the scope of this thesis examines the liability of hosting ISSPs and OCSSPs for trade mark and copyright violations that accrue within their networks respectively. While intellectual property rights are considered property rights,⁹⁷ a tort law perspective is adopted in this thesis in order to examine the type of liability of these information society service providers. This is because the correlation between tort law and intellectual property violations is undeniable.⁹⁸ Indeed, this understanding has been exemplified in a number of rulings that treat individuals who commit an intellectual property infringement as tortious liable. For instance, in *Ted Browne Music Co. v Fowler*,⁹⁹ it was noted that "courts have long recognized that infringement of a copyright is a tort, and all persons concerned therein are jointly and severally liable as such joint tortfeasors."¹⁰⁰ In similar fashion, in *Lawrence v Dana*¹⁰¹ it has been concluded that "rights secured by copyright are property within the meaning of the law of copyright, and whoever invades that property beyond the privilege conceded to subsequent authors commits a tort, and is liable to an action."¹⁰² Moreover, it has been argued that

services and, most importantly – as I will argue next – their inclusion is consistent with the aims pursued by Directive 2000/31."

⁹⁷ C. Geiger, "Fundamental Rights as Common Principles of European (and International) Intellectual Property Law" in M. Leistner, *Common principles of European Intellectual Property Law* (Mohr Siebeck 2012) 225 where he notes that "in the case law of European Court of Human Rights, intellectual property has also entered the field of fundamental rights as the Court has issued more and more rulings interpreting IP relevant provisions of the European Convention on Human rights, and especially the right to property" and "...even though intellectual property is not explicitly named, there is no longer any doubt that the exploitation right is also protected by Art. 1 of Protocol 1 of the Convention, which protects property."; P. Goold, "Unbundling the tort of copyright infringement" (2016) 102 *Virginia Law Review* 1842; *Anheuser-Busch Inc v. Portugal* (11 January 2007) Application no. 73049/01 where it has been concluded that "We therefore agree that Article 1 of Protocol No. 1 is applicable to intellectual property in general and to a duly registered trade mark."

⁹⁸ R. Arnold and P. Davies, "Accessory liability for intellectual property infringement: the case of authorisation" (2017) *The Law Quarterly Review* 1 where they have aptly remarked that "...intellectual property laws are treated as tort laws"

⁹⁹ *Ted Browne Music Co. v Fowler*, 290 F. 751, 754 (2d Cir. 1923).

¹⁰⁰ A. Dorfman and A. Jacob, "Copyright as tort" (2011) 12 *Theoretical Inquiries in Law* 80-82.

¹⁰¹ *Lawrence v Dana*, 15 F. Cas. 26, 61 (Circuit Court, D. Mass 1869)

¹⁰² P. Goold, "Unbundling the tort of copyright infringement" (2016) 102 *Virginia Law Review* 1842

intellectual property law has contributed to the development and shape of tortious liability doctrines and in particular tortious secondary liability.¹⁰³ Given that the tortious secondary liability doctrine is not harmonized at the European level or even under-analysed in many national jurisdictions,¹⁰⁴ intellectual property law cases have attempted to clarify or offer a better understanding of the different schemes of secondary liability.¹⁰⁵ For example, at UK level, Lord Templeman in *CBS Songs Ltd v Amstrad Consumer Electronics Plc*¹⁰⁶ framed the distinctive elements of the different schemes of tortious secondary liability doctrine, namely authorisation, common design and procurement.¹⁰⁷ Following this, Kitchin Justice in *Newzbin*¹⁰⁸ built on the *CBS Songs Ltd v Amstrad Consumer Electronics Plc* ruling and offered a narrower interpretation of the distinctive elements of tortious secondary liability.¹⁰⁹ A thorough analysis of the different schemes of tortious secondary liability doctrine is explored further in chapter 2.

In connection with the above, this thesis looks at the two types of tortious liability, which are attributed to OCSSPs and hosting ISSPs for copyright and trade mark infringements that are carried out by their users. More specifically, their liability is examined through the lens of primary and secondary tortious liability rules.

With regard to the term of primary tortious liability, there is a consensus in the literature that notes that an individual is found primary liable when she commits an intellectual property infringement. Within the online context, the concept of primary tortious liability has been endorsed with the DSMD and in particular under Article 17, which notes that “..an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users.” This concept, as already explained at the outset of this thesis, introduces primary liability rules for online content sharing providers and thus comes to

¹⁰³ P. Davies, “Accessory liability: protecting intellectual property rights” (2011) 4 Intellectual Property Quarterly 390.

¹⁰⁴ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 19.

¹⁰⁵ P. Davies, “Accessory liability: protecting intellectual property rights” (2011) 4 Intellectual Property Quarterly 390.

¹⁰⁶ *Amstrad CBS Songs v. Amstrad* [1988] UKHL 15.

¹⁰⁷ P. Davies, “Accessory liability: protecting intellectual property rights” (2011) 4 Intellectual Property Quarterly 390.

¹⁰⁸ *Twentieth Century Fox Film Corp v Newzbin Ltd* (2010) EWHC 608 (Ch).

¹⁰⁹ P. Davies, “Accessory liability: protecting intellectual property rights” (2011) 4 Intellectual Property Quarterly 390.

change the liability regime for information society providers with regard to copyright violations within their networks.

Importantly, Article 17 of the DSMD has been considered as *lex specialis* to Article 14 of the ECD. This means that the services, which are excluded from the scope of Article 17 of the DSMD, fall into the scope of Article 14 of the ECD that employs secondary liability rules for hosting ISSPs in cases of intellectual property infringements. Therefore, the activities of hosting ISSPs that do not fall into the category of Article 17 of the DSMD are regulated under the existing law of the ECD where a secondary liability regime is in force.

However, by contrast to the term primary tortious liability, the term secondary tortious liability is not subject to an international consensus in the literature. Indeed, there are many and varied definitions that are used by scholars in order to define the concept of secondary tortious liability rules.¹¹⁰

The reason behind the existence of these definitions on secondary liability doctrine is mainly attributed to the different legal traditions that impose different requirements in order to trigger secondary liability rules for the actions carried out by the internet users of an ISSP and not by the ISSP itself. These examples include joint-tortfeasance, accessory liability, contributory liability and indirect liability are employed by academic scholarship and different laws. Yet, the terms, as presented in chapter 2, do not necessarily trigger the same outcomes. Therefore, this diversity of definitions in secondary tortious liability might create confusion to scholars. Indeed, Dinwoodie points out that this divergence may trigger “some terminological difficulties for comparative analysis.”¹¹¹ This means that it would be complex for a scholar to find the equivalent of a secondary tortious liability doctrine to each jurisdiction and thus undertake a comparative analysis between different legal systems.

Hence, for the sake of clarity, this thesis uses the term ‘secondary liability’ in order to describe the liability of hosting ISSPs for violations carried out by their internet users.¹¹² Yet, it is crucial to point out that the wrongdoing according to which a hosting ISSP has

¹¹⁰ G. Dinwoodie, “A comparative analysis of the secondary liability of online service providers” in G. Dinwoodie (ed.), *Secondary liability of internet service providers* (Springer 2017) 6-7.

¹¹¹ *Ibid*, 6.

¹¹² In light of the expeditious developments in hosting ISSPs’ liability at legislative and case law level, it seems now even more difficult to offer a definition for the liability of hosting ISSPs with regard to the copyright and trade mark infringements within their networks.

been found secondary liable should not be confused with the wrongdoing of the primary infringer-user. This is because, as pointed out in chapter 2, hosting ISSPs under the ECD may be held secondary liable for enabling, facilitating the commission of copyright infringement by their users and not by committing a copyright or a trade mark violation themselves.

Finally, as already discussed in Section II of this chapter, the aim of this thesis is to critically assess the regulatory framework of hosting ISSPs and OCSSPs under the existing laws. It does not look at the conditions that constitute a wrongdoing, namely it refrains from examining whether a copyright or a trade mark violation takes place. Further, the scope of this thesis is limited to two kinds of intellectual property infringements, namely copyright and trade mark violations. This means that the regulatory framework of hosting ISSPs and OCSSPs for other violations, such as the violation of the right to privacy, defamation or other types of intellectual property rights, are not be examined. Yet, any case that may be equally applied to context of copyright and trade mark infringements is discussed.

V. Research Methodology

In order to answer the research question and fulfil the aim of this thesis, I adopt the following methodological approaches.

First, my work is primarily doctrinal. Through the lens of the doctrinal legal approach “the essential features of the legislation and case law are examined critically and then all the relevant elements are combined and synthesized to establish an arguably correct and complete statement of the law on the matter in hand.”¹¹³ Thus, this thesis critically assesses the current legal framework and builds upon the findings in order to recommend a more robust legal regime for hosting ISSPs. This doctrinal legal methodology consists of a positivist and normative approach. I adopt a positivist approach by looking at the existing legal framework and critically evaluating it and identifying any potential discrepancies. Following this, I continue with a normative approach. In doing so, I explore the legal principles underpinning the legal framework governing hosting ISSPs and, on the basis of these principles, I address how the law should be shaped in order to strike a fair balance between the interests at stake, as is clearly set out in my research question.

¹¹³ D. Watkins and M. Burton, *Research Methods in Law* (Routledge 2017).

However, what is important to point out is that in chapter 2, I look at the current legal framework that regulates hosting ISSPs' activities at European level and examine the national implementation of the EU legal framework in three selected national jurisdictions. These national jurisdictions are not examined from a comparative angle. They serve only as examples that illustrate the inconsistent approach of national courts towards the liability of hosting ISSPs. The three selected national jurisdictions are the UK, Germany and France and their choice has been made on the basis of them being the most representative jurisdictions at EU level, namely common law and civil law jurisdictions.

Chapter 6 of my thesis follows a normative approach. It builds upon the previous chapters and recommends the establishment of a hosting ISSP supervisory authority for copyright and trade mark violations in the digital ecosystem. Then, it suggests how such an authority would operate, and which principles and functions would be needed to maintain an equilibrium between the interests of right holders, hosting ISSPs and internet users.

Secondly, apart from the doctrinal legal methodology, my work benefits from a comparative legal methodology. This is understood as the examination of "one mass of legal data in relationship to another and then assessing how the two lumps of legal data are similar and how they are different. The essence of comparison is then aligning similarities and differences between data points, and then using this exercise as a measure to obtain understanding of the content and range of the data points."¹¹⁴ This is how the second part of chapter 4 functions. I draw parallels with the US legal system in order to inform my research. More specifically, I look at the Good Samaritan clause which is enshrined in Digital Millennium Copyright Act (DMCA).¹¹⁵ This clause exonerates hosting ISSPs from liability if they adopt proactive measures with regard to the termination of copyright infringements online. This Good Samaritan clause is an idiosyncrasy of the US legal system and appears to have merits, as evidenced by existing academic scholarship and court rulings in the US legal system. So, on the basis of the Good Samaritan clause, I recommend reforms to the current legal framework so as to strike a fair balance between the interests at stake. Finally, in chapter 6 I undertake an examination of already established ISSP authorities in Greece and Italy as well as draw parallels with other fields

¹¹⁴ E. Eberle, "The Methodology of Comparative Law" (2011) 16 *Roger Williams University Law Review* 52.

¹¹⁵ Us Congress, *Digital Millennium Copyright Act*, 105-304 (1998).

of law where authorities have been set up, namely data protection and competition law authorities.

VI. Originality of the thesis

The originality of this thesis draws upon three main aspects. Firstly, it focuses on the hosting ISSPs' liability for copyright and trade mark infringements. Although academic literature that addresses hosting ISSPs' liability for copyright and trade mark separately exists, no research has been found that critically assesses hosting ISSPs' liability for both copyright and trade mark infringements that occur within their networks. This is urgent for two main reasons. From an academic perspective, more attention should be drawn to these two intellectual property infringements since copyright and trade mark infringements constitute the most common intellectual property violations online. Indeed, as elaborated in chapter 2, a bedrock of case law reveals the frequency of copyright and trade mark violations online. The second reason is the dual liability regime that was endorsed with the DSMD. As explained at the outset of this chapter, Article 14 of the ECD includes a secondary liability regime for hosting ISSPs. By contrast, Article 17 of the DSMD introduces a primary liability framework for copyright infringements that accrue within their networks. A detailed analysis of the implications of this dual liability regime for hosting ISSPs and internet users seems crucial for innovation in the Digital Single Market and consumers' welfare in general.

Further, this research has been the first that assesses the current legislative framework under the DSMD, which was finalized on the 17th of April 2019. Even though the DSMD is a new Directive and its implications have not been tested yet in the courts' legal arena, the findings indicate a cluster of problematic aspects within Article 17 of the DSMD. So far, the existing literature has limited its discussion to the proposal for a DSMD and the compromise texts of the EU Council and the EU Parliament. For this reason, this thesis puts forwards a critical evaluation of the implications of the final draft of the DSMD, including a historical account of the whole legislative process that culminated in the DSMD. What is more, this thesis is the first work to address the intersection between Article 14 of the ECD and Article 17 of the DSMD. Under the scope of Article 14 of the ECD falls the hosting ISSPs' liability for trade mark infringements, while Article 17 of the DSMD regulates OCSSPs' liability for copyright infringements. Given that this thesis addresses both copyright and trade mark infringements, a critical examination of the intersection

between these two legislative tools is warranted. It is this intersection that is also problematic and thus might pose serious risks for the interests of intellectual property holders, internet users and hosting ISSPs' interests.

Finally, the main contribution of this thesis derives from the novel suggestions that it includes. It suggests a regulatory framework that takes into consideration to a great extent the different interests at stake. Although many scholars have addressed the thorny issues of hosting ISSPs' liability, they mostly considered one-sided amendments in the legislation, without attempting to balance the interests of intellectual property holders, internet users and hosting ISSPs. For this reason, this thesis aims to suggest plausible solutions for all the parties at stake and thus safeguard, to a great extent, fundamental rights, as they are explicitly included in the EU Charter of Fundamental Rights. More specifically, these novel recommendations include the establishment of a responsibility framework based on a co-regulatory approach. This framework is about imposing a set of responsibilities to hosting ISSPs along with the establishment of a hosting ISSP supervisory authority in cases of copyright and trade mark violations online. This authority will have specific duties such as, enforcement duties, adjudication duties and information awareness duties towards the negative effects of online piracy. These recommendations, which are set out in Part II, are developed through an extensive analysis on the basis of normative and theoretical underpinnings, a cluster of case law and policy initiatives at European level, and at national level across the EU member states.

VII. Structure of the thesis

This thesis is divided into two parts, with a conclusion and an introduction as separate chapters. The first part consists of chapters 2 and 3 and the concluding remarks of Part I that address a critical evaluation of the inefficiencies of the current legal framework that regulates hosting ISSPs' activities for copyright and trade mark infringements that accrue within their networks. The second part includes chapters 4, 5 and 6 and presents an array of recommendations about how to structure a more robust legal framework for hosting ISSPs with regard to copyright and trade mark violations online. Chapter 1 is the introduction of this thesis and chapter 7 encompasses the research findings, a summary of recommendations and an epilogue.

Chapter 1 sets forth the context of this thesis, explains its need, shapes the research question as well as the sub-questions and defines the scope of this thesis. Following this,

I explain the methodological approaches for addressing the research question, the originality of this thesis and present an outline of the chapters.

Chapter 2 critically evaluates the current legal framework that regulates hosting ISSPs' activities under the ECD. It analyses the legal nature of hosting ISSPs' liability, which is the secondary liability, the rationale for imposing secondary liability rules to hosting ISSPs and the theoretical background upon which hosting ISSPs' liability relies. Then, it explores the requirements that trigger hosting ISSPs' liability under Article 14 of the ECD, analyses their national implementation in three selected jurisdictions and identifies any flaws.

Chapter 3 critically engages with the DSMD. At the outset, I offer a historical account of Article 13 of the DSMD (which has been renamed Article 17 at the final draft of the DSMD) where I discuss the EU Commission's Proposal, and the EU Council's and EU Parliament's compromised texts.¹¹⁶ Following this, I critically assess Article 17 of the DSMD where I identify a set of problematic features that reinforce the suggestion that this provision undermines the rights of OCSSPs and internet users' rights. Finally, the chapter offers concluding remarks for both chapters 2 and 3, which constitute Part I of this thesis. In those concluding remarks, a critical examination of the implications of liability rules to hosting ISSPs and OCSSPs, intellectual property holders and internet users is presented.

Chapter 4 offers several normative and theoretical insights towards the creation of a responsibility framework based on co-regulation for hosting ISSPs with regard to copyright and trade mark infringements that take place within their networks. Further it engages with one of the responsibilities that hosting ISSPs have towards the dissemination of infringing content and counterfeit goods within their networks.

In chapter 5, I explore another responsibility that hosting ISSPs should have towards their users, namely a transparency obligation. In doing so, I observe the lack of a statutory transparency obligation and meticulously elaborate on the normative considerations for having such an obligation at European level. In light of this normative examination, I recommend how a transparency obligation should be implemented in practice by hosting ISSPs in order to achieve, to a great extent, the equilibrium between the interests of the

¹¹⁶ EU Parliament, "European Parliament approves new copyright rules for the internet" (Press release, 26 March 2019) is available at <<http://www.europarl.europa.eu/news/en/press-room/20190321PR32110/european-parliament-approves-new-copyright-rules-for-the-internet>> last accessed 23 April 2019.

parties involved, namely the interests of hosting ISSPs, internet users/ online consumers and right holders.

Following this, chapter 6 builds upon the previous chapters and recommends the establishment of a hosting ISSP supervisory authority. I demonstrate the normative considerations for creating such an authority, as well as suggest the principles and the functions under which the proposed authority would operate. In order to suggest the principles and functions of the proposed hosting ISSP authority I draw parallels with existing ISSPs authorities in Greece and Italy as well as authorities in other fields of law such as data protection authorities and competition law authorities.

Chapter 7 concludes this research. I present the main findings of this thesis and a set of recommendations that have been thoroughly discussed in the precedent chapters. It also entails an epilogue with two concluding remarks with regard to the enactment of the DSMD across the EU member states and Brexit.

Part I: The current EU legislative tools that regulate hosting ISSPs'¹¹⁷ liability for copyright and trade mark infringements within their networks

¹¹⁷ Hosting information society service providers, hereinafter hosting ISSPs.

Chapter 2: The Hosting Information Society Service Providers' (hosting ISSPs) liability framework under Article 14 of the E-Commerce Directive (ECD): an outdated approach

I. Introduction

The introduction of the E-Commerce Directive¹¹⁸ back in 2000 established the regulatory framework of hosting ISSPs' activities in the European Union.¹¹⁹ Following the rationale of the provisions that were included in its US counterpart, the Digital Millennium Copyright Act (DMCA),¹²⁰ the ECD offers immunity from liability to those ISSPs that provide mere conduit, caching and hosting services under specific circumstances. More specifically, under Article 14 of the ECD, which is the provision that is relevant for this research, hosting ISSPs are exonerated from liability if they do not have knowledge of the infringing material or illicit activity that takes place within their networks or when they expeditiously remove the infringing material upon receiving notification from the right holder.¹²¹

These immunity liability provisions, also known as safe harbour provisions, for hosting ISSPs were justified on the basis of boosting innovation and development in the European Digital Single Market.¹²² At that time, when the ECD was drafted at the European level, e-commerce was still in its infancy but had promising perspectives for rapid growth within the next few years.¹²³ In this way, hosting ISSPs continued their business operation without the fear of liability rules being imposed on them.

¹¹⁸ Hereinafter ECD.

¹¹⁹ Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178.

¹²⁰ 17 U.S.C. §§ 512 of Digital Millennium Copyright Act (hereinafter DMCA).

¹²¹ Articles 12, 13 and 14 of the ECD.

¹²² M. Pélissier du Rausas et al., "McKinsey Global Institute: Internet matters, the net's sweeping impact on growth, jobs, and prosperity" (May 2011) is available at <<https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/internet-matters>> last accessed 27 December 2019; C. Wright, "Actual versus legal control: Reading vicarious liability for copyright infringement into the Digital Millennium Copyright Act of 1998" (2000) 75 Washington Law Review 1005.

¹²³ EU Commission, "Commissioner Bolkestein welcomes political agreement on electronic commerce Directive" (8 December 1999) is available at <http://europa.eu/rapid/press-release_IP-99-952_en.htm?locale=en> last accessed 27 December 2019; it has been noted that "the global electronic commerce market is growing extremely fast and could be worth \$ 1.4 trillion by the year 2003 (source: Forrester Research). In Europe, electronic commerce is already worth €17 billion and is expected to reach €340 billion by 2003"; A. Wyckoff and A. Colecchia, *The Economic and Social Impact of Electronic Commerce* (1992) OECD 12; T. Verbiest, G Spindler, G Riccio & A Van der Perre, "Study on the Liability of Internet Intermediaries: general trends in the EU" (2007) 4.

However, with the rapid development of e-commerce services, a dramatic increase in the emergence of online infringements has been observed. What is more, this coincided with the increased occurrence of copyright and trade mark infringements on the internet. This thorny issue of online piracy has been aggravated by the advent of Web 2.0 era.¹²⁴ Within the context of the Web 2.0 era, hosting ISSPs offer new services to their users, which can increase the risk of unauthorized material or displaying counterfeit goods being uploaded online.¹²⁵ This understanding has been supported by a number of studies that demonstrate the correlation between the digital ecosystem and online infringements. For instance, pursuant to the report of EUIPO on intellectual property infringements in 2018, it has been found that the internet is a facilitator for the dissemination of unauthorized content and counterfeit goods online.¹²⁶ Likewise, in the recently published report by the EU Commission on Counterfeit and Piracy Watch list in 2018, it is possible to observe that the main type of hosting ISSPs that offer within their premises the circulation of unauthorized material are hosting ISSPs.¹²⁷

Witnessing this exponential growth in online copyright and trademark infringements, right holders decided to resort to courts with the aim of seeking compensation for their losses. However, while there have been cases where intellectual property holders have filed lawsuits against individual users,¹²⁸ there is increasing litigation where right holders bring civil proceedings against hosting ISSPs; asking the courts to hold them secondarily

¹²⁴ Web 2.0 era amounts to hosting ISSPs that provide new online services to their users such as social networks, online marketplaces and online music platforms; Tim O' Reilly, "What is Web 2.0" (30 September 2005) is available at <<https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>> last accessed 27 December 2019; L.W. Friedman and H.H. Friedman, "The New Media Technologies: Overview and Research Framework" (2008) 1; World Intellectual Property Organization, "Five Steps to Protect Your Trademarks in the Web 2.0 World" (September 2010) is available at <https://www.wipo.int/wipo_magazine/en/2010/05/article_0006.html> last accessed 27 December 2019.

¹²⁵ A telling example can be found in Amazon. What services Amazon has offered at its beginning and what services Amazon offers now to its online consumers, see A. Hartmans, "15 fascinating facts you probably didn't know about Amazon" (Business Insider, 23 August 2018) is available at <<https://www.businessinsider.com/jeff-bezos-amazon-history-facts-2017-4?r=US&IR=T#in-the-early-days-of-amazon-a-bell-would-ring-in-the-office-every-time-someone-made-a-purchase-and-everyone-would-gather-around-to-see-if-they-knew-the-customer-2>> last accessed 27 December 2019.

¹²⁶ European Intellectual Property Office, "Synthesis report on IPR infringement" (2018) 16 is available at <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/docs/Full%20Report/Full%20Synthesis%20Report%20EN.pdf> last accessed 27 December 2019

¹²⁷ EU Commission Staff working document, "Counterfeit and Piracy Watch List" SWD(2018) 492 final 8 is available at <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf> last accessed on 27 December 2019.

¹²⁸ *A&M Records v Napster* 9th Cir 2001; See also L. Edwards and C. Waelde, "Online intermediaries and liability for copyright infringement" (2005) WIPO 27; L. Edwards, "The fall and rise of intermediary liability online" in L. Edwards and C. Waelde, *Law and the Internet* (Hart Publishing 2009) 49; R. Giblin, *Code Wars: 10 Years of P2P software litigation* (Edward Elgar 2011) 2-3 where she notes that "From 2003-2007, members of the industry "filed, settled or threatened" lawsuits against more than 20.000 individuals."

liable for enabling or facilitating copyright and trade mark violations that accrue within their networks. The rise of tort claims from right holders can be justified due to the close connection between intellectual property law and tort law. This understanding has been reinforced in a bedrock of court rulings that perceive intellectual property infringements as torts and note that “courts have long recognized that infringement of a copyright is a tort, and all persons concerned therein are jointly and severally liable as such joint tortfeasors.”¹²⁹ In this sense, hosting ISSPs were subject to pay damages for the infringements or subject to injunctive relief that means either to block those webpages with illicit activities or install filtering technology to detect unauthorized material online. Yet, as critically discussed in this chapter, to hold hosting ISPPs secondarily liable for the illegitimate actions of their users seems challenging.

This is mainly due to the lack of harmonisation of secondary liability in tort at the European level, which has given rise to a sprawling patchwork of miscellaneous tortious secondary national doctrines across the European borders. In the absence of any harmonisation of secondary liability in tort, secondary liability rules have not been harmonized in a copyright context or trade mark context either but have only received peripheral attempts of harmonisation via the ECD. What is more, any attempts to offer a broader harmonisation perspective in the DSMD have not been fruitful.¹³⁰

Against this background, this chapter explores the liability that hosting ISSPs may incur for trade mark infringements that have been committed by their users under the ECD regime. What is worth to mention here, is that until the 17th of April 2019 when the Copyright in the Digital Single Market Directive (DSMD) has been finalized,¹³¹ the liability of hosting ISSPs for copyright violations has been regulated under Article 14 of the ECD. For this reason, existing case law that examines the liability of hosting ISSPs for copyright infringements under the ECD would be discussed in this chapter too. In this respect, the narrative starts with the theoretical and policy considerations that justify the imposition of secondary liability rules to hosting ISSPs. Following this, the discussion moves to the concept of secondary liability for trade mark infringements where the relationship between tort law and intellectual property law, as well as the peculiarities of tortious

¹²⁹ A. Dorfman and A. Jacob, “Copyright as tort” (2011) 12 *Theoretical Inquiries in Law* 80-82; *Ted Browne Music Co. v Fowler*, 290 F. 751, 754 (2d Cir. 1923).

¹³⁰ A critical analysis of the DSMD will follow in chapter 3 of this thesis.

¹³¹ Article 17 of the DSMD regulates the liability of OCSSPs for copyright infringements committed by their users

secondary liability doctrine, are discussed. Then, the concept of hosting ISPPs' liability as a form of secondary liability is presented. This enables the reader to gain an understanding of the potential drawbacks that the concept of secondary liability in tort may have on ISPPs. Having defined the concept of hosting ISPPs' liability, I then critically assess the conditions that trigger liability under the ECD and their national implementation in three selected legal systems, namely UK, Germany and France. These national legal systems have been chosen on the basis of them being the most representative legal traditions in Europe, with UK representing the common law tradition and Germany and France depicting the civil law tradition. The presentation of these national legal systems offers a clearer insight to the key aspects of the legal nature of tortious secondary liability rules.

In this regard, the narrative starts with the theoretical and policy justifications behind the imposition of secondary liability rules to hosting ISPPs.

II. Holding hosting ISPPs liable: theoretical and policy considerations

A. *Theoretical justifications of imposing a liability framework for hosting ISPPs in the form of secondary liability*

i. *Moral Theory*

In the brick and mortar world, an individual can be held liable from a moral perspective if she has committed the illegitimate acts by herself.¹³² This implies that an individual must not give account for third parties' actions; rather, she must be accountable only for her own actions.

Yet, within the online context, this view finds limited applicability since it has been argued that ISPPs should be morally liable for the tortious acts of their users.¹³³ This understanding, as Spinello explains, depends on how the term of cooperation is construed.¹³⁴ The term 'cooperation' is understood as the act of facilitation or

¹³² P. Davies, *Accessory Liability* (Hart Publishing 2015) 13.

¹³³ G. Frosio, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility" (2017) 25 *Oxford International Journal of Law and Information Technology* 5; L. Oswald, "International issues in secondary liability for intellectual property rights infringement" (2008) 45 *American Business Law Journal* 247; M. Bartholomew and J. Tehranian, "The secret life of legal doctrine: the divergent evolution of secondary liability in trademark and copyright law" (2006) 21 *Berkeley Technology Law Journal* 1419.

¹³⁴ R. Spinello, "Intellectual Property: Legal and Moral Challenges of Online File Sharing" in K. Einar Himma and H. Tavani (eds.), *Handbook of Information and Computer Ethics* (2008) 565.

inducement. More specifically, for hosting ISSPs it is understood as whether cooperation amounts to the facilitation or the inducement of a legitimate or an illegitimate activity.

From a general point of view, cooperation usually has positive connotations. Individuals cooperate with each other in communal activities in order to achieve a certain goal. However, there are stances where cooperation of individuals might lead to the commission of immoral acts. This may be the case for online intellectual property infringements. Representative examples of this line of thinking are the cases of file-sharing websites, online video exchange platforms or online marketplaces. For example, unauthorized content uploaded by internet users, is circulated online via online platforms, or counterfeit goods are offered for sale by sellers and are displayed online. Therefore, hosting ISPPs appear to cooperate with the wrongful acts of their users, who commit copyright or trade mark violations.

However, it could be argued that the above-mentioned examples are not similar. This is because an online-exchange platform such as YouTube¹³⁵, an online marketplace such as eBay, a file-sharing platform with unauthorized files such as the Pirate Bay, or a website that exclusively offers counterfeit goods,¹³⁶ are not based on the same business models. Rather, they are defined by different business goals and principles. This means that the main aim of an online video exchange platform or an online marketplace would be to enable their users to upload or download lawful content or to buy goods online respectively. By contrast, a file-sharing platform with illegitimate files or a website with fake products for sale engage in illicit activities by disseminating unlawful content online or deceiving potential customers with the offer of counterfeit goods. Therefore, to hold hosting ISSPs liable for the tortious acts of their internet users requires a higher degree of granularity for the concept of cooperation.

In this light, a distinction should be made between formal and material cooperation.¹³⁷ Insofar as formal cooperation is concerned, a hosting ISPP formally cooperates with the tortious acts of its internet users if its business model is deliberately designed to facilitate

¹³⁵ YouTube, Policies and safety <<https://www.youtube.com/intl/en-GB/yt/about/policies/#community-guidelines>> last accessed 27 December 2019.

¹³⁶ *Cartier International AG v. British Sky Broadcasting Ltd* [2015] ETMR 1.

¹³⁷ (St.) Alphonsus Liguori, *Theologia Moralis*. 4 volumes. ed. by L. Gaude (Rome: Ex Typographia 1912) 357 is available at <<https://archive.org/details/theologiamoralis01inligu>> last accessed 21 November 2017; R. Spinello, "Secondary Liability in the Post Napster Era: Ethical Observations on MGM v. Grokster" (2005) 3 *Journal of Information, Communication and Ethics in Society* 126.

the dissemination of unlawful content or the circulation of pirated goods. As Spinello states, formal cooperation occurs when a “person assists another person to commit a wrongful act, sharing its bad will and intention.”¹³⁸ Consider, for instance, the *Cartier II* case where the “targeted websites” exclusively offered the sale of counterfeit goods from luxury brands.¹³⁹ Hence, a hosting ISPP may be considered morally liable if it formally cooperates with the wrongdoings of its users, who either share unauthorized material or offer for sale fake goods online.

Furthermore, another option for a hosting ISPP to be considered morally liable for the intellectual property infringements that may occur within its platform is the material cooperation with the wrongdoings of its users. Material cooperation is understood as when an ISPP designs its business model for legitimate purposes but accepts that, in the course of its operation, the emergence of illicit activities will be unwanted side effect.¹⁴⁰ Indeed, this understanding emerges from Spinello’s theory which suggests that the act of material cooperation triggers moral liability if most of the following conditions are fulfilled: the action of the individual must be unjust, proportionate to the gravity and the proximity of contributing to the wrongdoing and the individual must have rejected the possibility to deploy an alternative mechanism which could restrict any negative interference of the action.¹⁴¹

This theory implies that, within the online context, the imputation of moral liability to those hosting ISSPs is excluded, insofar as those websites deploy appropriate technological measures and terminate, or at least curb to a great extent, the circulation of unauthorized content or pirated goods. Representative examples of this line of thinking can be found in video-music platforms and social networks.¹⁴² The popularity of these hosting ISSPs increased dramatically due to the services they offer to users.¹⁴³ Such services are focused on enabling users to upload and share authorized films, TV Programs or music files, without excluding the possibility of disseminating illegitimate content that

¹³⁸ R. A. Spinello, “Intellectual Property: Legal and Moral Challenges of Online File Sharing” in K Einar Himma and H Tavani (eds.), *Handbook of Information and Computer Ethics* (2008) 565.

¹³⁹ *Cartier and Another v BSKyB and Others* [2016] EWHC 339 (Ch).

¹⁴⁰ R. Spinello, “Secondary Liability in the Post Napster Era: Ethical Observations on MGM v. Grokster” (2005) 3 *Journal of Information, Communication and Ethics in Society* 128.

¹⁴¹ *Ibid*, 126.

¹⁴² Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644.

¹⁴³ “6 Reasons Why Social Networking is So Popular These Days” (Brandignity) is available at <<https://www.brandignity.com/2012/11/6-reasons-why-social-networking-is-so-popular-these-days/>> last accessed 27 December 2019.

has been uploaded by their users. Therefore, these websites are involved in the dissemination not only of legal content but also of unlawful content. Yet, in order not to be considered morally liable, those hosting ISSPs deploy filtering-based technology that identify and remove online intellectual property infringements. For instance, eBay deploys the so-called VERO, Verified Rights Owner Program, which is a database where brand owners submit reports with regard to the selling of fake goods on the eBay platform.¹⁴⁴ In this way, while unauthorized content or counterfeit goods might be circulated, hosting ISSPs undertake specific measures in order to curb or stop their circulation online. Hence, those hosting ISSPs are not be exposed to moral liability discourse.

By contrast, other hosting ISSPs might be subject to moral liability if they refrain from deploying filtering-based technological systems. Consider, for instance, the example of a hosting ISSP whose platform offers a number of counterfeit goods to its users. Indeed, a report conducted by the EU Commission on Counterfeit and Piracy Watch list demonstrates that a large amount of fake goods is circulated online.¹⁴⁵ Likewise, a bedrock of case law engages with the violation of trade marks in the digital ecosystem. A representative case is to found in the *Cartier II* case where the High Court of England and Wales has ordered a blocking injunction and required British Telecommunications to terminate access to a website that offered counterfeit Cartier bags and watches.¹⁴⁶ Therefore, given the circulation of fake goods online, the absence of any precautionary measures to tackle online infringements could justify the moral liability of hosting ISSP whose services address the online purchase of goods.

Therefore, in the light of the above, it could be extrapolated that a hosting ISSP can be conceived morally liable for the wrongdoings of its users if it engages either in formal or material cooperation with the tortious acts of its users. On the one hand, the act of formal cooperation leads to moral liability if an ISSP designs its business model in such a way that attracts only illegitimate content. On the other hand, material cooperation concerns a

¹⁴⁴ S. Pilutik, "eBay's Secondary Trademark Liability Problem and its VeRO Program" (2007) is available at <<http://www.cs.cmu.edu/~dst/Secrets/E-Meter/eBay-VERO-pilutik.html>> last accessed 27 December 2019; A. Cheung and KH. Pun, "Comparative study on the liability for trade mark infringement of online auction providers" (2009) 31 European Intellectual Property Review 7.

¹⁴⁵ EU Commission Staff Working Paper, "Counterfeit and Piracy Watch List" SWD (2018) 492 final is available at <http://trade.ec.europa.eu/doclib/docs/2018/december/tradoc_157564.pdf> last accessed 27 December 2019.

¹⁴⁶ *Cartier and Another v BSKyB and Others* [2016] EWHC 339 (Ch).

hosting ISSP whose business model attracts a number of illegitimate content or counterfeit goods. However, for a hosting ISPP, moral liability due to material cooperation may arise only under certain circumstances. This means that a hosting ISSP is not morally liable if it installs technological measures in order to stop any illicit activity within its platform. Rather, moral liability might occur when the hosting ISSP accepts the emergence of online infringements within its network and does not deploy any further measures to restrict them, thus accepting the harmful outcomes its business model on third parties' rights.

ii. Utilitarian Theory

Another theory that could influence the imposition of a liability framework in the form of secondary liability is utilitarian theory. This theory is about allocating a right after assessing the impact of an action on third parties in comparison to the impact of another action to those third parties.¹⁴⁷ Transposing this theory into the hosting ISSPs' liability regime means that the allocation of secondary liability rules on hosting ISSPs is contingent upon the impact that hosting ISPPs' activities might have on the different parties involved, namely content owners, brand owners and internet users.¹⁴⁸

Hosting ISSPs' liability in the form of secondary liability could find its roots in the gatekeeper liability theory.¹⁴⁹ One of the key proponents of gatekeeper theory is Kraakman. He developed the concept of gatekeeper liability, which can be described as liability "that is imposed on private parties who are able to disrupt misconduct by withholding cooperation with wrongdoers".¹⁵⁰ He noted that gatekeeping occurs when wrongdoings are not impeded by law authorities and the gatekeepers could identify the wrongdoing more efficiently without taking into consideration market standards and

¹⁴⁷ Pareto principle in Q. Zhou, "The Evolution of Efficiency Principle: From Utilitarianism to Wealth Maximization" (2005) SSRN 8; W. Fisher, "CopyrightX: Lecture: Supplements to Copyright: Secondary Liability" (2014) 81-82 is available at <http://copyx.org/files/2014/08/CopyrightX_-_Lecture_Transcripts_Book.pdf> last accessed 27 December 2019.

¹⁴⁸ G. Frosio, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility" (2017) 25 Oxford International Journal of Law and Information Technology 5.

¹⁴⁹ E. Laidlaw, "A framework for identifying Internet information gatekeepers" (2010) 24 International Review of Law, Computers & Technology 264-267; A. Tuch, "The limits of Gatekeeper liability" (2017) Washington and Lee Law Review Online 619; A. Hamdani, "Gatekeeper liability" (2003) 77 Southern California Law Review 98.

¹⁵⁰ R. H. Kraakman, "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy" (1986) 2 Journal of Law, Economics and Organization 54.

private incentives.¹⁵¹ This implies that the role of gatekeepers is twofold, namely to prevent infringements and to identify those infringements at a reasonable cost.

a. Gatekeepers as a source of deterrence

First, in order to reinforce the role of gatekeepers as “a source of deterrence” of the wrongdoings,¹⁵² Kraakman selects examples from various professions. For instance, he argues that accountants and lawyers are natural gatekeepers of financial transactions because they can detect fraudulent transactions with their audits or legal views. Moreover, doctors and pharmacists are natural gatekeepers of medicines as they can terminate the abuse of controlled substances through the prescription system.

This understanding could be applicable within the online world too. In this case, Barzilai-Nahon introduced the term of gatekeeper to the digital ecosystem and conceived ISPPs as gatekeepers.¹⁵³ According to her theory, hosting ISPPs appear to be the gatekeepers of hosted data and thus they can detect copyright infringements via their filter-based mechanisms. Following her writings, other scholars supported the notion that hosting ISPPs seem to be the gatekeepers of the online world. For instance, Laidlaw argues that hosting ISPPs are gatekeepers that control the flow of information that passes through their gates¹⁵⁴ while Thompson goes one-step further and posits that due to their role as gatekeepers, hosting ISPPs design the online word by choosing which information does and does not reaches the end-users.¹⁵⁵ Therefore, the imposition of secondary liability rules to hosting ISPPs might be justified due to their role as a source of deterrence of tortious acts online.

However, it is not only academic scholarship that is in favor of imposition a secondary liability framework in light of the role of hosting ISPPs as a source of deterrence of wrongdoings. Indeed, to treat hosting ISPPs as a source of deterrence of wrongdoings has been outlined at legislative and judicial level too. With regard to judicial level, Recital 59

¹⁵¹ Ibid, 61.

¹⁵² M. Bartholomew and J. Tehranian, “The secret life of legal doctrine: the divergent evolution of secondary liability in trademark and copyright law” (2006) 21 Berkeley Technology Law Journal 1366; they noted that “shift injury costs to those who are in a position to prevent future injuries.”

¹⁵³ K. Barzilai- Nahon, “Toward a theory of network gatekeeping: a framework for exploring information control” (2008) 59 Journal of the American Society for Information Science and Technology 1493.

¹⁵⁴ E. Laidlaw, “A framework for identifying Internet information gatekeepers” (2010) International Review of Law, Computers & Technology 263.

¹⁵⁵ M. Thompson, “Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries” (2016) 18 Vanderbilt Journal of Entertainment & Technology Law 783.

of the InfoSoc Directive notes that “...intermediaries are best placed to bring such infringing activities to an end.”¹⁵⁶ This means that European policymakers support the view that hosting ISSPs are best situated to terminate violations that accrue online. At judicial level, the role of hosting ISSPs as a source of deterrence has been exemplified in a bedrock of court rulings where the judiciaries have assessed whether auction platforms or other social networks could have done more to terminate or at least mitigate the sale of counterfeit goods or the downloading of unauthorized content. For instance, at European level in *L’Oreal v eBay*, L’Oreal brought a legal action against eBay, alleging that eBay’s efforts to prevent the selling of counterfeit goods on its network were insufficient.¹⁵⁷ Although the CJEU handed down that the ascription of liability rules on the is a matter left to the domestic courts of national member states,¹⁵⁸ what is important to stress in this case, is that the CJEU views hosting ISSPs as a source of deterrence of wrongdoings. In this regard, the Court referred to the opinion of Advocate General Jääskinen and described the role of website operators as follows: “if the operator of the online marketplace does not decide, on its own initiative, to suspend the perpetrator of the infringement of intellectual property rights in order to prevent further infringements of that kind by the same seller in respect of the same trade marks, it may be ordered, by means of an injunction, to do so.”¹⁵⁹ This implies that hosting ISSPs are seen by judicial authorities as a source of terminating the circulation of counterfeit goods online and for this reason hosting ISSPs are secondarily liable for not installing the appropriate measures to deter the emergence of online infringements.

Such a stance has been maintained by national courts where hosting ISSPs have been subject to secondary liability rules due to their role as a source of deterrence for online infringements. In particular, in Italy, Delta TV brought legal proceedings against Google and YouTube, alleging that a link to YouTube that included videos of episodes of Telenovelas without Delta TV’s consensus appeared once the internet user had accessed Google’s search results list.¹⁶⁰ In response to the allegations, Google and YouTube argued

¹⁵⁶ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (hereinafter InfoSoc Directive).

¹⁵⁷ Case C-324/09, *L’Oreal SA V eBay Int’l AG*, 2011 E.C.R. I-6011.

¹⁵⁸ Case C-324/09, *L’Oreal SA V eBay Int’l AG*, 2011 E.C.R. I-6011, para. 23.

¹⁵⁹ Case C-324/09, *L’Oreal SA V eBay Int’l AG*, 2011 E.C.R. I-6011 para. 141; CJEU, Opinion of Advocate General Jääskinen, case C-324/09, *L’Oreal v eBay International*, 9 December 2010, para. 181.

¹⁶⁰ *Delta TV v Google and YouTube* (2017) (Turin Court of First Instance); see also E. Rosati, “Italian court finds Google and YouTube liable for failing to remove unlicensed content (but confirms eligibility for safe harbour protection)” (IPKat, 20 April 2017) is available at <<http://ipkitten.blogspot.co.uk/2017/04/italian-court-finds-google-and-youtube.html>> last accessed at 16 December 2017.

that they expeditiously removed the illegal content upon receipt of a valid notification from the right holders. Interestingly, the Court of Torino handed down that, while YouTube was a hosting ISSP and thus is eligible to invoke the immunity provisions to be exonerated from liability as per Article 14 of the ECD, it took down the illegal videos and deterred the upload of further videos of similar kind only within the Italian borders and not worldwide. For this reason, the Court of Torino reached the conclusion that YouTube was secondarily liable for the unauthorized videos uploaded by its users since it did not remove and prevent further uploads of illicit content by users outside Italian jurisdiction.

In the light of the above, it seems that, from a utilitarian perspective, secondary liability rules to hosting ISSPs are justified due to their role as a source of deterrence. This understanding is supported by academic scholarship, policy and judicial authorities.

b. Gatekeepers as control points that identify the wrongdoings at a reasonable cost

It is not only the role of hosting ISSPs as a source of deterrence that warrants the ascription to them of a secondary liability framework. Indeed, as Kraakman acknowledges, gatekeepers can find wrongdoing at a reasonable cost.¹⁶¹ This means that hosting ISSPs can control and detect the online infringements at a reasonable cost; identifying illicit activity on their platforms faster and more efficiently than other parties, such as the right holders.¹⁶² This last-cost benefit understanding is supported by Levinson who argues that in the brick and mortar environment liability can be attributed to third parties that could identify wrongdoing more efficient. Transposing the last-cost benefit approach into the online context, it means that hosting ISSPs cannot only identify the primary wrongdoers that pass through their gates.¹⁶³ Rather, the imposition of liability rules might incentivize them to develop filtering-based technology that might reduce the transaction costs that

¹⁶¹ R. H. Kraakman, "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy" (1986) 2 *Journal of Law, Economics and Organization* 61; B. Martens, "JRC Technical Support reports: An economic policy perspective on online platforms" (2016) Institute for prospective technological studies digital economy working paper 34.

¹⁶² G. Frosio, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility" (2017) 25 *Oxford International Journal of Law and Information Technology* 5; see also W. Fisher, "CopyrightX: Lecture: Supplements to Copyright: Secondary Liability" (2014) 281 is available at < [http://copyx.org/files/2014/08/CopyrightX - Lecture Transcripts Book.pdf](http://copyx.org/files/2014/08/CopyrightX_-_Lecture_Transcripts_Book.pdf)> last accessed 20 May 2019.

¹⁶³ D. Levinson, "Collective sanctions" (2003) 56 *Stanford Law Review* 366 where he uses the example of last cost benefit approach in the context of child pornography.

would be generated by human review and achieve a higher degree of efficiency with regard to the removal of infringing content online.¹⁶⁴

This view is also shared by Lichtman and Posner.¹⁶⁵ Within the context of cyber-security, after a number of failed attempts by the American Government to battle cyber-crime, they posit that hosting ISSPs could control the malicious software and viruses that pass through the online gates. For this reason, they argue that hosting ISSPs might be in a better position than right holders to mitigate the increasing amount of malicious software while at the same time they could more easily identify primary infringer-users that disseminate the malicious software in the first place.¹⁶⁶ In similar fashion, Katyal argues that “ISPs could build software and hardware constraints into their systems” and therefore block internet users who attempt to access a website by using different credentials.¹⁶⁷ Along similar lines, in their influential paper, Mann and Belzley argue that the recent technological developments and the rapid advancement of knowledge of filtering means that filtering systems are now the cheapest tool to detect online wrongdoings more efficiently.¹⁶⁸ Therefore, it appears that hosting ISSPs could deploy such filtering mechanisms and thus terminate online infringements in a more efficient manner.

What is more, apart from the academic scholarship that views hosting ISSPs as the cheapest – cost avoiders, this last-cost benefit understanding has preoccupied the courts as well. For instance, in the case of *Cartier v Sky*,¹⁶⁹ Cartier brought legal proceedings against five main UK internet service providers and requested they terminate access to websites where fake copies of watches have been offered and sold to unsuspecting consumers. The English Court did not find that ISSPs that offered internet access to users were committing infringing acts, but it required them to block access to the particular

¹⁶⁴ Ibid, 367.

¹⁶⁵ D. Lichtman and E Posner, “Holding Internet Service Providers Accountable” (2006) 14 Supreme Court Economic Review 221-222.

¹⁶⁶ Ibid.

¹⁶⁷ N. K. Katyal, “Criminal Law in Cyberspace” (2001) 149 University of Pennsylvania Law Review 1097 where he argues that “ISPs could build software and hardware constraints into their systems. They may, for example, ensure that electronic traffic carries a specific source address consistent with the assigned address (a technique called egress filtering). ISPs might go further and only accept traffic from authorized sources (a technique called ingress filtering). Or ISPs could configure their systems to prevent subscribers from repeatedly trying to log in using different passwords.”

¹⁶⁸ R. J. Mann and S. R. Belzley, “The Promise of Internet Intermediary Liability” (2005) 47 William and Mary Law Review 268 who argue that “advances in information technology make it increasingly cost effective for intermediaries to monitor more closely the activities of those who use their networks.”

¹⁶⁹ *Cartier International AG v British Sky Broadcasting Ltd* [2016] ETMR 43 307, 377.

websites with illicit activity. This is because the Court considered that “it is economically more efficient” to request hosting ISSPs to deter the dissemination of counterfeit goods online than to enable brand owners to seek legal redress against the primary infringers.¹⁷⁰ This understanding means that ISPPs may be in a better position than right holders to mitigate the increasing number of intellectual property violations at the lowest cost.

On the basis of the above, it seems that the imposition of secondary liability framework to hosting ISPPs has been influenced by moral and utilitarian theories. Through the lens of those theories, a hosting ISSP can be seen either as morally liable due to its cooperation with the wrongdoings of its users, or from a utilitarian perspective, a hosting ISSP could be held liable since it is seen as a source of deterrence for online infringements in a less expensive manner. Such theoretical justifications might justify the choice of European policymakers to ascribe this specific liability regime to hosting ISPPs’ activities.

However, the ascription of secondary liability rules to hosting ISSPs is not backed up only by a theoretical framework. Indeed, policy and practical considerations reinforce the reasons that warrant the attribution of a liability regime in the form of secondary liability rules to hosting ISPPs. An examination of these considerations follows.

B. Policy and practical considerations for imposing a liability framework on hosting ISPPs in the form of secondary liability

From a policy perspective, the concept of imposing a liability framework in the form of secondary liability to hosting ISSPs rests on the premise of secondary regulation. Such concept was examined by Lessig in 1999 and stems from the idea that, by regulating hosting ISSPs, policymakers can control internet users’ behavior. According to Lessig, governments can control an individual’s conduct through four modalities, namely law, markets, architecture and norms.¹⁷¹ Lessig explains that, in the online world he treated the infrastructure of a hosting ISSP, or as he called it the code, as law.¹⁷² In this sense, he noted that if public authorities want to control internet users’ activities, they must regulate online services. This is because, being subject to secondary liability rules, hosting ISSPs may be incentivized to temper to a certain extent the dissemination of illegal

¹⁷⁰ *Cartier International AG v. British Sky Broadcasting Ltd* [2015] ETMR 1 para. 251; For an opposite view see M. Husovec, “Accountable, Not Liable: Injunctions Against Intermediaries” (2016) TILEC Discussion Paper 35-36; M Schellekens, “Liability of Internet Intermediaries: A Slippery Slope?” (2011) *SCRIPTed* 154.

¹⁷¹ L. Lessig, *Code and other Laws of cyberspace* (1999) 3, 88.

¹⁷² *Ibid.*

material either by terminating the access to websites with illicit activities or undertaking proactive measures, such as filter-based technology, in order to identify unwelcome content. This means that the negative impact of illicit behavior would be terminated or at least mitigated.

This view is supported by Balkin. According to him, the role of infrastructure can direct and control freedom of speech.¹⁷³ In order to clarify his view, Balkin draws parallels with the film industry and how films reach their audiences.¹⁷⁴ He notes that business organizations, contractual agreements, agents, actors and actresses, executive producers and directors, and other supporting entities cooperate before a film is distributed to the public.

This understanding could be equally applied to the digital ecosystem. So, in the online world, domain names, broadband networks, cloud companies, hosting ISSPs, merely transmit or cache information, advertising ISSPs and financial processors that form the infrastructure of the digital ecosystem cooperate in order to curb the dissemination of unlawful content. This implies that they decide which content is legitimate and non-legitimate, which information reaches the end-users, and how users can express their views. In this sense, the regulation of hosting ISSPs via indirect regulation may decisively influence end users' actions.¹⁷⁵

Furthermore, apart from the benefits of indirect regulation and its potential influence on internet users' behaviors, another policy reason that justifies the ascription of secondary liability framework to hosting ISSPs is the fact that an entity can escape from liability if it does not have knowledge of the illicit activity. For this reason, secondary liability framework has been endorsed for hosting ISSPs by the European policymakers. As discussed in Section IV of this chapter, the lack of knowledge is enshrined in Article 14 (1) of the ECD, which notes that hosting ISSPs are excluded from liability if they are not aware of the infringements that take place within their networks. This requirement of lack of knowledge was introduced in order to support e-commerce services, which were in an "embryonic and fragile"¹⁷⁶ stage back in 2000 when the ECD was finalized, and it still continues to apply in order to boost competitiveness and innovation within the Digital

¹⁷³ J. Balkin, "Old School/ new School speech regulation" (2014) 127 Harvard Law Review 2301.

¹⁷⁴ Ibid.

¹⁷⁵ A. Murray, *Information Technology Law* (Oxford University Press 2019) 62, 63.

¹⁷⁶ D. Friedmann, "Sinking the safe harbour with the legal certainty of strict liability in sight" (2014) 9 JIPLP 148

Single Market¹⁷⁷ as well as to provide a free space for exchanging information between internet users.¹⁷⁸

It is this requirement of lack of knowledge that has been used as a defense from hosting ISSPs in order to be exonerated from liability for intellectual property infringements that accrue within their networks. In this sense, by arguing lack of knowledge of the infringements online, hosting ISSPs can continue to operate their business without being afraid that the mere emergence of an online infringement within their network could amount to their liability. The defense of lack of knowledge has been seen as a shield of salvation from the pecuniary claims of content or brand owners and impede any disruption to the operation of their business model.

However, apart from the policy considerations that influence the imposition of secondary liability rules to hosting ISSPs, there are also other practical reasons. For instance, such reasons might be the difficulty to enforce intellectual property rights against primary infringers who are located in a foreign jurisdiction that provides a less favorable environment for enforcing intellectual property rights. Although courts can order the disclosure of the identity of the primary infringers,¹⁷⁹ the legal suit against them will not be reasonably practicable, as Riordan notes.¹⁸⁰ This is because the effectiveness of enforcing intellectual property rights is contingent upon the expenses of the enforcement procedure, the remedy for which the claimant has applied, and the recognition and enforcement of a foreign decision.¹⁸¹ Therefore, to turn against primary infringers might not be the ideal solution for right holders that mainly wish to compensate their losses from the violation of their intellectual property rights.

Moreover, another practical reason that justifies hosting ISSPs as the main target of right holders with regard to compensate their losses are their high revenues or as Angelopoulos

¹⁷⁷ G. Frosio, "Reforming Intermediary liability in the platform economy: a European Digital Single Market Strategy" (2017) 112 *Northwestern Law Review* 31.

¹⁷⁸ Joined Cases C-236/08, C-237/08 and C-238/08 of *Google France/Inc. v. Louis Vuitton Malletier* (2009) ECLI:EU:C:2009:569, para. 142 where the Advocate General notes that " To my mind, the aim of Directive 2000/31 is to create a free and open public domain on the internet. It seeks to do so by limiting the liability of those which transmit or store information, under its Articles 12 to 14, to instances where they were aware of an illegality."

¹⁷⁹ *Through Norwich Pharmacal orders*; see also *Golden Eye (International) Ltd and others v. Telefonica UK Ltd*, EWHC 723 (Ch) (2012).

¹⁸⁰ J. Riordan, *The liability of the internet intermediaries* (Oxford University Press 2016) 54.

¹⁸¹ A. Marsoof, *Internet intermediaries and Trade mark rights* (Routledge 2019) 6-7; D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 81-86; J. Riordan, *The liability of the internet intermediaries* (Oxford University Press 2016) 55-57.

aply points out “their deep pockets”.¹⁸² Undoubtedly, hosting ISSPs’ flourishing business model attracts the attention of rights holders.¹⁸³ This is because internet users, who are often the primary offenders, may not have the necessary assets to meet the compensatory expectations of intellectual property holders. In this regard, Facebook or YouTube, with annual incomes of approximately 27 billion dollars, seem more likely to compensate right holders in proportion to the harm triggered by their conduct.¹⁸⁴

What is more, another practical consideration that favors holding hosting ISSPs secondarily liable is the reputational harm that might arise if the right holders bring legal proceedings against individual internet users who have downloaded or uploaded unauthorized works.¹⁸⁵ For instance, in Europe, the French Government has been through severe public scrutiny and protests from civil society organizations with regard to the graduate response initiative aiming to fight music piracy.¹⁸⁶ According to this initiative, ISSPs that offer internet access to users must send up to three notifications to allegedly users-infringers. Lack of compliance with the notifications had resulted into harsh litigation proceedings against internet users. However, the picture of an average internet user who faces litigation procedures from multi-transnational music companies may cause feelings of sympathy and may lead to adverse reputation for the right holders.

Further, another practical reason that warrants the imposition of secondary liability rules to hosting ISSPs is the difficulty to identify the primary infringements. As Riordan remarked, right holders face discrepancies to seek redress against primary wrongdoers due to the fact that they usually hide behind their IP addresses and it is not easy to identify them.¹⁸⁷ Indeed, this understanding has already been outlined in the case of *L’Oreal v eBay*.¹⁸⁸ In this case, the Advocate General Jääskinen recognized that there may be cases

¹⁸² C. Angelopoulos, “Beyond the safe harbours: Harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 3 Intellectual Property Quarterly 253.

¹⁸³ N. Jondet, “The silver lining in Dailymotion’s copyright cloud” (2008) Juriscom. Net 2; see also Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011; Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644.

¹⁸⁴ “Facebook Reports Fourth Quarter and Full Year 2018 Results” is available at <<https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx>> last accessed 27 December 2019.

¹⁸⁵ J. Riordan, *The liability of the internet intermediaries* (Oxford University Press 2016) 57.

¹⁸⁶ P. De Filippi and D. Bourcier, “Three-Strikes’ Response to Copyright Infringement: The Case of Hadopi” in F. Musiani, D. Cogburn, L. DeNardis and N.S. Levinson (eds), *The Turn to Infrastructure in Internet Governance* (Palgrave-Macmillan 2016) 125; see also R. Giblin, *Code Wars: 10 Years of P2P software litigation* (Edward Elgar 2011) 2 where she gives the example of an undergraduate student who has been sued for downloading songs from file sharing platforms and has been fined with 675, 000 dollars in statutory damages.

¹⁸⁷ Footnote 50 in G. B. Dinwoodie, “Comparative analysis of the secondary liability of online service providers” in G.B. Dinwoodie (ed.) *Secondary liability of internet service providers* (Springer 2017).

¹⁸⁸ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011.

where “a third party is using the services of a hosting ISSP to infringe an intellectual property right, but the true identity of that infringer remains unknown.”¹⁸⁹ By contrast, right holders know hosting ISSPs’ establishments and therefore it is easier for them to turn against hosting ISSPs and pursue compensatory claims for their losses.

In short, one might conclude that within the policy context the rationale of imposing secondary liability rules on hosting ISSPs is warranted. Such rationale includes a plethora of reasons that are either based on the idea of secondary regulation as an instrument to influence internet users’ behaviors as well as on practicality and efficiency. Especially the latter reasons address cases where hosting ISSPs are targeted due to their high revenues, popularity and unknown domicile of primary infringers-users.

Having discussed the theoretical and policy considerations that warrant the imposition of a liability regime for hosting ISSPs in the form of secondary liability, the discussion now moves to the concept of secondary liability for copyright and trade mark infringements. Given that hosting ISSPs’ liability, as enshrined in the ECD, is a form of secondary liability, the following section provides a discussion of the peculiarities of secondary liability doctrine with regard to intellectual property infringements.

III. The concept of secondary liability for copyright and trademark infringements

In contrast to primary liability rules that penalize those actors who personally commit a tortious act, secondary liability is attributed to those actors who enable the commission of a wrongdoing by third parties.¹⁹⁰ Secondary infringement requires an act of primary infringement in order to take place. However, secondary liability may also be attributed to those involved in a wrongdoing, irrespective of the fact that it was not themselves carrying out the primary infringement.

Although in theory, there are distinctive lines between primary and secondary liability, in practice it seems that the concept of secondary liability is contingent upon primary

¹⁸⁹ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011, Opinion Jääskinen, para. 179.

¹⁹⁰ M. Sadeghi, “The Knowledge Standard for ISP Copyright and Trademark Secondary Liability: A Comparative Study on the Analysis of US and EU Laws” (Unpublished PhD thesis, 2013) 13; C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13-14; G.B. Dinwoodie, “A comparative analysis of the secondary liability of online service providers” in G.B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Springer 2016) 1; P. Davies, “Accessory liability for assisting torts” (2011) 70 *The Cambridge Law Journal* 353.

liability. Indeed, secondary liability is attached to the existence of a primary wrongdoing. As Lord Hoffman aptly pointed out there is “no secondary liability without primary liability”.¹⁹¹ This has been referred to as its parasitic or derivative nature.¹⁹² Right holders cannot substantiate secondary liability claims without a primary infringement. This means that a defendant can only be held liable for the harm, which is triggered by the primary tortious acts of a third person. Otherwise, if a primary wrongdoing does not take place, secondary liability claims lack a legal basis and thus cannot be invoked. Therefore, individuals who seek redress against secondary actors will not be compensated and thus legal uncertainty might arise.

What is more, a key difference between primary and secondary infringement is the mental element, in the sense that absence of knowledge of the wrongdoing can be a defence against allegations for secondary infringement. This defence has been extensively used by defendants in order to be exonerated from liability from secondary infringements in tort or intellectual property law. A representative example of this line of thinking can be found in the *L’Oréal v eBay* ruling¹⁹³ where L’Oréal brought legal proceedings against eBay alleging trade mark violation. In response to L’Oréal’s allegations, eBay claimed that it was not aware of the illicit activity within its platform and thus was eligible to the immunity provisions as set forth in Article 14 of the ECD.¹⁹⁴ In this way, by evoking the absence of knowledge, hosting ISSPs can be exonerated from secondary liability rules under the principles of tort law.

However, it seems that the concept of secondary liability under the principles of tort law is subject to a blurred understanding. As Davies describes it, secondary liability in tort is considered an “under-analyzed” area of law.¹⁹⁵ First, this is mainly because secondary liability in tort is seen as a new area of law.¹⁹⁶ In contrast to secondary liability in criminal

¹⁹¹ OBG, 31; J. Riordan, *The liability of the internet intermediaries* (Oxford University Press 2016) 70.

¹⁹² P. Davies, “Accessory liability: protecting intellectual property rights” (2011) *Intellectual Property Quarterly* 390; He notes that “Accessory liability is parasitic upon the commission of a primary wrong, so unless and until the purchasing and selling of such keywords is recognised, at least potentially, to be wrongful, there can be no accessory liability.”; *OBG Ltd and another v Allan and others Douglas and others v Hello! Ltd and others (No 3) Mainstream Properties Ltd v Young* [2007] UKHL 21 para. 31; Lord Hoffmann notes that “there could be no secondary liability without primary liability, and therefore a person could not be liable for inducing a breach of contract unless there had in fact been a breach by the contracting party”.

¹⁹³ *L’Oreal S.A v eBay International AG* [2009] EWHC 1094 (Ch).

¹⁹⁴ A. Rühmkorf, “eBay on the European Playing Field: A Comparative Case Analysis of *L’Oréal v eBay*” (2009) 6:3 *SCRIPTed* 685.

¹⁹⁵ P. Davies, “Accessory liability: protecting intellectual property rights” (2011) 4 *Intellectual Property Quarterly* 390.

¹⁹⁶ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13-14.

law, where secondary liability norms have been extensively used in the courts' legal arena in order to attribute criminal liability to the allegedly offenders¹⁹⁷ and are considered "well-established",¹⁹⁸ secondary liability in tort has been not well-developed.¹⁹⁹ This is probably because there have been very limited cases so far that preoccupied the courts with the ascription of secondary liability norms from a tort law perspective in the brick and mortar environment.²⁰⁰ For this reason, due to this limited applicability of secondary liability rules, the need to carve out clearly the concept of secondary liability in tort law theory and doctrine has been neglected.

Secondly, the blurred understanding of secondary liability in tort law relates to the miscellaneous definitions that have been attributed to secondary liability.²⁰¹ Although the concept of secondary liability remains the same, it has been interchangeably defined as accessory or vicarious liability or indirect liability or contributory liability. For instance, in the US legal system, instead of the broad term of secondary liability, the terms of vicarious or contributory liability are exclusively used. The former is about the defendant, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another"²⁰² while the latter emerges when the defendant "unfairly reaps the benefits of another's infringing behaviour"²⁰³ and "has the right and the ability to supervise the infringing activity and also has a direct financial interest in such activities."²⁰⁴ When it comes to the European level, there is no harmonised framework of tort law and policy. It is up to the laws of the various member states. EU member states use various definitions such as secondary liability, indirect liability, accessory liability or joint-tortfeasance.²⁰⁵ Whilst they are all subject to the same interpretation, i.e. the allocation of liability to an actor for the acts of a third party, it seems that some of the above-mentioned definitions treat the actor primary liable although her liability is

¹⁹⁷ G Williams, *Joints Torts and Contributory Negligence* (Stevens & Sons Ltd 1951) 11.

¹⁹⁸ P. Davies, "Accessory liability for assisting torts" (2011) 70 *The Cambridge Law Journal* 354.

¹⁹⁹ P. Birks, "Civil Wrongs: A New World" in *Butterworths Lectures 1990–1991* (1991) 55, 100; P. Birks considers secondary liability as an "obscure and under-theorized" area of law.

²⁰⁰ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13-14.

²⁰¹ J. Riordan, *The liability of internet intermediaries* (Oxford University Press 2016) 13.

²⁰² *Gershwin Publishing Corp v Columbia Artists Mgmt, Inc.* 443 F. 2d 1159, 1162 (2D Cir. 1971).

²⁰³ *Artists Music Inc. v Reed Publig., Inc.* 31 U.S.P.Q 623 (S.D.N.Y 1994).

²⁰⁴ *Fonovisa, Inc. v. Cherry Auction, Inc.* 76 F. 3d 259 (9th Cir. 1996).

²⁰⁵ J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (2018) 19-23; B. Martinet Farano, "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and US Approaches" (2012) TTLF Working Paper No 14 47.

secondary since it might arise if the primary infringement takes place.²⁰⁶ A telling example can be found in the UK joint-tortfeasance doctrine that treats joint-tortfeasors as equally liable next to the allegedly primary infringers.²⁰⁷ Further examination of different tortious secondary liability doctrines can be found in this chapter in Section IV. C.

Finally, the blurred understanding of secondary liability is aggravated by the lack of harmonisation of secondary liability at European level.²⁰⁸ Unlike primary liability rules which are harmonized, secondary liability rules in tort law do not fall under the umbrella of harmonisation. It is this lack of consensus at European level of the main elements of secondary liability rules that has led to the emergence of different doctrines at national jurisdictions. Such doctrines, as I outline with relevant case law in Section IV.C. of this chapter, include the joint-tortfeasance, authorisation, Stoererhaftung or disturber liability and civil liability.²⁰⁹ These might substantially differ from each other and thus give rise to legal uncertainty to right holders and defendants. For instance, in contrast to most EU national legal systems, the German legal system adopts the concept of disturber liability which excludes claims for damages and allows only injunctive relief. This comes in contrast with the system adopted in France where secondary infringers are subject to pecuniary claims, namely under Article 1382 of the French Civil Code which notes that “any act whatever of man, which causes damage to another, obliges the one by whose fault it occurred, to compensate it.”²¹⁰

²⁰⁶ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13; C. Angelopoulos notes that “these doctrines fail to identify cases of accessory liability as such, but instead formally categorise them as cases of primary liability, with the accessory treated either as a “joint tortfeasor”, who stands alongside the person who committed the material act of infringement as an equal principal in a single tort, or as the perpetrator, not of a participation in the wrong of somebody else, but of an independent act of negligence consisting of that participation”.

²⁰⁷ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13; *Football Dataco Ltd & Ors v Stan James Plc & Ors* [2013] EWCA Civ 27; *L’Oreal v eBay* [2009] EWHC 1094 (Ch).

²⁰⁸ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13; M. Leistner, “Structural aspects of secondary provider liability in Europe” (2014) 9 *Journal of Intellectual Property Law and Practice* 75; P. Davies, “Accessory liability: protecting intellectual property rights” (2011) *Intellectual Property Quarterly* 390; EU Commission, “Proposal on certain legal aspects of electronic commerce in the internal market” COM (1998) 12; Max Planck Institute for Intellectual Property and Competition Law Munich, “Study on the Overall Functioning of the European Trade Mark System” (2011) 213.

²⁰⁹ M. Leistner, “Structural aspects of secondary (provider) liability in Europe” (2014) 9 *Journal of Intellectual Property Law and Practice* 78; C. Angelopoulos, “Beyond safe harbours: harmonising substantive intermediary liability for copyright infringement in Europe” (2013) 3 *International Review of industrial property and copyright law* 262.

²¹⁰ Official translation of the French Civil Code is available at <file:///C:/Users/krokida/Downloads/Code_22.pdf> last accessed 27 December 2019.

In the midst of the uncertainty regarding a harmonised concept of secondary liability in tort or intellectual property law, the national examples discussed later on in this chapter will offer a clearer understanding of key aspects of the legal nature of secondary liability. Before entering this discussion, however, it is essential to establish how and why hosting ISSPs' liability is a form of secondary liability, according to the legislative framework set forth by the ECD. Such discussion is necessary to the extent that discrepancies and drawbacks in the definition of tortious secondary liability may also impact on the scope and meaning of hosting ISSPs' liability.

IV. Hosting ISSPs' liability as a form of secondary liability: Article 14 of the ECD and legal traditions of EU Member States

This section addresses the concept of hosting ISSPs liability under Article 14 of the ECD at European level, discusses the implementation of Article 14 of the ECD into the national legal systems of three representative EU member states as well as the liability of hosting ISSPs under the legal traditions of those three representative EU member states.

A. *Article 14 of the ECD: Concept of hosting ISSPs' liability*

ISSPs' liability is about holding hosting ISSPs liable for tortious acts committed by their users, notably acts of intellectual property infringements. It is set out in Article 14 of the ECD of 2000²¹¹ which states that a hosting ISSP can escape from liability if it does not have knowledge of the illicit activity or upon obtaining knowledge of the illicit activity to take down the infringing content. Hosting ISSPs' liability is established in a horizontal way²¹² and it can be defined, as noted by Dinwoodie, both from a "negative" and a "positive" perspective.²¹³

²¹¹ Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L 178 ; K. Parti and L. Marin, "Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content" (2013) 9 *Journal of Contemporary European Research* 149.

²¹² This means that it addresses all types of unlawful content. In contrast to its counterpart in the US legal system; See M. Peguera, "The DMCA Safe Harbors and their European Counterparts: a comparative analysis of some common problems" (2008) 32 *Colum. J.L. & Arts* 482; EU Commission, "First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)" COM (2003) 702 final 4.

²¹³ G.B. Dinwoodie, "Comparative analysis of the secondary liability of online service providers" in G.B. Dinwoodie (ed.) *Secondary liability of internet service providers* (Springer 2017) 19.

From the negative perspective, the definition of hosting ISSPs' liability is set out in the provisions of the ECD. As Angelopoulos points out, hosting ISSPs' liability is defined in the current legal framework in an "evasive, negative fashion, dictating only when Member States can't impose liability for intermediary activities, not when they can."²¹⁴ This means that the legal provisions determine only the conditions that shelter hosting ISSPs from liability and dictate what hosting ISSPs should not do in order to avoid liability. These legal provisions are known as immunity or safe harbor provisions. They are described by Husovec as "a conditional liability-free zone, in which you can move freely as long as you respect its predefined boundaries."²¹⁵

Effectively, what the provisions of the ECD do is to carve out the specific circumstances that trigger instances where hosting ISSPs are not liable. For instance, Articles 12 and 13 concern only the mere conduit and caching ISSPs accordingly and prescribe the specific conditions of exemptions from legal liability. Likewise, Article 14 of the ECD, which is relevant for this research, addresses the ISSPs that host material. In particular, it dictates that a hosting ISSP can avoid liability if it does not have actual knowledge of the illegal activity or takes down expeditiously the infringing material upon receiving a notification. In such cases, courts may rule out liability for the hosting ISSP to the extent that the conditions that grant immunity apply.

The "negative" understanding of hosting ISSPs' liability under Article 14 of the ECD has been upheld at the European level in a number of rulings. According to those cases, the absence of knowledge and the prompt removal of infringing content upon notification are used as defences against ISSPs' liability. Consider, for instance, the case of *L'Oreal v eBay*,²¹⁶ which was referred by the English High Court to CJEU in order to clarify the concept of knowledge as set forth in Article 14 (1) of the ECD. In this case, the Court clarified that the requirement of knowledge addresses the cases where a hosting ISPP is "aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1) (b) of Directive 2000/31".²¹⁷ In this sense, given that hosting ISPPs are not aware of the infringing content on the basis of a diligent economic operator, then they could evoke the

²¹⁴ C. Angelopoulos, "Beyond the safe harbors: harmonizing substantive intermediary liability for copyright infringement in Europe" (2013) 3 Intellectual Property Quarterly 254.

²¹⁵ M. Husovec, "Injunctions against intermediaries in the European Union: Accountable but not liable?" (Cambridge University Press 2017) 50.

²¹⁶ Case C-324/09, *L'Oreal SA V eBay Int'l AG* (2011) E.C.R. I-6011.

²¹⁷ Case C-324/09, *L'Oreal SA V eBay Int'l AG* (2011) E.C.R. I-6011, para. 120.

defense of absence of knowledge. The concept of the diligent economic operator will be thoroughly discussed in Section IV.B of this chapter.

Along similar lines, national courts have also held that hosting ISSPs could use the defense of absence of knowledge. A representative example can be found in *Audiencia Provincial Sentencia A.P.S. Madrid*²¹⁸ where the Spanish broadcaster Telecinco sued YouTube, alleging that YouTube's users were uploading unauthorized content on the video music platform.²¹⁹ Amidst the arguments in its defense line, YouTube claimed that it was not aware of the illicit activity and did not receive any notification with regard to the infringing nature of the content. In this way, YouTube evoked the lack of knowledge as set forth in Article 14 (1) of the ECD in order to escape from liability. Its allegations were further confirmed with the ruling from the Madrid Court of Appeals that held that YouTube cannot be held liable since the notifications that were sent by Telecinco do not entail removal requests for specific copyright infringements and thus do not fall into the scope of actual knowledge.²²⁰ Therefore, in this case YouTube was not liable because it lacked knowledge of the infringing content.

In similar fashion, the defense of prompt removal of infringing content upon being notified has been evoked in Belgium. More specifically, in the *Lancôme v eBay* case, Lancôme sued eBay for trade mark infringements.²²¹ eBay argued that it removed the pirate goods as soon as it was notified and thus it is eligible to evoke the defense of Article 14 (2) of the ECD which notes that "the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information." In response, Lancôme argued that eBay did not have a passive role towards the goods that were displayed on its platform. Rather, it had an active stance and exceeded its role as hosting provider.²²² For this reason, according to Lancôme's claims, eBay could not invoke

²¹⁸ *Audiencia Provincial Sentencia A.P.S. Madrid Jan* [2014] (Provincial Court Sentence).

²¹⁹ J. Halliday, "Google wins YouTube case in Spain Google wins case against Spanish broadcaster that claimed YouTube had damaged its business" (The Guardian, 23 September 2010) is available at <<https://www.theguardian.com/technology/2010/sep/23/google-wins-youtube-case-spain>> last accessed 17 May 2019.

²²⁰ M. Peguera, "Internet Service Providers' Liability in Spain: Recent Case Law and Future Perspectives" (2010) JIPITEC 159; M. Peguera, "Telecinco v. YouTube: the ruling in its context" (ISP liability, 26 September 2010) is available at <<https://ispliability.wordpress.com/2010/09/26/telecinco-v-youtube-the-ruling-in-its-context/>> last accessed 17 May 2019.

²²¹ *eBay v. Lancôme* [2008] Unreported (Brussels Commercial Court).

²²² A. Cheung and KH. Pun, "Comparative study on the liability for trade mark infringement of online auction providers" (2009) 31 European Intellectual Property Review 2; A. Bain, "Is it an infringement of trade mark law for the operator of an online marketplace (such as eBay) to allow counterfeit goods to be sold? As a matter of policy, should it be?" (2011) 33 European Intellectual Property Review 164.

the immunity provision of Article 14 of the ECD and had to be liable as per the general provisions of Belgian tort law. However, the Brussels Commercial Court accepted eBay's defense, according to which eBay acted expeditiously upon being notified about the illicit activity on its network, namely by verifying the validity of the request and subsequently removing the counterfeit goods from its platform.²²³ Such measures were considered realistic and efficient by the Belgian Court since eBay cooperated with the right holders in order to terminate the circulation of counterfeit goods that infringed Lancôme's rights.²²⁴ Hence, the Brussels court accepted eBay's defense to avoid liability pursuant to Article 14 (2) of the ECD.

In the light of the above, it is possible to observe that the ECD does not offer a definition of the concept of hosting ISSPs' liability. Rather, it offers specific requirements that outline how hosting ISSPs would avoid liability. Such requirements are used as defences by hosting ISSPs so that they could be eligible to immunity liability provisions under the ECD scheme. The absence of any definition of hosting ISSPs' liability at European level shifts the narrative to EU member states in order to identify how hosting ISSPs' liability could be defined. For this reason, the following section looks at the implementation of the requirements of the ECD in three selected EU jurisdictions, namely UK, Germany and France. The choice of these EU jurisdictions has been made on the basis that they are the most representative legal systems at European level, namely the civil and common law tradition respectively.

B. Hosting ISSPs' liability under the national implementation of Article 14 of the ECD into three selected EU member states: UK, Germany and France

This section examines the three selected EU member states implementation of the ECD. Following the rationale of the ECD, these EU member states refrain from defining what hosting ISSPs' liability concerns and dictate under which requirements hosting ISSPs can evade from liability, namely with the absence of knowledge and the expeditious removal of infringing content upon notification. What is more, these EU member states fail to offer

²²³ M. Rimmer, "Breakfast at Tiffany's": eBay Inc., Trade Mark Law and Counterfeiting" (2011) 21 Journal of Law, Information, and Science 150.

²²⁴ Ibid.

a solid interpretation of the requirements and thus triggering for hosting ISPPs legal uncertainty.

First, with regard to the “negative” understanding of hosting ISPPs’ liability, EU member states follow the rationale of the ECD and refrain from defining to what hosting ISPPs’ liability amounts. This “negative” understanding can be found in national laws that have been enacted for the purposes of implementing the ECD at national level. In the UK, the E-Commerce Regulations 2002/2013 were enacted in order to transpose the ECD onto national legal system. The English legal system followed verbatim the requirements set forth in Article 14 of the ECD, and Article 19 (a) of the E-Commerce Regulations 2002/2013 which notes that “the service provider (i) does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or (ii) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information...”.

Likewise, in the German legal system, the Telemediengesetz (TMG) was enacted for the purposes of implementing the provisions of the ECD. § 10 of TMG, which adopts the negative understanding of hosting ISPPs’ liability and dictates that a hosting ISPP can be exonerated from liability if it has “1. no knowledge of the illegal activity or the information and, as regards claims for damages, is not aware of any facts or circumstances from which the illegal activity or the information is apparent, or 2. upon obtaining such knowledge, have acted expeditiously to remove the information or to disable access to it.”²²⁵

In a similar fashion, in France, the Act on Confidence in Digital Economy (LCEN) has been enacted for implementing ECD provisions. So, Article 6 (4) of LCEN dictates that a hosting ISPP cannot be held liable if it has no knowledge of the illicit nature of the infringement, or no awareness of the facts and circumstances that would make the illicit nature of the

²²⁵ Telemediengesetz (TMG), English translation of the Telemediengesetz in Hunton Privacy blog is available at https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2016/02/Telemedia_Act_TMA_.pdf > last accessed 27 December 2019; In German § 10 TMG “Diensteanbieter sind für fremde Informationen, die sie für einen Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben.“

infringement apparent to the ISSP, or if it reacts expeditiously in order to remove the infringing information or terminate the access to it.²²⁶

Therefore, it appears that a definition of hosting ISSPs' liability cannot be found in the national laws of EU member states either since they refrain from engaging in the difficult task of conceptualizing hosting ISSPs' liability and reproducing the requirements of the ECD, which dictate the stances where hosting ISSPs cannot be held liable for the actions of their users.

However, the EU member states failed not only to offer a definition for hosting ISSPs' liability but also to provide a solid interpretation of the defences that hosting ISSPs have available to them in order to be exonerated from liability for intellectual property infringements.

Indeed, at European level the public consultation on the ECD in 2011 illustrated that there were inconsistent views among different stakeholders with regard to the correct exegesis of the requirement of knowledge.²²⁷ For instance, a number of stakeholders specified the notion of knowledge as when they receive the notification for the illegal material. Others think that a general awareness of the illicit content suffices to define actual knowledge while a more stringent opinion supports that only a court order can be considered as actual knowledge. Finally, hosting ISPPs subscribe to a broad notion of actual knowledge since this requires a general filtering obligation which is prohibited as per Article 15 of the ECD.²²⁸

This broad notion of actual knowledge is possible because, as Wang²²⁹ and Sadeghi²³⁰ point out, the ECD does not specify either the concept of knowledge of the illicit activity or the expeditious removal of infringing content and thus passes the tricky problem of interpretation of those requirements to EU member states. It is only with regard to the

²²⁶ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, French translation of Article 6 (4) of LCEN "...si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. » is available at <<https://wipolex.wipo.int/en/text/276258>> last accessed 27 December 2019.

²²⁷ EU Commission Staff Working Paper, "Online Services, Including E-Commerce, in the Single Market", SEC (2011) 1641 final 33-34.

²²⁸ Ibid.

²²⁹ J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 19-23.

²³⁰ M. Sadeghi, "The Knowledge Standard for ISP Copyright and Trademark Secondary Liability: A Comparative Study on the Analysis of US and EU Laws" (Unpublished PhD thesis 2013) 103.

concept of awareness to which the CJEU has given guidance and which amounts to the principle of diligence. In this light, in *L’Oreal v eBay*,²³¹ the CJEU has construed the requirement of awareness through the lens of diligence²³² and concluded that a hosting ISSP is not eligible to invoke the liability immunity provisions of Article 14 of the ECD if it is “aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1) (b) of Directive 2000/31”.²³³ In this respect, , the CJEU endorsed a subjective/objective standard which dictates that the hosting ISSP should be aware on its own of facts or circumstances from which the illegal activity comes and examine this behavior through the lens of a diligent economic operator.²³⁴

The notion of the diligent economic operator refers to the concept of a “reasonable person” which stems from the idea of “the ideal man”²³⁵ as elaborated in Aristotle’s work.²³⁶ It appeared for the first time in the legislative text of Digesta of Justinian in the Byzantine Empire in 533 AD where it was used to examine the liability of debtors.²³⁷ Since then, it has a broad application in all parts of law, but it is correlated mostly with tort law provisions.²³⁸ It describes the actions of a person who acts according to societal expectations and does not prioritize her needs against third parties’ interests.²³⁹ The concept of a reasonable person has been integrated in many different EU jurisdictions, such as the English, French, Spanish and German legal systems. As Kulesza notes “This standard corresponds with the practical *bonus pater familias* estimate, present in national systems of civil law.”²⁴⁰ For example, in English Law the reasonable man threshold is the “the man of ordinary prudence and intelligence”, in French Law “bon père de famille or

²³¹ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011.

²³² Acting in a certain standard of care.

²³³ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011, para. 120.

²³⁴ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 84-85; C. Riefa, *Consumer Protection and Online Auction Platforms: Towards a Safer Legal Framework* (Ashgate 2015) 198-201.

²³⁵ Σπουδαῖος ἀνὴρ.

²³⁶ J. Kochanowski, “The ‘reasonable man’ standards in continental law” (2007) *The Journal of Legislative studies* 1.

²³⁷ *Ibid.*

²³⁸ J. Gardner, “The Many Faces of the Reasonable Person” (2015) *Law Quarterly Review* 2 is available at <https://www.law.nyu.edu/sites/default/files/upload_documents/The%20Many%20Faces%20of%20the%20Reasonable%20Person.pdf> last accessed 27 December 2019.

²³⁹ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 297-299 where she notes that “it stems from the Roman term of “bonus pater familias» that is translated as the good father of the family who acts with prudence and diligence after taking into consideration the outcomes of his actions for the others”;

²⁴⁰ J. Kulesza, “Due diligence in International Internet Law” (2014) *Journal of Internet Law* 28.

homme raisonnable et avisé”, in Spanish Law “Buen padre di familia”, and in German Law “a sorgfältiger Mensch von durchschnittlicher Umsicht und Tüchtigkeit.”²⁴¹

Therefore, the idea behind the introduction of a subjective/objective threshold test for knowledge was mainly to give courts proper guidance on how to understand the requirement of knowledge with reference to a well-established principle of a reasonable person.²⁴² In this regard, a hosting ISSP must on his own assess the illegality of an activity which becomes apparent to a diligent economic operator. This is why Angelopoulos comments that the objective/subjective test seems to “provide the most logical answer consistent with the usual legal patterns governing such issues.”²⁴³

Yet, in the context of online infringements the application of the diligent economic operator standard could be problematic.²⁴⁴ This is mainly due to the lack of a uniform interpretation of the concept of diligence. This means that the notion of diligence could be construed following industry’s practices and standards.²⁴⁵ Such practices and methods, however, might be defined between industry representatives and hosting ISSPs and therefore be biased towards the interests of rights holders and hosting ISSPs, thus undermining users’ interests.²⁴⁶

Further, the notion of diligence is not harmonized at European level and national jurisdictions across member states construe the term of diligence in a different way.²⁴⁷ As Synodinou notes “the standards of duty of care imposed by national courts continue to

²⁴¹ ²⁴¹ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 297-299; C. Van Dam, *European Tort Law* (Oxford University Press 2007) 231-232.

²⁴² C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 84-85; J. Wang, *Regulating Hosting ISPs’ responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 19-23.

²⁴³ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 84-85.

²⁴⁴ T. Synodinou, “Intermediaries’ Liability for Online Copyright Infringement in the EU: Evolutions and Confusions” (2015) 31 *Computer Law & Security Review* 57.

²⁴⁵ B. Sander, “Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation” (2020) 43 *Fordham International Law Journal* 939; U. Carsten, “Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective” (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 114.

²⁴⁶ S. Jacques, K. Garstka, M. Hviid and J. Street, John, “Automated anti-piracy systems as copyright enforcement mechanism: a need to consider cultural diversity” (2018) 40 *European Intellectual Property Review* 218; E. Rosati, “Public Lecture on Copyright and the Court of Justice of the European Union: Role, Action, Legacy” (27 February 2019) University of Reading, Reading (UK).

²⁴⁷ J. Kulesza, “Due diligence in International Internet Law” (2014) *Journal of Internet Law* 28; C. Angelopoulos, “Beyond safe harbors: Harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 2013 *Intellectual Property Quarterly* 13.

differ significantly from jurisdiction to jurisdiction.”²⁴⁸ For example, in France a diligent hosting ISSP must act after being notified of the illicit activity or when it has reasonable doubts that an unlawful content has been transmitted via its network²⁴⁹ while in Germany, the notion of diligence is attributed to anyone whose actions can impinge upon others’ rights and interests.²⁵⁰ Hence, this implies that the CJEU gives leeway for EU national courts to construe the notion of diligent economic operator, with a potential risk of fragmented interpretations across the European borders.

In this light, and in the absence of any clear guidance, it appears that these defences have been the subject of heterogenous interpretations in EU jurisdictions.²⁵¹ This means that each EU member state has endorsed its own interpretation regarding the requirements of knowledge and expeditious removal of infringing content upon notification. Indicative examples of these interpretations are presented below.

i. UK: E-Commerce Regulations 2002/2013

With regard to the requirement of knowledge, it has been argued that a hosting ISSP obtains knowledge of the infringing content only via a competent notice.²⁵² What amounts to a competent notice can be found in Article 22 of the E-Commerce Regulations 2002/2013²⁵³ which states that a competent notice must include the name and address of the sender of the notice, the location of the information and the unlawful nature of the activity.

This implies that a notice must include evidence of the illegality of the activity. Indeed, in the *Tamiz case*,²⁵⁴ the claimant brought legal proceedings against a blog where

²⁴⁸ T. Synodinou, “Intermediaries’ Liability for Online Copyright Infringement in the EU: Evolutions and Confusions” (2015) 31 Computer Law & Security Review 65.

²⁴⁹ C. Angelopoulos, “Beyond safe harbors: Harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 2013 Intellectual Property Quarterly 11; *Madame L. c/ les sociétés Multimania* (1999) (Tribunal de Grande Instance de Nanterre).

²⁵⁰ C. Angelopoulos, “Beyond safe harbors: Harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 2013 Intellectual Property Quarterly 13.

²⁵¹ EU Commission, “Overview of the legal framework of notice and action procedures in Member States SMART 2016/0039” (2018) 2-3; L. Essers, “German, French Courts Disagree on Responsibility of ISPs for Illegal Content” (PCWorld, 16 July 2012) is available at <https://www.pcworld.com/article/259294/germany_french_courts_disagree_on_responsibility_of_isps_for_illegal_content.html> last accessed 27 December 2019.

²⁵² With regard to the threshold criteria for awareness, English courts remain silent and thus no comprehensive interpretation of the concept of awareness exists until now see in J. Wang, *Regulating Hosting ISPs’ responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 23.

²⁵³ E-Commerce Regulations 2002/2013 is available at <<http://www.legislation.gov.uk/uksi/2002/2013/contents/made>> last accessed 27 December 2019.

²⁵⁴ *Tamiz v Google* (2012) EWHC 449 (QB).

defamatory comments about him were posted by users. Yet, in order to attribute liability to the blog, the English Court held that a complaint sent from the claimant regarding content posted on a blog does not constitute a notice. As Eady Justice noted "Liability may turn upon the extent to which the relevant ISP entity has knowledge of the words complained of, and of their illegality or potential illegality."²⁵⁵ Rather, the illegal nature of the content must be outlined in the notice.

However, the infringing nature of the content must not rely on general statements of unlawfulness. Rather, it must be demonstrated through specific acts. A representative line of such thinking can be found in *Bunt v Tilley and others*.²⁵⁶ In this case, the claimant sued a number of individuals and the hosting ISSP for libel comments on a chat room. After a careful consideration of the facts, Eady Justice did not find the hosting ISSP liable since as he noted the notice about defamatory content, which has been sent to the ISSP from the claimant, did not fulfil the conditions for a competent notice as per Article 22 of the E-Commerce Regulations 2002/2013. The notice did not include the location of the defamatory comment and the illicit nature of the activity.²⁵⁷ For this reason, the ISSP could not be held liable. Along similar lines, in *Newzbin II*,²⁵⁸ which was unauthorized file-sharing platform, Arnold Justice stated that in order to find a file-sharing platform liable for copyright infringements within its network, actual knowledge of a specific infringement is required. Otherwise, notices that do not entail specific acts of infringements, such as specific URLs with the illegal content, would be dismissed by courts.

What is more, in the English legal system there is a debate on the ways that could generate the notice for infringing content, namely whether it should be an automatic or a human-based notification. The prevailing view leans in favour of a human-based approach. Indeed, in *McGrath v Dawkins and Amazon*,²⁵⁹ a bookseller brought legal proceedings

²⁵⁵ *Tamiz v Google* (2012) EWHC 449 (QB) para. 33.

²⁵⁶ *Bunt v Tilley and others* (2006) EWHC 407 (QB) para. 72.

²⁵⁷ *Bunt v Tilley and others* (2006) EWHC 407 (QB) para. 70 which notes that "In determining whether a service provider has actual knowledge for the purposes of regulations 18(b)(v) and 19(a)(i), a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, among other things, shall have regard to - (a) whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and (b) the extent to which any notice includes -(i) the full name and address of the sender of the notice; (ii) details of the location of the information in question; and (iii) details of the unlawful nature of the activity or information in question."

²⁵⁸ *Twentieth Century Fox Film Corporation v British Telecommunications Plc* (2011) EWHC 1981 (Ch) para. 126.

²⁵⁹ *McGrath v Dawkins and Amazon* (2012) EWHC B3 (QB).

against Amazon for the posting of defamatory comments on the review of a book. In order to determine whether there was a competent notice to Amazon concerning the defamatory comments, HHG Moloney QC stated that “A corporation can have actual knowledge only through a human representative, and given the vast size and diverse nature of Amazon's website there is no reason to suppose that anyone in Amazon was actually aware of these postings, let alone of their possible unlawfulness.”²⁶⁰ This understanding excludes any possibility for Amazon to identify on its own any defamatory comments and thus reinforces the view that a notice must be triggered by human providers.

Yet, apart from the defence of the absence of knowledge, Article 19 (a) (ii) of the E-Commerce Regulations 2002/2013 states that a hosting ISSP can be exonerated from liability if “upon obtaining such knowledge or awareness, [it] acts expeditiously to remove or to disable access to the information.” What amounts to expeditious removal, however, has been subject to different interpretations. On the one hand, it has been argued that expeditious removal is about the sole act of removing the allegedly infringing content while others claim that it extends to additional measures that impede the re-emergence of the allegedly infringing content within the network.

Insofar as the sole act of taking down the allegedly infringing content is concerned, the E-Commerce Regulations 2002/2013 refrain from specifying the timeframe within which an ISSP must remove the content after being notified. In contrast, with regard to the additional steps of hosting ISSPs to prevent the re-emergence of infringing content, guidance has been provided by the English High Court in *Twentieth Century Fox et al. v. British Telecommunications*.²⁶¹ The English High Court ordered UK internet access ISSPs to terminate the access of users to Newzbin2, a website that indexed and made available unauthorized works to its users. British Telecommunications argued that it was devoid of actual knowledge of the infringements that took place on its network and that a blocking injunction should not be allowed because it constituted a general monitoring obligation. After careful consideration of the facts, Arnold Justice noted that terminating the access to a specific website does not amount to general monitoring obligation since it does not

²⁶⁰ *McGrath v Dawkins and Amazon* (2012) EWHC B3 (QB) para. 42.

²⁶¹ *Twentieth Century Fox et al. v. British Telecommunications PLC* (2010) EWHC 608 (Ch).

require “detailed inspection of the data of any BT’s subscribers.”²⁶² Rather, it is a blocking order based on the specific case and solely aims to address the targeted URLs.²⁶³

Accordingly, it seems that UK transposed verbatim Article 14 of the ECD into its national legal system and thus fail to define hosting ISSPs’ liability. At the same time, there is lack of judicial guidance as to how the defences that hosting ISSPs use in order to escape from liability shall be construed.

ii. *Germany: Telemediengesetz*

In Germany, ECD provisions were transposed verbatim into the national legal system with the Telemediengesetz (TMG). This implies that German law follows the rationale of the ECD and does not define the liability of hosting ISSPs. Rather, it provides defences to hosting ISSPs in order to be exonerated from liability for infringements that take place online. However, it must be noted that TMG uses the term of knowledge instead of actual knowledge which is used in Article 14 of the ECD.²⁶⁴

In this light, as per § 10 TMG, the hosting ISSP must not have knowledge of the illegal act or of the information in order to be exonerated from liability. Any negligent ignorance or conditional intent or general awareness do not fall into the scope of the concept of knowledge.²⁶⁵ Rather, the concept of knowledge is about the knowledge of the specific infringement.²⁶⁶ This means that an ISSP can escape liability only if the hosting ISSP demonstrates that it lacks knowledge of the particular violation that took place within its platform.

Yet, in the German legal system, the concept of knowledge of hosting ISSPs has been the subject of different interpretations, which is enshrined in § 10 TMG and reads as follows: “the hosting ISSP avoids liability if it does not have knowledge of the illegal act or information.” On the one hand, many scholars argue that knowledge revolves around the illegality of the act and not the information itself.²⁶⁷ This means that the court focus on

²⁶² *Twentieth Century Fox et al. v. British Telecommunications PLC* (2011) EWHC 1981 (Ch) para. 162.

²⁶³ *Twentieth Century Fox et al. v. British Telecommunications PLC* (2011) EWHC 1981 (Ch) para. 70; Arnold Justice recommended the adoption of Cleanfeed, which is a filtering technology, and which has proved to be technically feasible and not easily circumvented by users.

²⁶⁴ T. Verbiest and others, “Study on the liability of internet intermediaries” (2007) 34 is available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2575069> last accessed 22 August 2019.

²⁶⁵ *Ibid*, 35-36.

²⁶⁶ *Ibid*, 35-36.

²⁶⁷ For the debate see J. Wang, *Regulating Hosting ISPs’ responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 96.

the illegal conduct such as the unauthorized file-sharing or downloading and not on the unauthorized copy of a film, book or a song which is made available online.²⁶⁸ On the other hand, other scholars claim that the hosting ISSP must not have knowledge both of the illegal conduct and the illegal information.²⁶⁹ However, it was not until 2010 in the *Vorschaubilder* rulings, which concerned the downloading of unauthorized photographs,²⁷⁰ when the German Supreme Court clarified that the hosting ISSP must have knowledge of the illegal nature of the information and thus undertake the appropriate measures to terminate its dissemination.²⁷¹

Further, with regard to the concepts of awareness and the diligent economic operator, there is no further guidance by German case law.²⁷²

What is more, as far as the second defence of expeditious removal of infringing content upon notification is concerned, it has been subject to different interpretations. Similar to the approach in the English legal system, the removal of infringing content upon the hosting ISSP being notified can be construed either as a sole act of removal or a prevention of an infringement. First, TMG does not include any provision that addresses the timeframe within which the infringing content must be removed by the ISSP. By contrast, it is only recently with the Social Networks Act that hosting ISPPs are required to remove the allegedly infringing content upon being notified according to the degree of severity of the infringement.²⁷³ For instance, they must take down within 24 hours any blatantly illegal content while a timeline of 7 days is provided in cases of unlawful content.²⁷⁴

As far as the prevention of infringements is concerned, the German legal system endorses the theory of the same nature of infringement, commonly known as *Kerntheorie*, which

²⁶⁸ G. Spindler, *Recht der elektronischen Medien: Kommentar* (3rd edition) para. 1531; G. Spindler in Spindler and Wiebe (eds.), *Internet Aktionen und Elektronische Marktplätze* (2004) Chapter 6.

²⁶⁹ J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 97.

²⁷⁰ Bundesgerichtshof, *Vorschaubilder III*, 21. September 2017 - I ZR 11/16.

²⁷¹ *Ibid.*

²⁷² T. Verbiest and others, "Study on the liability of internet intermediaries" (2007) 36.

²⁷³ G. Spindler, "Internet Intermediary Liability Reloaded: The new German act on Responsibility of Social Networks and its (In-) compatibility with European Law" (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 166; H. Tworek and P. Leerssen, "An Analysis of Germany's NetzDG Law" (2019) *Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression 1* is available at <https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf> last accessed 27 December 2019.

²⁷⁴ G. Spindler, "Internet Intermediary Liability Reloaded: The new German act on Responsibility of Social Networks and its (In-) compatibility with European Law" (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 166.

concerns the imposition of duty of care on hosting ISSPs with regard to infringements of the same nature.²⁷⁵ According to this theory, hosting ISSPs must prevent the reappearance of similar infringements through the use of monitoring technology. Similar infringements can be subject to different interpretations. For instance, they can either be described as those infringements that violate the same work but with a copy in another file or those infringements that fall into the same category and are committed by the same infringer user.²⁷⁶

Interestingly, the application of *Kerntheorie* which was enshrined in the *Internetversteigerung I*²⁷⁷ case was reaffirmed by the following court rulings of *Internetversteigerung II*²⁷⁸ and *Internetversteigerung III*²⁷⁹ as well as the *Rapidshare II*²⁸⁰ ruling in 2010. In the latter case, the Hamburg Court of First Instance examined the dispute between Rapidshare, a hosting ISSP and copyright holders. According to the line of reasoning, Rapidshare was providing financial benefits to its subscribers with a view to upload highly demanded files and increase website's traffic. For this reason, the Hamburg Court noted that the deletion only of infringing links that directed to files upon notification was not an adequate reaction. Rather, the operator of the website was under an obligation to detect and take down any future links of the same kind. In this way, the adequate reaction of a hosting ISSP upon notification could be extended to specific monitoring duties in reference to infringing material or illicit activities that had already been notified.

However, it has been argued that the application of *Kerntheorie* might be in conflict with Article 15 of the ECD,²⁸¹ which notes that hosting ISSPs are not obliged to deploy general monitoring obligations within their networks. In addition, an array of court rulings at European level have rejected the imposition of general monitoring obligations. Consider,

²⁷⁵ M. Leistner, "Störerhaftung und mittelbare Schutzrechtsverletzung" (2010) GRUR-Beil 1; T. Verbiest and others, "Study on the liability of internet intermediaries" (2007) 51.

²⁷⁶ J. B. Nordemann, "Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach" (2011) 2 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 37.

²⁷⁷ Bundesgerichtshof, *Internetversteigerung I*, 11 March 2004, I ZR 304/01.

²⁷⁸ Bundesgerichtshof, *Internetversteigerung II*, 19 April 2007, I ZR 35/04.

²⁷⁹ Bundesgerichtshof, *Internetversteigerung III*, 30 April 2008, I ZR 73/05.

²⁸⁰ Oberlandesgericht Düsseldorf, *Rapidshare I*, 27 April 2010, I-20 U 166/09.

²⁸¹ T. Hoeren and S. Yankova, "The Liability of Internet Intermediaries – The German Perspective" (2012) International Review of Intellectual Property and Competition Law (IIC) 501.

for instance, the case of *Scarlet v Sabam*.²⁸² In this case, Sabam, which is the Belgian association for authors, requested a filtering injunction against Scarlet, an internet access ISSP, alleging copyright infringement. Sabam argued that Scarlet's subscribers use its network in order to file-share unauthorized material peer to peer. However, the Court refused to issue an injunction under the reasoning that the imposition of a filtering obligation would "oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31."²⁸³

Such a stance was maintained in *Netlog v Sabam* where the CJEU rejected for a second time the application to order a filtering injunction.²⁸⁴ In this case, Sabam requested a filtering injunction against Netlog, a social network platform, alleging copyright infringements. Sabam argued that Netlog's users uploaded unauthorized material on the platform such as films and songs, from its film repository. Yet, drawing parallels with the *Scarlet v Sabam* ruling, CJEU refrained from issuing a filtering injunction under the basis of "the injunction imposed on the hosting service provider requiring it to install the contested filtering system would oblige it to actively monitor almost all the data relating to all of its service users in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the hosting service provider to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31 (see, by analogy, *Scarlet Extended*, paragraph 40)."²⁸⁵

Along similar lines, in the *McFadden* ruling, a dispute between the owner of a wifi connection that does not require a password to access internet and Sony Music,²⁸⁶ the CJEU delivered that "monitoring all of the information transmitted, such a measure must be excluded from the outset as contrary to Article 15(1) of Directive 2000/31, which

²⁸² Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

²⁸³ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 36.

²⁸⁴ Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85.

²⁸⁵ Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85, para. 38.

²⁸⁶ Case C-484/14 - *Mc Fadden* (2016) ECLI:EU:C: 2016:689.

excludes the imposition of a general obligation on, inter alia, communication network access providers to monitor the information that they transmit.”²⁸⁷

Therefore, similar to the transposition of the ECD in the English legal system, TMG fails to define the hosting ISSPs’ liability and does not provide adequate guidance to the existing defences that exonerate hosting ISSPs from liability for violations that take place within their networks.

iii. *France: Act on Confidence in Digital Economy*

The provisions of the ECD have been transposed verbatim in the French legal system with the Act on Confidence in Digital Economy, known as LCEN Law.²⁸⁸ So, similar to the English and German Laws, LCEN provides hosting ISSPs with defences which enable them to be exonerated from liability for infringements within their networks. As per Article 6-I-2 of LCEN, a hosting ISSP is not liable if it does not have knowledge of the illegal nature of the stored data or the facts and circumstances that indicate the illegal nature of the data.²⁸⁹ Knowledge can only be obtained if the hosting ISSP receives a competent notice.²⁹⁰ The requirements of a competent notice are set forth in Article 6 I (5) of LCEN which dictates that the notice must include the date of notification, the identity of the sender, the name and the address of the recipient, the infringing material and a written evidence of communication between the sender and the recipient outlining the infringement and the request for removal.²⁹¹

²⁸⁷ Case C-484/14 - *Mc Fadden* (2016) ECLI:EU:C: 2016:689, para. 87.

²⁸⁸ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique is available at <<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT00000801164&dateTexte=&categorieLi=en=id>> last accessed 27 December 2019.

²⁸⁹ Article 6-I-2 of LCEN “Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.”; J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 97; S. Nerisson, “Intellectual Property Liability of Consumers, Facilitators and Intermediaries: The Position in France” in A. Kamperman Sanders and C. Heath (eds.), *Intellectual Property Liability of Consumers, Facilitators and Intermediaries* (Kluwer Law International 2012) 70.

²⁹⁰ J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 98.

²⁹¹ Article 6-I-5 of LCEN “La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants :

- la date de la notification ;

This understanding has been reinforced by several rulings where it has been concluded that a notice must entail precise information about the allegedly infringing content as well as detailed information about senders and recipients of the notice. For instance, in the case of *Nord-Ouest v. Dailymotion*,²⁹² the French Supreme Court handed down that the notice must not include a general statement about an unauthorized video on the online network. Rather, it must entail the precise location of the allegedly infringing video, such as the URLs, so that the hosting ISSP can effectively identify the unlawful content and thus remove it.

However, apart from the notice which can trigger knowledge of the hosting ISSP, another interpretation of the knowledge requirement can be found in the principle of the diligent economic operator. This principle was endorsed at European level in the case of *L’Oreal v eBay*.²⁹³ As explained in Section IV. A of this chapter, in this case the CJEU offered guidance on the interpretation of the requirement of knowledge by equating an ISSP with a diligent economic operator. This means that if a diligent economic operator could be aware of an illicit activity within its business model, an ISSP could also be aware of the infringing content or counterfeit goods that are disseminated via its network.

In this vein, French courts were the first to apply this principle in the ruling of *LVHM V eBay*.²⁹⁴ In this case, *LVHM* brought legal proceedings against the online market platform eBay on the basis of trademark violations. The Paris Court of First Instance ruled that eBay was liable for the trademark infringements which occurred on its platform since it had knowledge of the counterfeit goods. This is because eBay acted as a brokerage site and exercise commercial activity by sending notices to its users about upcoming offers. It is its commercial activity that cannot demonstrate but knowledge and control of the goods that have been circulated within its platform.²⁹⁵ Therefore, by virtue of its business model, the

- si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;

- les nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;
- la description des faits litigieux et leur localisation précise ;

- les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;

- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.”; T. Verbiest and others, “Study on the liability of internet intermediaries” (2007) 46.

²⁹² *Nord Ouest Production et al v. Dailymotion, UGC Images* (2011) (Cour de Cassation).

²⁹³ *Case C-324/09, L’Oreal SA V eBay Int’l AG* [2011] E.C.R. I-6011.

²⁹⁴ *LVHM v eBay* (2008) (Commercial Court of Paris).

²⁹⁵ *LVHM v eBay* (2008) (Commercial Court of Paris); see also J. de Chavez, "Building a Trademark Safe Harbor for Contributory Counterfeiting Liability After Tiffany v. eBay," (2012) 86 St. John's Law Review 267.

French judges thought that eBay should have stopped the distribution of counterfeit goods by either checking the originality of the products which were on sale or shutting down any seller's account who has been found liable for offering fake goods or removing any displacement of illegal goods upon notification.²⁹⁶

With regard to the expeditious removal of infringing content upon notification, LCEN remains silent. Further guidance has been given by French courts which offered different timeframes for the removal of infringing content.²⁹⁷ For example, in *TF1 v YouTube*²⁹⁸ the Court of First Instance in Paris concluded that YouTube was not eligible to the defence of Article 14 of the ECD since the removal of the infringing video 5 days after notification did not amount to expeditious removal. For this reason, YouTube was held liable for not removing in a reasonable period of time the unauthorized video. In a similar fashion, in *TF1 v. Dailymotion*²⁹⁹ the Court of Appeal in Paris sanctioned Dailymotion for a late take down of infringing content upon being notified. Although the Court noted that Dailymotion qualifies as hosting ISSP under Article 14 of the ECD, it then concluded that the removal of the allegedly infringing video 4 days after notification did not exclude Dailymotion from being liable as per Article 14 (1) of the ECD.

What is more, similar to English and German courts, French courts have extended the removal of infringing content to the prevention of emergence of similar infringements within online platforms. Indicative examples can be found in an array of court rulings. For instance, in the case of *Andre Rau v Google and Aufeminin.com*³⁰⁰ the Court of Appeal in Paris held that Google not only had an obligation to remove the infringing content upon

²⁹⁶ See in B. Martinet Farano, "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and US Approaches" (2012) TTLF Working Paper No 14 89-90 where the author notes that eBay was required to "supply the sellers, upon request, the purchase invoice or a certificate of authenticity of the products offered for sale, in sanctioning any guilty vendor by finally terminating his account as soon as the breach is ascertained, in immediately withdrawing any illicit advertisements notified by the departments of LOUIS VUITTON MALLETTIER in charge of combating infringement."

²⁹⁷ J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 168.

²⁹⁸ *TF1 v YouTube* [2012] (Court of First Instance Paris); C. Jasserand, "France -Youtube guilty but not liable? some more precisions on the status of hosting providers" (Kluwer copyright blog, 18 June 2012) is available at <<http://copyrightblog.kluweriplaw.com/2012/06/18/france-youtube-guilty-but-not-liable-some-more-precisions-on-the-status-of-hosting-providers/>> last accessed 27 December 2019; J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 168.

²⁹⁹ *TF1 v Dailymotion* [2014] (Court of Appeal Paris); C. Jasserand, "France- Dailymotion heavily fined for the late removal of infringing content" (Kluwer copyright blog, 18 September 2012) is available at <<http://copyrightblog.kluweriplaw.com/2012/09/28/france-dailymotion-heavily-fined-for-the-late-removal-of-infringing-content/>> last accessed 27 December 2019; J. Wang, *Regulating Hosting ISPs' responsibilities for Copyright Infringement: The freedom to operate in the US, EU and China* (Springer 2018) 168.

³⁰⁰ *André Rau v. Google and Aufeminin.com* [2011] (Court of Appeal Paris).

notification, but it also had the duty to take all the appropriate measures and thus impede the re-emergence of the same infringements online.³⁰¹

Along similar lines, in *Zadig Productions v Google video*³⁰² the Paris Court of First Instance held Google liable for not undertaking the appropriate measures to terminate any further dissemination of the unauthorized video. Although the Court acknowledged Google's expeditious response to remove the unauthorized video of "Tranquillity Bay" upon receiving a complaint, Google failed to deploy technological mechanisms that could prevent the re-uploading of the video.³⁰³ It is this omission of preventing the emergence of similar infringements that obliged Google to pay damages to Zadig Productions, the owners of the "Tranquillity Bay" video.

Overall, it appears that LCEN follows verbatim the provisions of the ECD and does not define ISSPs' liability. By contrast, it offers defences for ISSPs to use in order to escape from liability. However, the interpretation of these defences seems to be examined on a case by case basis by courts and thus offers legal uncertainty to right holders and hosting ISSPs.

In the light of the above, it seems that the national implementation of the ECD does not offer answers to the hosting ISSPs' liability conundrum. This is because, as presented above, the national implementation of the ECD in the EU member states fails to provide a definition for hosting ISSPs' liability while at the same time it also fails to give concrete guidance with regard to the interpretation of the defences that hosting ISSPs use in order to be exonerated from liability.

For this reason, national courts turn to their national tort law theories and doctrines in order to define hosting ISSPs' liability in the form of secondary liability rules in tort law. Yet, while the EU member states could offer a definition of hosting ISSPs' liability, they

³⁰¹ Jurisprudence sur la communication en ligne is available at <https://wiki.laquadrature.net/Jurisprudence_sur_la_communication_en_ligne#--Cour_d.27appel_de_Paris.2C_4_f.C3.A9vrier_2011.2C_Andr.C3.A9_Rau_c.2F_Google_.26_AuFeminin.com> last accessed 27 December 2019.

³⁰² *SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud c. Sté Google Inc. et AFA* [2007] (Court of First Instance Paris).

³⁰³ YS Avocats, "Google Video held liable for not doing all it could to stop the broadcasting of a film" (20 November 2007) is available at <<http://copyrightfrance.blogspot.com/2007/11/google-video-held-liable-for-not-doing.html>> last accessed 27 December 2019.

seem to differ from each other. What is more, in many stances it seems challenging for EU national courts to fit tortious secondary liability rules into hosting ISPPs' activities.

Against this background, the following section offers a critical examination of the legal traditions of three selected jurisdictions. It identifies the key aspects of the legal nature of secondary liability rules and thus provides an understanding of the difficulties not only of harmonizing secondary liability rules at European level but also the underlying challenges for EU national jurisdictions to impose secondary liability rules to hosting ISSPs' activities.

C. Hosting ISPPs' liability under the legal traditions of three EU member states: UK, Germany and France

As discussed in the previous section, the national implementation of Article 14 of the ECD into three selected EU member states fails to offer a solid answer to the ISSPs' liability conundrum. For this reason, the section below examines how hosting ISSPs' liability is defined outside the ECD and in particular how it is defined under the legal traditions of those three EU member states.

i. UK

Given that E-Commerce Regulations 2002/2013 fail to offer a comprehensive definition of hosting ISSPs' liability, English courts were forced to turn to national tort law doctrines in order to establish liability for hosting ISSPs. In particular, the courts use the doctrine of joint tortfeasance that consists of three participation links which, according to Carty's meticulously analysis, are authorisation, procurement and combination.³⁰⁴

All three-participation links have been deployed by English courts with limited success. Authorisation was the first attempt of English courts to ascribe liability on ISSPs.³⁰⁵ Yet, its success has been limited since a different interpretation from its traditional meaning has been offered by courts in terms of online infringements.

³⁰⁴ H. Carty, "Joint tortfeasance and assistance liability" (1999) 19 *Legal studies* 10.

³⁰⁵ C. Angelopoulos "Beyond the safe harbors: harmonizing substantive intermediary liability for copyright infringement in Europe" (2013) 2013 *Intellectual Property Quarterly* 3.

The concept of authorisation stems from *Falcon v Famous Players Film Company Ltd* in 1929.³⁰⁶ It amounts to “sanction, approve and countenance.”³⁰⁷ Authorisation requires a degree of authority. This understanding was exemplified in *CBS Inc v. Ames Records* ruling in 1981 where Whitford J noted that “any ordinary person would, I think, assume that an authorisation can only come from somebody having or purporting to have authority and that an act is not authorized by somebody who merely enables or possibly assists or even encourages another to do that act, but does not purport to have any authority which he can grant to just the doing of the act.”³⁰⁸ Such a view was reinforced in 1988 in *CBS v Amstrad* which was a legal dispute between CBS, a music production company, and Amstrad, a company that produced hi-fi technological tools.³⁰⁹ In this case, Lord Templemann declared that authorisation requires authority but also distinguished authorisation from mere facilitation or assistance. In particular, the court noted that blank tapes can be used for lawful as well as unlawful recording. However, as it has been noted “no manufacturer and no machine confer on the purchase authority to copy unlawfully....By selling the recorder, Amstrad may facilitate copying in breach of copyright but does not authorize it.”³¹⁰ Otherwise, to hold Amstrad liable under the basis of facilitating copying seems unfair.

However, the tool of authorisation has been construed in a different way for online disputes. This is probably due to the impact of the ECD, which was endorsed in 2000, and the trend of case law at European level that equated a hosting ISSP with a diligent economic operator. Following the impact of this EU legislation and case law, in the case of *Dramatico Entertainment*,³¹¹ Arnold Justice carved out specific requirements that define authorisation in the online world. Such requirements include the nature of the relationship between the authorizer and the alleged infringer, the degree of control the authorizer has over the commission of infringements, the means the authorizer adopt in

³⁰⁶ *Falcon v Famous Players* [1926] 2 KB 474.

³⁰⁷ *Falcon v Famous Players* [1926] 2 KB 474 para. 48: as Atkin LJ put it more accurately, “grant or purport to grant to a third person the right to do the act complained of, whether the intention is that the grantee shall do the act on his own account, or only on account of the grantor.”

³⁰⁸ *CBS Inc v. Ames Records and Tapes* [1981] 2 All ER 812; P. Davies, “Accessory liability for assisting torts” (2011) 70 *The Cambridge Law Journal* 359.

³⁰⁹ T. Hays, “The evolution and decentralisation of secondary liability for infringements of copyright-protected works: Part 1” (2006) 28 *European Intellectual Property Review* 620; D. Seng, “Comparative analysis of the national approaches to the liability of internet intermediaries- Part I” *WIPO* (2010) 46.

³¹⁰ *CBS Songs v. Amstrad* [1988] UKHL 15.

³¹¹ *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2012] EWHC 268 (Ch).

order to authorize the commission of infringements, and the steps the authorizer undertook in order to prevent the infringement.³¹²

Moreover, another interpretation of authorisation can be found in the inevitable consequence of the provision of torrent files by The Pirate Bay. This means that it was inevitable for infringements not to occur since the business model of The Pirate Bay was based on the provision of unauthorized material. To cite a few elements of its business model, The Pirate Bay uses a pirated ship for a logo and states that it is founded by a Swedish anti-copyright organization. Finally, the Judge found that while TPB could prevent the file-sharing of unlawful content, it did not take any preventive steps in order to terminate or at least curb the infringements. *A contrario*, the Judge continued that The Pirate Bay has received many requests to block certain torrent files but did not comply with the notifications, while in other cases they were mocking the notices they received from music industry representatives.³¹³

This means that the interpretation of authorisation under the above-mentioned criteria seems to be incompatible with the traditional notion of authorisation. This is because, as many commentators observed, it is dubious whether authority amounts to the refusal of the hosting ISSP to remove the allegedly infringing material after receiving a notification and therefore whether it justifies the attribution of liability rules to hosting ISSPs.³¹⁴

In light of this doubt, the courts resorted to other forms of joint tortfeasance in order to impose liability rules to ISSPs. More specifically, the courts turned to the participation links of procurement or combination. Such links, however, find limited applicability since the courts experienced discrepancies in fitting them into the ISSPs' context.

Procurement, or inducement, is when an individual procures or induces another individual to commit an infringing activity. In this regard, as Davies explained "procurement tends to give another person an idea he would not otherwise have had."³¹⁵

³¹² *Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors* [2012] EWHC 268 (Ch) para. 75-80: "TPB provides a sophisticated and user-friendly environment in which its users are able to search for and locate content."

³¹³ M. Manner, T. Siniketo and U. Polland, "The Pirate Bay ruling: When the fun and game ends" (2009) 20 *Entertainment Law Review* 198.

³¹⁴ H. Laddie, P. Prescott, M. Vitoria and A. Speck, *The Modern Law of Copyright and Designs* (3rd ed. Butterworths 2000) 1776; D. Seng, "Comparative analysis of the national approaches to the liability of internet intermediaries- Part I" WIPO (2010) 46.

³¹⁵ P. Davies, "Accessory liability for assisting torts" (2011) *The Cambridge Law Journal* 358.

Its definition stems from *Amstrad CBS Songs v. Amstrad*³¹⁶ where Lord Templeman explained that procurement amounts to “inducement, incitement or persuasion.” In particular, he added that “inducement, incitement or persuasion to infringe must be by a defendant to an individual infringer and must identifiably procure a particular infringement...”³¹⁷ This means that an individual must encourage a specific person to commit a specific infringement. However, such an interpretation is not easy to apply within the hosting ISSPs’ context. This is because it is problematic to prove that a hosting ISSP encouraged a specific user to commit a tortious act.

Procurement should be distinguished from providing assistance. This is because procurement has a limited scope of liability while to provide assistance covers a wider scope of liability.³¹⁸ Indeed, as Honore notes, procurement aims to make an infringing act appealing to the allegedly infringer who without procurement would not have considered to commit the infringing act.³¹⁹ By contrast, providing assistance concerns any act which leads the primary infringer to commit the violation of the right.³²⁰ Finally, while a procurer can be jointly liable,³²¹ mere assistance cannot affirm joint tortfeasance.³²² This is because the causal link between wrongdoing and providing assistance is weaker than the causal link between wrongdoing and inducing an infringing activity.³²³

By contrast, to provide mere assistance in terms of common design constitutes joint tortfeasance, in other words, assistance in combination amounts to participation in common design.³²⁴ The participation link of common design stems from the *Koursk* ruling in 1924.³²⁵ According to this ruling “persons are said to be joint tortfeasors when their respective shares in the commission of the tort are done in furtherance of a common design.”³²⁶ This means that two or more persons must commit a “concerted action to a common end.”³²⁷ Yet, this does not mean that joint tortfeasors shall cause independent

³¹⁶ *Amstrad CBS Songs v. Amstrad* [1988] UKHL 15.

³¹⁷ *Ibid.*

³¹⁸ P. Davies “Accessory liability for assisting torts” (2011) 70 *The Cambridge Law Journal* 358-359.

³¹⁹ L. A. Hart and T. Honore, *Causation in the Law* (2nd edn. Oxford 1985) 187–188.

³²⁰ P. Davies “Accessory liability for assisting torts” (2011) 70 *The Cambridge Law Journal* 359.

³²¹ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 165.

³²² M. Leistner “Structural aspect of secondary provider liability in Europe” (2014) 9 *GRUR INT* 83; *Credit Lyonnais Bank Nederland NV v Export Credits Guarantee Department* [1996] C.L.C. 11.

³²³ P. Davies, “Accessory liability for assisting torts” (2011) 70 *The Cambridge Law Journal* 359-360.

³²⁴ M. Leistner “Structural aspect of secondary provider liability in Europe” (2014) 9 *GRUR INT* 83.

³²⁵ *Koursk* [1924].

³²⁶ *Koursk* [1924] P. 140, 156.

³²⁷ *Ibid.*

damage. Rather, as the *Koursk* ruling affirms, if only one commits the tortious act, then all independent actors are treated as joint liable for the unlawful act.³²⁸

Within online infringements, this understanding has been mirrored in the *L'Oréal v eBay* ruling.³²⁹ In this case, L'Oréal brought legal proceedings against eBay. L'Oréal argued that eBay had violated its trade mark in a common design under the reasoning that "eBay had combined with the other defendants, who used eBay's services to secure the doing of acts which proved to be infringements." However, Arnold Justice dismissed these allegations. In the line of reasoning, he explained that eBay was a neutral online action platform that did not have control over the fake goods and did not have any duty to implement technological measures in order to stop the dissemination of counterfeit goods on its platform.³³⁰ In this light, eBay cannot be held jointly liable for trademark infringements.

Crucially, this ruling reveals the difficulty of holding a hosting ISSP jointly liable for the actions of its users. On the one hand, although Arnold Justice found the different standards of preventive measures eBay uses across EU member states insufficient, he noted that "facilitation with knowledge and an intention to profit is not enough... to establish joint liability."³³¹ This is because eBay is considered a neutral online platform and liability rules cannot be easily ascribed to it. On the other hand, while eBay has not committed the infringing act itself, in the context of joint tortfeasance, a hosting ISSP is considered a principal in the course of the commission of the tortious act. As Angelopoulos has pointed out "these doctrines fail to identify cases of accessory liability as such, but instead formally categorise them as cases of primary liability, with the accessory treated either as a "joint tortfeasor", who stands alongside the person who committed the material act of infringement as an equal principal in a single tort, or as the perpetrator, not of a participation in the wrong of somebody else, but of an independent act of negligence consisting of that participation."³³² This understanding could open a Pandora's box with a number of rulings in the future by considering ISSPs as primary

³²⁸ Ibid.

³²⁹ *L'Oréal v. eBay* (2009) (EWHC) 1094 (Ch).

³³⁰ *L'Oréal v. eBay* (2009) (EWHC) 1094 (Ch) para. 359.

³³¹ *L'Oréal v. eBay* (2009) (EWHC) 1094 (Ch) para. 382.

³³² C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 13.

infringers and thus endangering their business welfare and in general the innovation within the EU Digital Single Market.³³³

In this light, through a theoretical lens, one might conclude that UK tort law could offer a definition for hosting ISSPs' liability. This understanding is in contrast with Article 14 of the ECD as well as its national implementation since, as presented above, a definition for hosting ISSPs' liability has not yet been provided. Yet, from an implementation perspective, UK national courts face difficulties as to how to implement national tort law doctrines in the context of hosting ISSPs' activities. This is because the traditional tort law doctrine of joint tortfeasance cannot fit into the hosting ISSPs' business model and the services they provide. For instance, while most ISSPs' business models are profit-based, they are considered neutral and without duties to prevent the dissemination of unlawful material. Concomitantly, it is problematic to prove that a hosting ISSPs induces a specific user to commit a specific infringing act, such as in the offline world. Furthermore, in attempting to apply joint tortfeasance doctrine, the UK courts interpret the participation links of procurement or authorisation or participation through common design in an excessive way and thus negate their main essence. Finally, if the courts held hosting ISSPs liable as joint tortfeasors, this means that they would be equally placed next to the primary infringers and thus create the impression that they contributed through their participation to the wrongdoing.

However, it is not only the UK legal system that does not offer a solid answer to hosting ISSPs' liability conundrum. Indeed, the German legal system seems to face similar difficulties in establishing hosting ISSPs' liability.

ii. Germany

Similar to the English legal system, the German legal system turned to its national tort law rules in order to grapple with the concept of hosting ISSPs' liability. In this regard, German national courts have looked at disturber liability and joint-tortfeasance liability. Yet, these national tort law doctrines have limited success, either due to the inadequate degree of protection they offer to rights holders or the difficulty to apply offline provisions to the online ecosystem.

³³³ This is what has happened with the Copyright in the Digital Single Market Directive which ascribes primary liability rules to a specific type of ISSPs, hosting ISSPs.

The first type of liability which has been extensively used by German courts in order to define hosting ISSPs' liability is the disturber liability. This type of liability is not enshrined in the German Civil Code and it is a case law fiction. It finds its roots in the ruling of *Constanze II* in 1954³³⁴ and since then has an extensive application within case law. In order to establish disturber liability, a set of the following criteria must be met: a deliberate and adequately causal contribution to the infringement and the breach of a reasonable duty of care.

In the context of online infringements, the principle of disturber liability was developed in the *Rapidshare* case. In particular, in *Rapidshare I*³³⁵ the Hamburg Court of First Instance held that apart from removing the links upon being notified by rights holders, Rapidshare had to actively monitor any already notified infringing content and thus prevent the emergence of future links that violate the rights of copyright holders. This is because, as the German judges highlighted, Rapidshare's business model was based on offering financial incentives to subscribers so that they can upload popular files with films or TV series. Echoing *Rapidshare II*,³³⁶ in *Rapidshare III*,³³⁷ the German Supreme Court (BGH) noted that Rapidshare had a duty to monitor the already notified infringing content. The German Federal Court clearly noted that Rapidshare's business model was not deliberately designed to infringe the intellectual property holders' rights and it could also be used for legitimate purposes. However, the German court agreed that Rapidshare could not be prevented from having a duty to review with the excuse of the emergence of a high number of infringements in its business model which is considered lawful.

Yet, this understanding does not mean that hosting ISSPs must monitor all the material that passes through their networks. By contrast, as Leistner notes, "only reasonable and technically possible measures in order to identify comparable infringements should be imposed."³³⁸ Reasonable measures, as established by BGH's case law, should take into consideration various factors. Such factors may vary from the role of the disturber in the commission of the wrongdoing, the risk of the wrongdoing, the possibilities to bring legal proceedings against the primary infringer³³⁹ or, as declared in the *Jugendgefaehrdende*

³³⁴ BGH, *Constanze II*, 6 July 1954, I ZR 38/532.

³³⁵ OLG Hamburg, *Rapidshare I*, 27 April 2010, I-20 U 166/09.

³³⁶ BGH, *Rapidshare III*, 21 December 2010, I-20 U 59/10.

³³⁷ BGH, *Rapidshare III*, 15 August 2013, I ZR 80/12.

³³⁸ M. Leistner, "Structural aspects of secondary provider liability in Europe" (2014) 9 GRUR INT 79.

³³⁹ *Ibid*, 88.

Medien bei eBay ruling,³⁴⁰ the financial feasibility of the measures for the hosting ISSP.³⁴¹ Otherwise, measures might put an additional burden on the hosting ISSP, thus endangering its business model. In this light, reasonable duties of a hosting ISSP must not be limited to the removal of unlawful material, but also must be extended to the removal of infringements of the same nature in the future.³⁴² Crucially, the removal of future infringements should not be made the burden of the hosting ISSP.

Likewise, lower German courts addressed the matter of adopting post measures. For instance, in 2012 in *GEMA v YouTube*,³⁴³ the Hamburg District Court reached the conclusion that the music-video sharing platform had not expeditiously take down the allegedly infringing content upon notification and did so only seven months after notification. While this finding does not come in conflict with Article 15 of the ECD, it enhanced its reasoning and addressed the obligation of YouTube to bear filtering duties for future infringements of similar nature which have been already notified by the right holders. For this reason, YouTube was required to use an automated tool of Content ID system which provided the opportunity to right holders to file their work into a database. If the video that was uploaded, matched with a work that existed in the database, the Content ID system automatically removed the file. Therefore, this means that YouTube was forced to use a specific filtering-based measure in order to identify the violations within its network and not solely be contingent upon rights holders' warnings. Following the outcome of the ruling, GEMA concluded an agreement with YouTube to license the work of its members.³⁴⁴

Crucially, the doctrine of disturber liability has been the subject of serious debate among German scholars.³⁴⁵ This is because, as Hoeren and Yankova point out, it establishes a form of causal liability.³⁴⁶ In this sense, the ISSP might be held liable for any infringement

³⁴⁰ BGH, *Jugendgefährdende Medien bei eBay*, 12 July 2007, I ZR 18/04; M. Schellekens, "Liability of Internet Intermediaries: a slippery slope?" (2011) 8 SCRIPTed 154.

³⁴¹ M. Leistner, "Structural aspects of secondary provider liability in Europe" (2014) 9 GRUR INT 79.

³⁴² K. Parti and L. Marin, "Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content" (2013) 9 Journal of Contemporary European Research 149.

³⁴³ Landesgericht Hamburg, *GEMA v YouTube*, 20 April 2012- 310 O 461/10.

³⁴⁴ S. Kulk, *Internet Intermediaries and Copyright Law: EU and US perspective* (Kluwer Law International 2019) 224.

³⁴⁵ G. Spindler and M. Leistner, "Secondary Copyright Infringement – New Perspectives from Germany and Europe" (2006) 37 International Review of Intellectual Property and Competition Law 788; T. Hoeren and S. Yankova, "The Liability of Internet Intermediaries – The German Perspective" (2012) 43 International Review of Intellectual Property and Competition Law 504.

³⁴⁶ T. Hoeren and S. Yankova, "The Liability of Internet Intermediaries – The German Perspective" (2012) 43 International Review of Intellectual Property and Competition Law 504.

that take places on an online platform. Yet, in order to mitigate the negative consequences this kind of liability could cause, the courts endorsed that disturber liability may arise under the specific case of a breach of reasonable duties. This means that a hosting ISSP could be treated as a disturber only if there is a breach of a reasonable duty. However, the concept of reasonable duties of hosting ISSPs has been construed differently by the courts. As discussed earlier, for example, for hosting ISSPs the rise of reasonable duties is contingent upon their technical and financial capability or the impact of the violation of the rights or the limitations by fundamental rights such as the freedom of expression.³⁴⁷ Thus, the concept of reasonable measures should be assessed on a case by case basis.

Furthermore, given that disturber liability aims to address “active” hosting ISSPs that induced infringements within their networks, one might wonder why courts choose to limit their power to disturber liability which only applies to injunctive relief and not extend to joint- tortfeasance doctrines, as do their UK counterpart courts. This concern has been noted by Angelopoulos who points out that “If however it is agreed that the neutrality or lack thereof of a service should make a difference and the courts wish to impose consequences on hosting ISSPs for the “active” inducement of third party copyright infringement, it might would make more sense to bite the bullet and impose liability as a participant in the commission of a wrong.”³⁴⁸ This implies that since the courts want to attribute liability to hosting ISSPs, it seems reasonable to impose a type of liability which can compensate right holders for their losses.

In the light of the above disagreements, the courts resorted to an alternative route and treated hosting ISSPs as direct infringers, namely as tortfeasors. However, as is demonstrated below, the application of tortfeasance doctrine is not compatible with the rationale of tortious secondary liability that is set forth in the ECD. This is because tortfeasance doctrine views hosting ISSPs as primary liable for violations that accrue within their networks.

Pursuant to the German Civil Code, primary liability is governed by § 823 (1) BGB which notes that “A person who, intentionally or negligently, unlawfully injures the life, body,

³⁴⁷ BGH, *Rapidshare III*, 15 August 2013, I ZR 80/12; BGH, *Jugendgefährdende Medien bei eBay*, 12 July 2007, I ZR 18/04; Landesgericht Hamburg, *GEMA v YouTube*, 20 April 2012- 310 O 461/10.

³⁴⁸ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 256-257.

health, freedom, property or another right of another person is liable to make compensation to the other party for the damage arising from this.”³⁴⁹ This means that liability arises directly from unlawful activities or from a breach of a statutory tort. Within the copyright context, a statutory tort is enshrined in Section 97 of the German Copyright Act. Accordingly, this Act notes that “Any person who intentionally or negligently performs such an act shall be obliged to pay the injured party damages for the prejudice suffered as a result of the infringement.”³⁵⁰ Within the trade mark context, Section 14 (6) of the German Trade mark Act notes that “Any person who performs the act of infringement intentionally or negligently shall be obliged to compensate the proprietor of the trade mark for the damage incurred by the act of infringement.”³⁵¹

Yet, to hold hosting ISSPs as direct infringers is a tricky matter. This is because hosting ISSPs do not commit the unlawful acts themselves. Rather, their users commit unlawful activities. However, this understanding did not impede the German Federal Court from using the concept of ‘adopting the information of others.’³⁵² In the case at hand, in *marions-kochbuch.de* the Court found that if the operator of a website checks the content of the material prior its online availability to internet users, it has adopted the material as its own. More specifically, the requirements of one’s own making³⁵³ are to be met if : 1. the website gives the impression to its Internet users that the content has been edited by the administrators of the website and not by third parties, 2. the logo of the website is placed next to the content, 3. the content constitutes the core content of the specific website, 4. the website’ business model has financial gains from this content.³⁵⁴ If the requirements are fulfilled, the operator of a website can be held liable under the general provisions as a content provider. This means that the hosting ISSP is seen as primarily liable for violations which have been committed by its users.

³⁴⁹ Official translation of the German Civil Code is available at <https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p3489> last accessed 22 May 2019.

³⁵⁰ Official translation of the German Copyright Act is available at <https://www.gesetze-im-internet.de/englisch_urhg/englisch_urhg.html> last accessed 27 December 2019.

³⁵¹ Official translation of the German Trade mark Act is available at < http://www.gesetze-im-internet.de/englisch_markeng/englisch_markeng.html#p0092 > last accessed 28 December 2019.

³⁵² S. Kulk, *Internet Intermediaries and Copyright Law: EU and US perspective* (Kluwer Law International 2019) 194 where the author names it “one’s own making principle”; C. Angelopoulos, *European intermediary liability in copyright: a tort-based analysis* (Kluwer Law International 2016) 261.

³⁵³ Zu eigen macht.

³⁵⁴ BGH, Urteil v. 12.11.2009, Az. I ZR 166/07I; see *Telemedicus, Recht der Informationsgesellschaft* is available at <<https://www.telemedicus.info/urteile/Internetrecht/Forenhaftung/1056-BGH-Az-I-ZR-16607-marions-kochbuch.de.html>> last accessed 27 December 2019.

However, this doctrine has been contested by prominent scholars. For instance, Hoeren and Yankova argue that the German Federal Court presumed that since the immunity provisions of the ECD are not applicable, then there is a need to impose liability on hosting ISSPs.³⁵⁵ This understanding, however, conflicts with the existing regulatory framework under the ECD whose main aim is to shield hosting ISSPs from liability.³⁵⁶ What is more, Dinwoodie argues that the lack of immunity provisions as set forth in Article 14 of the ECD does not amount to liability of ISSPs. As he points out, “the scope of the immunity provision in a particular country will not necessarily map to the scope of the secondary liability standard.”³⁵⁷ This means that the inability of hosting ISSPs to provide defences in order to be exonerated from liability for intellectual property infringements within their networks does not equate to their liability. Therefore, when a hosting ISSP does not meet the requirements of liability immunity provisions of Article 14 of the ECD, this does not imply that the hosting ISSP is liable for the wrongdoings of its users. By contrast, whether a hosting ISSP is liable is to be decided by national courts after a careful examination of national tort law provisions.

Yet, despite the criticism raised by prominent scholars, the German courts still seem to follow the principle of “adopting the information of others.” Indeed, it was in 2018 with the dispute between a music producer and YouTube. After receiving a number of notices for copyright infringements by a music producer, YouTube removed the allegedly infringing videos. However, some of those videos have been re-uploaded on the music exchange platform urging the music producer to bring legal proceedings against YouTube alleging copyright violation.³⁵⁸ The German Supreme Court has referred the case to the case has been referred to the CJEU,³⁵⁹ awaiting clarification for six questions. The most relevant for my narrative is question one which addresses whether YouTube performs an act of communication to the public within the definition of Article 3 of the InfoSoc Directive.³⁶⁰ In this sense, the German Supreme Court requires more guidance on whether

³⁵⁵ T. Hoeren and S. Yankova, “The Liability of Internet Intermediaries – The German Perspective” (2012) 43 *International Review of Intellectual Property and Competition Law* (IIC) 503.

³⁵⁶ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 261.

³⁵⁷ Footnote 150 in G.B. Dinwoodie, “A comparative analysis of the secondary liability of online service providers” in G.B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Springer 2016) 25.

³⁵⁸ J. Van Mill, “German BGH – Does YouTube Perform Acts of Communication to the Public?” (Kluwer copyright blog, 27 January 2019) is available at <<http://copyrightblog.kluweriplaw.com/2019/01/27/german-bgh-does-youtube-perform-acts-of-communication-to-the-public/>> last accessed 27 December 2019.

³⁵⁹ BGH, Beschluss I ZR 140/15.

³⁶⁰ Article 3(2) InfoSoc Directive “1. Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making

YouTube is primary liable for the information that is disseminated via its platform from its users, thus implying that YouTube adopts as its own the uploaded content by its internet users. The referral is still ongoing but the commentators expect a positive answer to the question, especially now in light of the new EU regulatory regime for hosting ISSPs for copyright violations, which will be discussed in chapter 3 of this thesis.

In the light of the above-mentioned discrepancies, German courts turn to joint-tortfeasance doctrine in order to base liability for ISSPs. However, the application of joint-tortfeasance is a contested area. It is enshrined in Article 830 (1) II BGB which notes that “(1) If more than one person has caused damage by a jointly committed tort, then each of them is responsible for the damage. The same applies if it cannot be established which of several persons involved caused the damage by his act.”³⁶¹

In order to establish liability based on joint tortfeasance, the requirement of intent or knowledge have to be met. This concerns the intent of hosting ISSPs to commit the infringing act or knowledge of hosting ISSPs about the unlawful nature of the act.³⁶² However, as Angelopoulos noted “this condition is not usually met by online intermediaries.”³⁶³ This is because hosting ISSPs are devoid of general monitoring obligations that concern the control of the transmission of material via their platforms. This of course does not imply that lack of knowledge could exonerate hosting ISSPs from liability based on joint tortfeasance. By contrast, the consistent ignoring of notifications for allegedly infringing material could constitute liability. For instance, a ruling delivered by *OLG Hamburg*, handed down that a hosting ISSP was an accessory to commission of the infringement because it ignored notifications for specific infringements and thus violated its duty of care.³⁶⁴ This means that whereas ISSPs are prohibited from engaging in monitoring activities and thus are deprived of the requirement of knowledge, a violation of a duty of care can take place when the hosting ISSP does not consider

available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.”

³⁶¹ Official translation of the German Civil Code is available at <https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p3489> last accessed 27 December 2019.

³⁶² C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 258.

³⁶³ C. Angelopoulos, “Beyond the safe harbors: Harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 2013 Intellectual Property Quarterly 14.

³⁶⁴ OLG Hamburg, 13.05.2013 - 5 W 41/13.

notifications for infringements within its platform. Therefore, in this case, pursuant to German scholarship, the hosting ISSP could be held liable as joint-tortfeasor.

Moreover, apart from the joint-tortfeasance doctrine, German courts developed the concept of additional joint-tortfeasance. Additional joint tortfeasors include as per Article 830 (2) II BGB those that participate in the commission of the wrongdoing, such as the instigators and the accessories of the unlawful act.³⁶⁵ Based on this civil law provision, the Tenth Civil Senate of the German Supreme Court has further developed the notion of additional joint-tortfeasance which includes the willful causal contribution to the infringing act, the breach of a duty of care and possible prevention of the infringing act.³⁶⁶ Additional tortfeasance has similarities with the disturber liability but covers punitive damages as well.³⁶⁷ This is because, as Leistner notes, “the standard for the duty of care can be structured along the lines of the case law on *Stoererhaftung*.”³⁶⁸ Yet, additional tortfeasance has limited applicability and in particular it only applies to unfair competition law cases.³⁶⁹ This understanding has been reiterated in the case of *the Jugendgefaehrdende Medien bei eBay*.³⁷⁰ In this case, the German Federal Court of Justice found that eBay had a duty of care to prevent the commission of unfair competition acts within its platform. By not terminating the commission of unfair competition acts, the German court argued that for eBay the mere provision of a platform that enables unfair competition acts by internet users constitutes an act of unfair competition itself. This means that in order to be exonerated from liability for unfair competition acts, the hosting ISSP must have undertaken all the appropriate measures and prevented unfair competition acts by its users.

However, it seems that this outcome is strictly limited to cases of unfair competition law.³⁷¹ This is because an extension of this understanding to copyright or trademark law

³⁶⁵ Official translation of the German Civil Code is available at <https://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.html#p3489> last accessed 27 December 2019.

³⁶⁶ M. Leistner, “Structural aspect of secondary provider liability in Europe” (2014) 9 GRUR INT 80; M. Leistner, “Common Principles of Secondary Liability?” in A. Ohly (ed.), *Common Principles of European Intellectual Property Law* (Mohr Siebeck 2012) 127.

³⁶⁷ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 269.

³⁶⁸ M. Leistner, “Structural aspects of secondary provider liability in Europe” (2014) 9 GRUR INT 80.

³⁶⁹ T. Hoeren and S. Yankova, “The Liability of Internet Intermediaries – The German Perspective” (2012) 43 International Review of Intellectual Property and Competition Law (IIC) 506.

³⁷⁰ BGH, *Jugendgefaehrdende Medien bei eBay*, 12 July 2007, I ZR 18/04.

³⁷¹ M. Leistner, “Common Principles of Secondary Liability?” in A. Ohly (ed.), *Common Principles of European Intellectual Property Law* (Mohr Siebeck 2012) 127.

could be troublesome. Consider, for instance, the case of *Sommer unseres Lebens*.³⁷² In this case, the Court did not consider the operator of an insecure wireless connection liable. This is because although the operator had a duty to secure her connection, the functioning of a wireless network without a password does not amount to unauthorized act to communication to the public as per § 19 A of the German Copyright Act. In this light, although the operator of the connection violated its duty, the act to provide connection without password does not constitute copyright infringement itself.³⁷³

Bearing in mind the above, German courts have attempted to define hosting ISSPs' liability on the basis of various tort law doctrines or general civil law doctrines. Such doctrines could vary from disturber liability to tortfeasance, joint tortfeasance and additional tortfeasance. However, as illustrated throughout this section, these doctrines are difficult to apply in the context of online platforms. As presented in this section, disturber liability is triggered upon the violation of a reasonable duty of care. However, how a reasonable duty of care should be understood depends on various factors and is mostly considered on a case by case basis. On the other hand, tortfeasance or joint tortfeasance places ISSPs next to the primary infringers and users and thus creates the impression that they are also primary infringers for intellectual property violations within their networks. Finally, while the adoption of additional tortfeasance doctrine could make more sense, its applicability appears to be limited to unfair competition law matters and is not extended to copyright or trade mark context.

iii. France

Along similar lines, in France, there is no special legal basis to establish hosting ISSPs' liability. For this reason, French courts rely primarily upon the provisions of the French Code Civil, namely Articles 1382 and 1383.³⁷⁴ That said, liability arises if the elements of fault, damage and a causal link between fault and damage are met.³⁷⁵ Article 1382 notes that "Any act whatever of man, which causes damage to another, obliges the one by

³⁷² BGH, *Sommer unseres Lebens*, 12 May 2010- I ZR 121/0; M. Leistner, "Common Principles of Secondary Liability?" in A. Ohly (ed.), *Common Principles of European Intellectual Property Law* (Mohr Siebeck 2012) 127.

³⁷³ M. Leistner, "Structural aspects of secondary provider liability in Europe" (2014) 9 GRUR INT 80.

³⁷⁴ X. Amadei, "Standards of liability for Internet for Internet Service Providers: A comparative study of France and the United States with a specific focus on copyright, defamation and illicit content" (2002) 35 Cornell International Law Journal 203.

³⁷⁵ Y. Benhamou, "Compensation of Damages for Infringements of Intellectual Property Rights in France, Under Directive 2004/48/EC and its Transposition Law – New Notions?" (2009) 40 International Review of Intellectual Property and Competition Law 126.

whose fault it occurred, to compensate it”³⁷⁶ and Article 1383 expands the duty to repair in cases of negligence or imprudence and reads as follows “Everyone is liable for the damage he causes not only by his intentional act, but also by his negligent conduct or by his imprudence.”³⁷⁷

In the light of the above and following the German approach, French courts also imposed a general duty of care on hosting ISSPs. A failure to comply with the obligation may give rise to fault. This general rule has been exemplified in a number of case laws that outlined that hosting ISSPs have a duty to take precautionary measures in order to be exonerated from liability. This understanding has been encapsulated in the *Lacoste* ruling³⁷⁸ where Nanterre Court of First Instance applied Articles 1382 and 1383 of French Civil Code and specified three obligations that should be imposed on hosting ISSPs, namely the obligations of information, proactive measures and action against illicit activities.³⁷⁹ This means that hosting ISSPs must encourage their users to respect third parties’ rights, undertake precautionary measures to prevent the reappearance of infringing material as well as be alert towards the circulation of infringing material within their networks and react upon being notified of an illicit activity.³⁸⁰

However, these obligations do not have a uniform interpretation,³⁸¹ thus, they are divided into those before and those after the adoption of the ECD. On the one hand, before the implementation of the ECD the duty of care was interpreted in an excessive manner.³⁸² For instance, in the *Calimero* ruling in 2000,³⁸³ the French Court held liable the hosting provider of a website with sadomasochistic material on the basis of Article 1382 of French Civil Code. In this case, the website operator named the domain name of the website after the popular cartoon Calimero and hosted pictures with sadomasochistic content. The hosting provider requested the operator of the website with unlawful material to move

³⁷⁶ Official translation of the French Civil Code by G. Rouhette and A. Rouhette-Berton is available at <[file:///C:/Users/br918285/Downloads/Code_22%20\(1\).pdf](file:///C:/Users/br918285/Downloads/Code_22%20(1).pdf)> last accessed 27 December 2019.

³⁷⁷ Official translation of the French Civil Code by G. Rouhette and A. Rouhette-Berton is available at <[file:///C:/Users/br918285/Downloads/Code_22%20\(1\).pdf](file:///C:/Users/br918285/Downloads/Code_22%20(1).pdf)> last accessed 27 December 2019.

³⁷⁸ *Lacoste/multimania, Eterel and Cybermedia* (1999) (Tribunal de Grande Instance de Nanterre)

³⁷⁹ X. Amadei, “Standards of liability for Internet for Internet Service Providers: A comparative study of France and the United States with a specific focus on copyright, defamation and illicit content” (2002) 35 *Cornell International Law Journal* 204.

³⁸⁰ C. Angelopoulos, “Beyond the safe harbors: harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 3 *Intellectual Property Quarterly* 262.

³⁸¹ *Ibid.*

³⁸² C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 221.

³⁸³ *Cons P v Monsieur G.* [2005] (Tribunal de Grande Instance de Paris).

his website to another provider, but it still accepted to host the website with illicit material.³⁸⁴ In this regard, according to French Judges, it was the inaction of the hosting provider to block access to the website, despite its ability to terminate the access to it, that held the hosting provider liable for violating its duty of care.

On the other hand, following the transposition of the provisions of the ECD into the French legal system through the LCEN Law in 2004, the principle of duty of care has been construed in a restrictive manner. This understanding has been exemplified in the *SARL Zadig Productions ruling* in 2007³⁸⁵ where the Court of First Instance in Paris held that upon notification of the infringing copies of film, Google was under the obligation either to mitigate the diffusion of unauthorized works or block users from accessing the website with the infringing content.³⁸⁶ This is because, as the French court concluded, that Google qualified as a hosting ISSP that offered space to its users to commit infringing acts.³⁸⁷ A failure to terminate the access or at least impede infringing material from reaching end-users could trigger ISSPs' liability. This means that, upon being notified, ISSPs have a duty to remove any unlawful material and prevent its re-emergence within their networks.³⁸⁸

This line of thinking has been reiterated by several French courts. For instance, in the landmark case of *Joyeux Noel* in 2007³⁸⁹ Nord Ouest Productions brought legal proceedings against Dailymotion alleging that its users uploaded the movie of Joyeux Noel without permission and thus asking 34,813 euros in damages for copyright infringements.³⁹⁰ Responding to film production allegations, Dailymotion argued that it is a hosting provider and thus is entitled to immunity liability provisions as enshrined in Article 14 of the ECD. However, after a careful examination of the facts, Paris Court of First Instance found that Dailymotion's intention was to attract unauthorized material and thus increase its advertisement revenues. In particular, it was found that "the success of

³⁸⁴ X. Amadei, "Standards of liability for Internet for Internet Service Providers: A comparative study of France and the United States with a specific focus on copyright, defamation and illicit content" (2002) 35 Cornell International Law Journal 205.

³⁸⁵ *SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud c. Sté Google Inc. et AFA* [2007] (Tribunal de Grande Instance de Paris).

³⁸⁶ C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 193-194.

³⁸⁷ M. Farano, "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and US Approaches" (2012) TTLF Working Paper 74.

³⁸⁸ C. Jasserand, "France: The Court of Cassation puts an end to the Notice and Stay Down Rule" (Kluwer copyright blog, 14 August 2012) is available at <<http://copyrightblog.kluweriplaw.com/2012/08/14/france-the-court-of-cassation-puts-an-end-to-the-notice-and-stay-down-rule/>> last accessed 6 April 2019.

³⁸⁹ *Christian C., Nord Ouest Production c. Dailymotion, UGC Images* [2007] (Tribunal de Grande Instance de Paris).

³⁹⁰ N. Jondet, "The silver lining in Dailymotion's copyright cloud" (2008) Juriscom. Net 2.

Dailymotion implied that the broadcasting of well-known marks, the only ones enable to increase the sites audience, and thus ad revenues.”³⁹¹ For this reason, as the Court noted, Dailymotion had a duty to prevent illicit activities by adopting filtering mechanisms. Failure to comply with this duty would have resulted into holding Dailymotion liable for copyright infringements of its users.

Such a stance has been retained by *the Google Inc. c/ Les Films de la Croisade, Goatworks Films* case from the Court of Appeal in Paris.³⁹² In this case, it was decided that Google qualified as hosting ISSP under Article 14 of the ECD and thus was under the obligation to take precautionary measures to prevent the dissemination of unlawful content within its network after being notified.³⁹³ Otherwise, Google would have not been eligible to evoke the immunity liability provisions of the ECD and therefore would be liable.

Yet, to define hosting ISSPs’ liability, imposing on them duty of care to prevent the re-emergence of similar infringements might come in conflict with Article 15 of the ECD. This is in line with the German legal system, as discussed above. In *Google v Viaticum et Luteciel*,³⁹⁴ the Court found Google liable because of its AdWords system. In particular, the Court considered that Google should have prevented the registration of trademarks’ keywords by deploying filtering technology thus negating the need to be notified of the allegedly infringing act. Crucially, this outcome has been severely criticized since it goes against the existing EU Law and more specifically with Article 15 of the ECD that prohibits the imposition of general monitoring obligations.³⁹⁵ By the same token, in *Sedo GmbH v. Hotel Meridien*,³⁹⁶ the French Supreme Court examined the dispute between an online domain name’s auction platform and the Hotel Meridien trademark. In this case, the court found Sedo secondarily liable because the selling of a specific domain name on its platform violated the trademarks of other parties. This is because, as the Court handed down, “every operator acting in business owes to third party a duty not to harm third party’s business.”³⁹⁷ This outcome could imply that ex-ante control or regular screening

³⁹¹ Translation from N. Jondet, “The silver lining in Dailymotion’s copyright cloud” (2008) Juriscom. Net 5.

³⁹² *Google Inc. c. Les Films de la Croisade, Goatworks Films* [2011] (Cour d’appel de Paris).

³⁹³ M. Farano, “Internet Intermediaries’ Liability for Copyright and Trademark Infringement: Reconciling the EU and US Approaches” (2012) TTLF Working Paper 75.

³⁹⁴ *Google v Viaticum et Luteciel* [2011] (Cour d’appel de Versailles).

³⁹⁵ M. Leistner, “Structural aspects of secondary provider liability in Europe” (2014) 9 Journal of Intellectual Property Law and Practice 90.

³⁹⁶ *Sedo GmbH v Hotel Meridien, Stephane H.* [2008] Cour de Cassation.

³⁹⁷ Footnote 160 in B. M. Farano, “Internet Intermediaries’ Liability for copyright and trademark infringement: Reconciling the EU and US approaches” (2012) TTLF Working Paper 44.

should be performed in order to prevent the infringements of trademarks on its platform and thus give rise to concerns with regard to the compatibility of a duty of care for ISSPs with Article 15 of the ECD.

For this reason, this line of thinking was reconsidered by the French Supreme Court in 2012 with three rulings, namely *Google & Aufeminin.com v. Mr. X*,³⁹⁸ *L'affaire Clearstream*³⁹⁹ and *Les dissimulateurs*.⁴⁰⁰ In these cases, French judges reassessed the imposition of a duty for ISSPs to prevent the reappearance of infringing, which has been intensively used by the courts since 2007.⁴⁰¹ In particular, they disconnected the obligation to remove the infringing material with the subsequent monitoring obligation. In this regard, it has been argued that it is up to the copyright holders to monitor the network of hosting ISSPs and detect any violation of their rights. This means that hosting ISSPs must not be under the obligation to monitor the unwelcome content since it could contradict with Article 15 of the ECD which advocates a general prohibition for filtering activities. This is because, as Angelopoulos has noted, if the hosting ISSP wants to be exonerated from liability, it must keep up controlling its network for future infringements of the same core.⁴⁰² Otherwise, the hosting ISSPs will be considered to violate its duty of care and thus be held liable.

In the light of the above, under French tortious secondary liability rules, a hosting ISSP can be held liable if it intentionally or negligently gives rise to copyright or trademark infringements. This understanding has enabled the wide application of the concept of duty of care for hosting ISSPs since the violation of duty of care would amount to negligence. How the general duty of care should be defined rests on the assessment of each domestic court. In this light, French courts have construed the general duty of care in different terms, either in a restrictive or excessive manner. Yet, while a restrictive interpretation of a duty of care for hosting ISSPs is compatible with Recital 47 of the ECD, an excessive interpretation of a duty of care could incite severe criticism since it contradicts with existing EU Law provisions and, specifically, with Article 15 of the ECD

³⁹⁸ *Google & Aufeminin.com v. Mr. X* [2012] Cour de Cassation.

³⁹⁹ *La société Google France c. la société Bach films* (L'affaire Clearstream) [2012] Cour de Cassation.

⁴⁰⁰ *La société Google France c. La société Bac films* (Les dissimulateurs) [2012] Cour de Cassation.

⁴⁰¹ C. Jasserand, "France: The Court of Cassation puts an end to the Notice and Stay Down Rule" (Kluwer copyright blog, 14 August 2012) is available at <<http://copyrightblog.kluweriplaw.com/2012/08/14/france-the-court-of-cassation-puts-an-end-to-the-notice-and-stay-down-rule/>> last accessed 27 December 2019.

⁴⁰² C. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Kluwer Law International 2016) 196.

that prohibits the deployment of precautionary measures such as ex-ante filtering of all the information that is transmitted online.

Bearing in mind the above, it could be concluded that the legal traditions of the English, German and French jurisdictions fail to offer a solid answer to the conundrum of hosting ISSPs' liability. This is because, as presented in this section, each jurisdiction has its own secondary tort law doctrine. For instance, the French tort law system extends the direct breach of tort law provisions to additional actors and ascribes a duty of care on hosting ISSPs which urges them to undertake precautionary measures to avoid future infringements. In line with this, the German legal system develops the notion of disturber liability and places a reasonable duty of care on hosting ISSPs. Insofar as the English tortious legal tradition is concerned, whereas the doctrine of joint-tortfeasance is applicable to hosting ISSPs' activities, to endorse a duty of care for ISSPs seems to be out of the question. This creates a patchwork of miscellaneous tort law doctrines that differ from each other and offer legal uncertainty to the parties at stake. Given the lack of a uniform approach towards hosting ISSPs' liability, right holders might not be able to compensate their losses in cases of intellectual property infringements on the online networks while hosting ISSPs might overzealously remove material which could be lawful, thus preventing lawful material to reach end-users.

What is more, there have been many stances where national courts have faced discrepancies in order to fit secondary tortious liability doctrines to hosting ISSPs' activities. This is either because some tortious secondary liability doctrines require a duty of care for hosting ISSPs. For example, under French jurisdiction a duty of care shall be imposed on hosting ISSPs. This means that once hosting ISSPs are notified of the allegedly illicit activity, they have a duty to act and prevent the dissemination of unlawful material within their networks. Failure to comply with the duty of care amounts to their liability. However, what falls under the scope of duty of care is subject to a case by case assessment, thus leading to contradicting outcomes. Another reason that reiterates the difficulties that national courts face in order to find hosting ISSPs liable is the fact that some secondary tortious liability rules in some jurisdictions consider hosting ISSPs as primary infringers. For instance, the joint-tortfeasance doctrine, which has a wide application in the German and English legal systems, places the hosting ISSPs next to the principal infringer of the tortious act. This is because joint-tortfeasor is considered a direct infringer as well. This understanding, however, prompts further reflection on the

appropriateness of fitting joint-tortfeasance doctrines into hosting ISSPs' activities. To treat a hosting ISSP as a direct infringer does not only negate the main intention of European policymakers to offer a secondary liability regime for hosting ISSPs but also aggravates, without reason, the role of ISSPs with regard to intellectual property infringements committed on its platform.

V. Conclusion

This chapter has critically engaged with the secondary liability of ISSPs under the ECD. After demonstrating the theoretical approaches that warrant the ascription of liability rules to ISSPs, the narrative delved into the regulatory framework of ISSPs under Article 14 of the ECD.⁴⁰³ Since 2000, the ECD has been the main instrument that regulates ISSPs' liability for infringements that may accrue within their networks and are committed by their users. It had been warmly welcomed by ISSPs since its main intention was to enhance e-commerce which was at its infancy at that time and boost innovation at European level.

However, a critical analysis of the ECD, and in particular of Article 14, demonstrated that the regulatory framework of hosting ISSPs is outdated. This is because Article 14 of the ECD defines hosting ISSPs' liability in a reverse logic. This means that hosting ISSPs are offered a number of defences in order to be exonerated from liability, or to put it more accurately, Article 14 offers the specific conditions under which hosting ISSPs are not liable for intellectual property infringements that take place within their networks. For instance, hosting ISSPs can escape from liability if they are not aware of the illicit activity or if they remove the unlawful content upon being notified. Hence, this means that the ECD does not provide a definition of hosting ISSPs' liability.

What is more, the findings indicate that the transposition of the ECD in three selected jurisdictions follows the rationale of the ECD and therefore does not offer a solid answer to hosting ISSPs' liability. For instance, all three jurisdictions follow *verbatim* the rationale of the ECD and endorse defences for ISSPs that they could invoke in order to defend themselves against allegations of liability. Therefore, the implementation of the ECD into national legal systems fails to provide a solid answer to the conundrum of hosting ISSPs' liability.

⁴⁰³ See chapter 2 III A, B, C.

In this light, many courts have turned to their national secondary tortious liability rules in order to attribute liability to ISSPs. Given the lack of harmonisation of secondary liability rules at European level, each jurisdiction applies its national tort law system in order to seek the appropriate tortious liability doctrines and thus define ISSPs' liability. While, from a theoretical perspective, secondary tortious liability could offer a definition of hosting ISSPs' liability, it appears that national courts face difficulties fitting them into online disputes. This is either because tortious secondary liability doctrines require a duty of care for hosting ISSPs which can only be assessed on a case by case basis, or because other secondary tortious liability rules in some jurisdictions treat hosting ISSPs as primary infringers of the unlawful act.

Further, the idea of each jurisdiction adopting its own national tort rules could create a puzzle of different secondary tortious liability doctrines that stem from the legal traditions of each national jurisdiction respectively. However, this understanding could result in legal uncertainty to the parties involved and thus undermine their interests.

In the light of the above, a legal reform is extremely urgent so as to clarify the liability that hosting ISSPs might incur in case of intellectual property infringements within their networks. Yet, before presenting a number of recommendations, it is necessary to critically assess the second legislative piece that regulates hosting ISSPs' liability for copyright infringements within their networks. This new legislative tool is the Copyright in the Digital Single Market Directive (DSMD). As discussed in chapter 1, this legislative tool was introduced in April 2019 and has severe controversy among different stakeholders at European level. Although the DSMD has not been tested yet in the courts' legal arena and given that its transposition into the national legal systems of the 27 European member states runs until 2021, an array of structural problems have already been identified. For this reason, the following chapter critically examines the DSMD and in particular Article 17 which addresses the liability of online content sharing service providers, which is new type of hosting ISSPs, that host material uploaded by their users within their networks.

Chapter 3: The regulatory framework of Online Content Sharing Service Providers (OCSSPs) under Article 17 of the Copyright in the Digital Single Market Directive (DSMD): a controversial approach

I. Introduction

As discussed in chapter 2, the regulatory framework of hosting ISSPs as set forth in the ECD⁴⁰⁴ seems outdated. This is because Article 14 of the ECD offers a set of defences for hosting ISSPs⁴⁰⁵ in order for them to be exonerated from liability for infringements committed by their users.⁴⁰⁶ What is more, the transposition of the ECD into national legal systems follows the rationale of the ECD and thus fails to provide an answer to the ISSPs' liability conundrum. Finally, given that the ECD does not define hosting ISSPs' liability, national courts turn to their national secondary tortious legal doctrines. However, given that tortious secondary liability rules are not harmonized at European level, the result is a landscape of different secondary liability rules in tort that not only differ in each jurisdiction but also are difficult to apply within the context of online disputes.

However, as well as the ECD, there is another legislative tool that regulates ISSPs' liability for copyright infringements. The Copyright in the Digital Single Market Directive (DSMD) has been finalized on the 17th of April 2019.⁴⁰⁷ Given that this research addresses trade mark as well as copyright infringements online, a critical evaluation of the newly introduced DSMD is extremely urgent in order to provide a complete picture of the regulatory framework of hosting ISSPs at the European level.

⁴⁰⁴ Council Directive (EC) 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 (hereinafter ECD).

⁴⁰⁵ As discussed in chapter 2, Article 14 notes that hosting ISSPs can exonerate from liability if they lack knowledge or they are not aware of the infringement or take down the infringement upon obtaining knowledge of it.

⁴⁰⁶ Chapter 2 IV A, B, C.

⁴⁰⁷ Council Directive (EC) 2019/790/EC of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130 (hereinafter DSMD).

Following the outcomes of the impact assessment on the modernization of European copyright rules launched by the European Commission,⁴⁰⁸ it has been concluded that there is an unfair distribution of the revenues with regard to the content that is circulated online between hosting ISSPs and right holders. In order to resolve this mismatch,⁴⁰⁹ the EU Commission initiated the Proposal for a new Copyright in the Digital Single Market Directive (DSMD).⁴¹⁰ As Jean Claude Juncker stated, the DSMD entails “clear rules that guarantee fair remuneration for creators, strong rights for users and responsibility for platforms. When it comes to completing Europe's Digital Single Market, the copyright reform is the missing piece of the puzzle.”⁴¹¹

Among the provisions of this Directive, the most relevant to the current discussion is Article 17 (formerly Article 13) which deals with the liability of OCSSPs', which is a new type of hosting ISSPs, for copyright infringements. It is this provision in the DSMD that has raised severe controversy among different stakeholders. Here it bears noting that Article 17 has not been tested yet in the courts' legal arena while its transposition to EU national member states is still ongoing.⁴¹² However, a number of problematic aspects of Article 17 have been identified.⁴¹³ This is because Article 17 of the DSMD is complex and not easy to follow even by legal experts. What is more, it has been argued that Article 17 of the

⁴⁰⁸ EU Commission Staff working document, “Executive summary of the impact assessment on the modernisation of EU copyright rules” SWD (2016) 302 final 1.

⁴⁰⁹ T. Madiaga, “EU Legislation in Progress: Copyright in the digital single market” (2019) European Parliamentary Research Service 1- 3; S. von Lewinski, “Comments on the ‘value gap’ provisions in the European Commission’s Proposal for a Directive on Copyright in the Digital Single Market (Article 13 and Recital 38)” (Kluwer Copyright Blog, 10 April 2017) is available at <http://copyrightblog.kluweriplaw.com/2017/04/10/comments-value-gap-provisions-european-commissions-proposal-directive-copyright-digital-single-market-article-13-recital-38/> last accessed 28 December 2019; A. Bridy, “EU Copyright Reform: Grappling with the Google Effect” (2019) Vanderbilt Journal of Entertainment & Technology Law 2.

⁴¹⁰ Council Directive (EC) 2019/790/EC 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 (Text with EEA relevance) PE/51/2019/REV/1, OJ L 130, 17.5.2019 (DSMD).

⁴¹¹ EU Commission, “Copyright reform clears final hurdle: Commission welcomes approval of modernised rules fit for digital age” (15 April 2019) is available at http://europa.eu/rapid/press-release_IP-19-2151_en.htm last accessed 28 December 2019.

⁴¹² Transposition into EU member states 7 June 2021.

⁴¹³ “Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics” (November 2019); S. Stalla-Bourdillon and others, “Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society” (2016); C. Angelopoulos and J. P. Quintais, “Fixing copyright reform: a better solution to online infringement” (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 153.

DSMD is biased in favor of right holders⁴¹⁴ since it appears to promote the rights of copyright holders and subordinates the interests of OCSSPs and internet users.⁴¹⁵

Indicative of its controversy are the sizeable protests that have been organized across EU member states⁴¹⁶ as well as numerous speeches and signed statements by prominent public figures and large inventors. For instance, the UN Representative on freedom of expression and opinion, David Kaye, noted⁴¹⁷ while it is imperative that Europe modernizes its copyright rules, “this should not be done at the expense of the freedom of expression that Europeans enjoy today”⁴¹⁸ while at the same time the founder of the world wide web, Sir Tim Berners-Lee, stated that “the DSM transforms the internet “from open platform for sharing and innovation, into a tool for the automated surveillance and control of its users.”⁴¹⁹ What is more, a set of stakeholders’ dialogues have been already taken place at the University of Amsterdam⁴²⁰ and in the EU Commission⁴²¹ so as to provide more guidance to member states on how to implement the DSMD into their

⁴¹⁴ E. Rosati, “Public Lecture on Copyright and the Court of Justice of the European Union: Role, Action, Legacy” (27 February 2019) University of Reading, Reading (UK); A. Guadamuz, “New EU Directive threatens the Internet as we know it” (TechnoLlama, 23 February 2019) is available at <<https://www.technollama.co.uk/new-eu-directive-threatens-the-internet-as-we-know-it>> last accessed 28 December 2019.

⁴¹⁵ M. Husovec, “How Europe wants to redefine global online copyright enforcement” in T. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer Law International 2019) 529; G. Frosio, “To filter or not to filter? That is the question in EU Copyright Reform” (2018) 36 *Cardozo Arts and Entertainment Law Journal* 122; G. Frosio and S. Mendis, “Monitoring and Filtering: European Reform or Global Trend” (2019) Center for International Intellectual Property Studies Research Paper 21.

⁴¹⁶ M. Maker, “Inside the giant German protest trying to bring down Article 13” (Wired, 26 March 2019) is available at <<https://www.wired.co.uk/article/article-13-protests>> last accessed 28 December 2019.

⁴¹⁷ P. Samuelson, “The EU’s Controversial Digital Single Market Directive – Part I: Why the Proposed Internet Content Filtering Mandate Was So Controversial” (Kluwer Copyright Blog, 10 July 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/07/10/eus-controversial-digital-single-market-directive-part-proposed-internet-content-filtering-mandate-controversial/>> last accessed 28 December 2019; D. Kaye, “Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression” (13 June 2018) is available at <<https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf>> last accessed 28 December 2019.

⁴¹⁸ Office of the High Commissioner, United Nations Human Rights, “EU must align copyright reform with international human rights standards” is available at <<https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24298&LangID=E>> last accessed 28 December 2019.

⁴¹⁹ P. Samuelson, “The EU’s Controversial Digital Single Market Directive – Part I: Why the Proposed Internet Content Filtering Mandate Was So Controversial” (Kluwer Copyright blog, 10 July 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/07/10/eus-controversial-digital-single-market-directive-part-proposed-internet-content-filtering-mandate-controversial/>> last accessed 28 December 2019

⁴²⁰ European Copyright Roundtable, “Over-blocking: How to safeguard creators’ and users’ rights? & Closing Remarks” (17 June 2019) is available at <<https://www.youtube.com/watch?v=9zRjXr6xxSQ>> last accessed 28 December 2019.

⁴²¹ EU Commission, “Organisation of a stakeholder dialogue on the application of Article 17 of Directive on Copyright in the Digital Single Market” (28 August 2019) is available at <<https://ec.europa.eu/digital-single-market/en/news/organisation-stakeholder-dialogue-application-article-17-directive-copyright-digital-single>> last accessed 28 December 2019.

national legislation. Finally, the controversy that revolves around DSMD led Poland to file a challenge before the CJEU and requested the annulment of Article 17. As for the reasoning of application, the Polish Minister of Culture and Heritage outlined that “in our opinion this mechanism introduces solutions with preventive censorship features. Such censorship is forbidden by both the Polish Constitution and EU law – the Charter of Fundamental Rights guarantees freedom of expression.”⁴²² The application is still under review.

Against this background, this chapter aims to critically assess the DSMD. The narrative starts with a historical account of Article 17 that provides a comprehensive discussion of the legislative process that led to the final vote of the DSMD. This historical account includes the EU Commission’s original Proposal, the EU Council’s Proposal, and the EU Parliament’s final compromised text after the trilogues. The narrative on the legislative process that preceded the final text of the DSMD will not be analysed since most of the problematic features that were included in the EU Commission’s Proposal, and the EU Council’s and EU Parliament’s texts also exist in the final text of the DSMD. Thus, in order to avoid repetitions but also to draw attention to the final text of the DSMD, the historical account is condensed. Following this, the discussion moves to the final draft of Article 17 of the DSMD and critically addresses its problematic features. These issues entail the introduction of primary liability rules, the dual liability regime with the ECD as well as a number of obligations that contradict with the *EU acquis*. Finally, this chapter offers the concluding remarks of Part I of this thesis where a critical evaluation of the implications of liability rules under Article 14 of the ECD, which was examined in chapter 2, and Article 17 of the DSMD, which is assessed in this chapter, is presented. This concluding section of Part I is necessary since the detrimental impact of both legislative tools to the rights of hosting ISSPs and OCSSPs, right holders and internet users are discussed.

⁴²² N. Mileszyk, “The Copyright Directive challenged in the CJEU by Polish government” (Communia, 1 June 2019) is available at < <https://www.communia-association.org/2019/06/01/copyright-directive-challenged-cjeu-polish-government/>> last accessed 28 December 2019; Action brought on 24 May 2019 — Republic of Poland v European Parliament and Council of the European Union (Case C-401/19) is available at <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=216823&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=8371710>> last accessed 28 December 2019.

II. Historical account of Article 17 of the DSMD

The following section discusses the different legislative stages of the implementation of Article 17 of the DSMD, starting from the EU Commission Proposal to the texts of the EU Council and the EU Parliament.

A. *EU Commission's Proposal for the Copyright in the Digital Single Market Directive (DSMD)*

In September 2016, the EU Commission published its Proposal for a Copyright in the Digital Single Market Directive at the State of the Union.⁴²³ This Proposal, as the Commissioner for Digital Affairs stated, was expected to provide a “copyright environment that is stimulating, fair and rewards investment.”⁴²⁴ This Proposal was part of the Digital Single Market Strategy that was announced in March 2015⁴²⁵ and whose aim was to modernize intellectual property rights’ enforcement rules in the online world.⁴²⁶ It traces back to the EU Commission’s Public Consultation on the Review of European Copyright rules that outlined the need for modernizing copyright rules at the European level.⁴²⁷

However, this much anticipated legislative proposal, whose main purpose was to fight against the value gap and ensure fair remuneration for creators whose works are disseminated in the digital ecosystem, seems to be biased. This means that right holders’ rights were prioritized while hosting ISSPs’ and internet users’ interests were subordinated.⁴²⁸

⁴²³ Hereinafter EU Commission Proposal, for the full text of Article 13 of the EU Commission Proposal for a Copyright Directive in the Digital Single Market see Appendix I.

⁴²⁴ EU Commission, “State of the Union 2016: Commission proposes modern EU copyright rules for European culture to flourish and circulate” (Strasbourg 14 September 2016) is available at <http://europa.eu/rapid/press-release_IP-16-3010_en.htm> last accessed 28 December 2019.

⁴²⁵ EU Commission, “A Digital Single Market Strategy for Europe” {SWD (2015) 100 final} Brussels, 6.5.2015 COM (2015) 192 final.

⁴²⁶ EU Commission, “Press release on Digital Single Market Creating a Digital Single Market European Commission actions since 2015” (June 2018) is available at <http://ec.europa.eu/information_society/newsroom/image/document/2018-25/creatingadigitalsinglemarket-europeancommissionactionssince2015pdf_996FEA88-AD3C-940E-050B64C9A7B33CF5_53055.pdf> last accessed 27 December 2019.

⁴²⁷ EU Commission, “Public Consultation on the Review of EU Copyright Rules” (2013) 1.

⁴²⁸ O. Fischman Afori, “Universal measures in the service of global challenges: proportionality, blocking orders, and online intermediaries as hybrid bodies” in T. Synodinou, *Pluralism or Universalism in international copyright law* (Kluwer Law International 2019) 657.

The provision that addressed the liability of hosting ISSPs is to be found in Article 13 of the EU Commission’s Proposal, which is now Article 17 of the final draft of the DSMD. Article 13 of the EU Commission’s Proposal introduced a set of obligations for ISSPs. Following the definition of information society service providers (ISSPs) as enshrined in the ECD, Article 13 of the Proposal noted that hosting ISSPs shall enter into license agreement with rights holders and deploy appropriate measures to ensure the right functioning of those agreements. Yet, as Article 13 of the Proposal noted, this is an obligation only for those ISSPs who are not eligible to the liability immunity provisions under Article 14 of the ECD. *A contrario*, for those ISSPs who fall outside the scope of Article 14 of the ECD, Article 13 of the Proposal assumes that they have an active role. What amounts to active role has been described in Recital 38 of the Proposal, which notes that the provider must go “beyond the mere physical facilities” or “optimising the presentation of the uploaded works or subject matter or promoting them, irrespective of the nature of the means used therefor.”⁴²⁹ While the latter understanding of what constitutes an active provider has already been confirmed at judicial level with the *L’Oreal v eBay* case in the CJEU,⁴³⁰ this does not mean that ISSPs with an active role are excluded from liability immunity provisions. Rather, pursuant to the *L’Oreal v eBay* ruling, hosting ISSPs who offer hosting services and have an active role may still be eligible to the liability exemption under Article 14 of the ECD.⁴³¹ Therefore, confusion has emerged with regard to the stances where hosting ISSPs are subject to liability immunity provisions and on which stances they are not.

Further, another point of the EU Commission Proposal that has been subject to criticism is the notion of storing and providing access to large amounts of copyrighted material. Both definitions were new and might be subject to different interpretations. Some scholars have argued that the notion of providing access to large amounts of copyrighted works amounts to communication to the public.⁴³² If so, this means that the Proposal slightly opens the door for attributing primary liability rules to hosting ISSPs. Yet, given

⁴²⁹ Recital 38 of the Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM/2016/0593 final .

⁴³⁰ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011, para. 116.

⁴³¹ S. Stalla-Bourdillon, “Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well” in M. Taddeo and L. Floridi (eds.) *The Responsibilities of Online Service Providers* (2017) 281; E. Rosati, “Why a Reform of Hosting Providers’ Safe Harbour is Unnecessary Under EU Copyright Law” (2016) 38 *European Intellectual Property Review* 668.

⁴³² G. Frosio, “To filter or not to filter? That is the question in EU Copyright Reform” (2018) 36 *Cardozo Arts and Entertainment Law Journal* 342.

that the wording is vague, it was not possible to be sure about the intentions of the European policymakers who drafted this provision at that time.

Moreover, pursuant to Article 13, the obligations that hosting ISSPs must follow give rise to mounting concerns. This is because they are either non-feasible as such or they might pose serious threats to internet users' fundamental rights. In particular, Article 13 notes that hosting ISSPs must enter into licensing agreements or deploy filtering mechanisms. On the one hand, with regard to licensing agreements, it seems an "impossible feat"⁴³³ for hosting ISSPs to license all the works. On the other hand, this means that in order to comply with the obligation and prevent the availability of unauthorized works with their networks, hosting ISSPs are forced to deploy filtering technologies. Such filtering mechanisms have attracted negative criticism and, without any safeguard, might encroach upon users' fundamental rights.⁴³⁴ This is mainly due to the "dangers" this kind of technological measures could trigger.⁴³⁵

It is these risks of violations of the rights of internet users that urged Germany to address a question to the legal service of the Council to clarify the issue of content identification filtering technology as set forth in Article 13 of the Proposal for the DSMD. The question reads as following:

"How do Article 13 and Recital 38 of the draft relate to the liability privileges for service providers that have been established in the Directive on electronic commerce (2000/31/EC)? How could Article 13 of the draft be put in more clear terms?"⁴³⁶

This question seems plausible since filtering or blocking technology could create a serious threat for hosting ISSPs, namely encroaching upon their freedom to conduct business. The right to conduct business is guaranteed pursuant to Article 16 of the EU Charter of Fundamental rights and dictates the right of each person to "pursue a business without

⁴³³ J. Reda, "The text of Article 13 and the EU Copyright Directive has just been finalised" (Julia Reda's website, 13 February 2019) is available at <<https://juliareda.eu/2019/02/eu-copyright-final-text/>> last accessed 28 December 2019.

⁴³⁴ F. La Rue, "Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression" (13 June 2018) is available at <<https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-OTH-41-2018.pdf>> last accessed 27 December 2019.

⁴³⁵ M. Senftleben and others, "The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform" (2017) is available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3054967> last accessed 17 June 2019.

⁴³⁶ Council of the European Union (18 September 2017) Interinstitutional File: 2016/0280 (COD) is available at <<http://data.consilium.europa.eu/doc/document/ST-12291-2017-INIT/en/pdf>> last accessed 7 January 2020.

being subject to either discrimination or disproportionate restrictions.”⁴³⁷ Within the context of ISSPs, the right of freedom to conduct business was invoked for the first time in the *Scarlet Extended* case⁴³⁸ where the CJEU examined the issue of an injunction for the implementation of filtering technology in order to terminate or mitigate the online infringements. According to the Court, while intellectual property rights are fundamental rights as per Article 17(2) of the Charter of Fundamental Rights of the European Union, this does not mean that the right is inviolable. Rather the protection of intellectual property rights should be in conjunction with the other fundamental rights. For this reason, “in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures.”⁴³⁹ In this light, the Court found that a filtering system would constitute a serious infringement of the hosting ISSPs’ freedom to conduct business since the system would be expensive and the hosting ISSP should bear also the costs for the implementation. The equilibrium between different interests at stake has not been reached because the measure is disproportionate and comes in conflict with Article 3 of the Enforcement Directive that notes that “Those measures, procedures and remedies shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the creation of barriers to legitimate trade and to provide for safeguards against their abuse.”⁴⁴⁰

What is more, the implementation of filtering or blocking- based technology may impinge upon the freedom of expression of the users. As Zittrain points out, blocking or filtering injunctions against online platforms should be treated with skepticism as they must abide by “changes to information technologies which are themselves quite frequently speech-related.”⁴⁴¹ This is because the filtering technology cannot distinguish the lawful and unlawful content and might block the dissemination of legal material or the continuation of lawful activities. There are many examples where the legal activities of users have been

⁴³⁷ European Union Agency for Fundamental rights, “Report on Freedom to conduct a business: exploring the dimensions of a fundamental right” (2015) 21 is available at <file:///C:/Users/bc810741/Downloads/fra-2015-freedom-conduct-business_en.pdf> last accessed 27 December 2019.

⁴³⁸ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

⁴³⁹ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

⁴⁴⁰ Council Directive (EC) 2004/48/EC on the enforcement of intellectual property rights (2004) O.J. L 157.

⁴⁴¹ J. Zittrain, “A History of Online Gatekeeping” (2006) 19 *Harvard Journal of Law and Technology* 253.

restricted by filtering software regardless of the fact that YouTube declares that this kind of measures perform satisfactory outcomes.⁴⁴² This can be seen in a case where YouTube removed a video of a University lecture delivered by a Harvard Law Professor. This happened because the Professor, during his lecture, included samples of lyrics of popular songs. However, the video was lawful because it was for educational purposes.⁴⁴³ Hence, the filtering obligation could restrict at certain extent the freedom of speech.

The importance of respecting the freedom of expression of the subscribers in light of blocking or filtering injunctions has been highlighted at European level. For instance, the preamble of the InfoSoc Directive stresses that any measure to be adopted must be in “compliance with the fundamental principles of law and especially of property, including intellectual property, and freedom of expression and the public interest.”⁴⁴⁴ In this vein, para. 9 of the Preamble of the ECD highlights that “directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of freedom of expression as per [Article 10(1) ECHR]⁴⁴⁵ subject only to the restrictions laid down in paragraph 2 of that Article.”⁴⁴⁶

The importance of respecting the freedom of expression of the users has preoccupied the court’s legal arena too. In the landmark case of *Yildirim v Turkey* case,⁴⁴⁷ the European Court of Human Rights highlighted the danger of violating the rights of expression of users and endorsed more precise circumstances on how the blocking technology should be implemented in order to strike a fair balance between the different interests at stake. In

⁴⁴² J. Reda, “When filters fail: These cases show we can’t trust algorithms to clean up the internet” (28 September 2017) available at < <https://juliareda.eu/2017/09/when-filters-fail/>> last accessed 27 December 2019.

⁴⁴³ Ibid.

⁴⁴⁴ Preamble of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.

⁴⁴⁵ Article 10 of the EU Charter of Fundamental Rights– Freedom of expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. “The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

⁴⁴⁶ Preamble of the 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.

⁴⁴⁷ *Ahmet Yildirim v Turkey* (18 December 2012) Application no. 3111/10; For a commentary of the case see <<https://globalfreedomofexpression.columbia.edu/cases/ahmed-yildirim-v-turkey/>> last accessed 27 December 2019.

the case at hand, a Turkish national operated a website hosted by “Google Sites” portal. In 2009 the Criminal Court in Turkey ordered a blocking injunction against a website that insulted the memory of Kemal Ataturk. That website was hosted also by the “Google Sites” portal. The Turkish Telecommunication and Data Protection Authority advised the Criminal Court to block access to the entire “Google Sites” portal, thus blocking access to the website of Yildirim as well. For this reason, Yildirim submitted an application to the European Court of Human Rights in Strasbourg arguing that the blocking of Google sites had resulted into collateral censorship, i.e. termination of the access to his own website. In this way, the blocking of his website constituted violation of the right to freedom of expression as enshrined in Article 10 of the European Convention of Human Rights.⁴⁴⁸ According to the Court, a restriction is compatible with Article 10 only if the restriction “is prescribed by law” and meets the demands of a democratic society.⁴⁴⁹ This understanding implies that when a court orders a blocking injunction, it must take into consideration “the scope of the website ban”⁴⁵⁰ and “the guarantee of the judicial review”⁴⁵¹ so as to avoid any violation of European fundamental rights such as the freedom of expression of users. After careful consideration of the facts, the Court held that the blocking of Yildirim’s website was not warranted since there was no connection between the allegedly infringing site and Yildirim’s website, and the blocking of Yildirim’s website was decided after the recommendations of an administrative body, the Telecommunications Directorate, and not based on judicial scrutiny. Therefore, website blocks should stem from a clear legal basis and on the grounds of a thorough court’s assessment.⁴⁵² Otherwise, restricting the freedom of expression without any clear legal basis is unnecessary and disproportionate.

Furthermore, the installation of filtering technology might pose serious risks for the protection of users’ personal data. This is because as the Court noted in *Scarlet v Sabam* “a filtering system would involve a systematic analysis of all content and the collection and identification of users’ IP addresses from which unlawful content on the network is

⁴⁴⁸ European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

⁴⁴⁹ Ibid.

⁴⁵⁰ M. Husovec, “Injunctions against Innocent Third Parties: The case of Website Blocking” (2013) 4 Journal of Intellectual Property, Information Technology and E-Commerce Law para. 19.

⁴⁵¹ Ibid, para. 40.

⁴⁵² ARTICLE 19, “Landmark European court decision finds google ban was a violation of freedom of expression” is available at <<https://www.article19.org/resources.php/resource/3567/en/turkey:-landmark-european-court-decision-finds-blanket-google-ban-was-a-violation-of-freedom-of-expression>> last accessed 27 December 2019_where_Dr. Agnes Callamard, ARTICLE 19 Executive Director noted that “a victory for online freedoms at a time when governments around the world increasingly seek to regulate the Internet.”

sent”.⁴⁵³ This means that in the process of filtering, filtering software identifies the IP addresses of users which is considered, according to the prevailing view, personal data of the users.⁴⁵⁴ This understanding has been mirrored in the opinion of Article 29 Working Party,⁴⁵⁵ which was an independent body of data privacy experts that advises the European Commission on data protection issues.⁴⁵⁶ In particular, the Working Party noted that IP addresses are personal data since "Internet access providers and managers of local area networks can, using reasonable means, identify Internet users to whom they have attributed IP addresses as they normally systematically “log” in a file the date, time, duration and dynamic IP address given to the Internet user. The same can be said about Internet Service Providers that keep a logbook on the HTTP server. In these cases, there is no doubt about the fact that one can talk about personal data in the sense of Article 2 a) of the Directive ...).”⁴⁵⁷

The view that IP addresses are considered personal data becomes more relevant in cases where the process of IP addresses aims to unveil the identity of primary infringers. There are a number of cases outlining an obligation of ISPs to give all the necessary details to the rights holders in order to attack direct infringers. This has also reached the CJEU, which, in *Promusicae* ruling,⁴⁵⁸ held that member states are entitled to request ISSPs to unveil the identity of individual infringers who are also users of their networks. In this regard, should member states decide to allow this possibility, right holders will be provided with information in order to pursue actions against primary infringements. This has not been without challenge however. In Ireland, for instance, in *EMI V Eircom*,⁴⁵⁹ the Irish High Court found that the settlement which had been agreed between record companies and Eircom, an internet service provider, did not infringe privacy and other

⁴⁵³ CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL* (2011) ECR I- 11959.

⁴⁵⁴ CJEU, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL* (2011) ECR I- 11959, para. 51.

⁴⁵⁵ Article 29 Working Party, “Opinion 4/2007 on the concept of personal data” (WP 136, 20 June 2007) 16

⁴⁵⁶ It is now replaced by the European Data Protection Board.

⁴⁵⁷ Recommendations, “WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection” adopted on 21.11.2000.

⁴⁵⁸ CJEU, C-275/06, *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* (2008) ECR I- 00271; Frabboni M, File-sharing and the role of intermediaries in the marketplace” in I. Stamatoudi (ed.), *Copyright enforcement and the Internet* (Kluwer Law International 2010) 132 where she outlines the debate between property versus privacy.

⁴⁵⁹ High Court, *EMI v Eircom* [2009] IEHC 411.

data protection laws since IP addresses are not personal data and cannot identify the subscribers.⁴⁶⁰

Finally, filtering technology itself has an “opaque nature.”⁴⁶¹ This means that, unlike usual practices for censorship that specify the content which should be restricted,⁴⁶² automatic filtering does not entail specific guidance on which material should be targeted. This is because, as the Advocate General in his opinion for *Scarlet v Sabam* stressed, in order for filtering to be effective, “it must be systematic, universal and progressive.”⁴⁶³ This implies that filtering cannot be targeted or narrowed. Rather, filtering is about the monitoring of all the data that is transmitted through the internet service provider.⁴⁶⁴ Yet, this understanding is not compatible with EU Law provisions and mostly it conflicts with Article 15 of the ECD which prohibits general monitoring obligations. Moreover, the opaque nature of filtering enables manufacturers of filtering technology to control which information can reach the end-users and which cannot.⁴⁶⁵ For instance, it has been reported that in Saudi Arabia the filtering software of Smart Filter has blocked the access to websites with non-pornographic gay material. After severe criticism from human rights organizations, the Saudi Arabian government abolished the unreasonable blocking and permitted the access to these websites.⁴⁶⁶ Thus, the opaque nature of filtering leaves space for potential abuses which could be used from states or private entities in order to satisfy their own interests

What is more, these obligations must be undertaken indiscriminately by all hosting ISSPs. This means that commercial as well as non-commercial hosting ISSPs must either enter into license agreements or deploy filtering technologies. As mentioned earlier, the

⁴⁶⁰ T. Train, “Three Strikes’ settlement between EMI and Eircom approved by Irish court” (Weblog of the Journal of Intellectual Property Law and Practice) is available at < <http://jiplp.blogspot.co.uk/2010/08/three-strikes-settlement-between-emi.html> > last accessed 27 December 2019.

⁴⁶¹ T.J. McIntyre and C. Scott, “Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility” in Brownsword and Yeung (eds.) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008).

⁴⁶² Ibid.

⁴⁶³ Case C-70/10, Opinion of AG Cruz Villalon on *Scarlet Extended SA v Société Belge des auteurs compositeurs et éditeurs (SABAM)* (2011) ECLI:EU:C:2011:255, para. 48.

⁴⁶⁴ C. Angelopoulos, “Filtering the Internet for copyrighted content in Europe” (2009) Legal Observations of the European Audiovisual Observatory 3.

⁴⁶⁵ T.J. McIntyre and C. Scott, “Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility” in R. Brownsword and Yeung (eds.) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing 2008) 3.

⁴⁶⁶ N. Villeneuve, “The Filtering Matrix: Integrated Mechanisms of Information Control and the demarcation of borders in cyberspace” (2006) 11 First Monday is available at < <https://journals.uic.edu/ojs/index.php/fm/article/view/1307/1227> > last accessed 27 December 2019.

obligation to enter into licensing agreements is non-feasible. For this reason, hosting ISSPs might resort to filtering mechanisms. However, to force non-commercial ISSPs to apply filtering technology might have a corrosive effect on their business welfare. For instance, the non-profit website Wikipedia, which lacks any financial resources to either develop in-house its own technology or license filtering technology from others, would be forced to terminate its business.⁴⁶⁷

Finally, Article 13 of the EU Commission Proposal encourages the cooperation between right holders and hosting ISSPs. For instance, it urges providers to inform right holders for the functioning of the agreements. In case they do not enter into agreement, they will cooperate with hosting ISSPs to develop best practices to tackle infringement online. However, such a cooperation might prompt reflections on the methods that would be agreed between right holders and hosting ISSPs⁴⁶⁸ and whether such methods would be “one-sided” and thus would not take into consideration the fundamental rights of Internet users.

B. European Council’s text for the Copyright in the Digital Single Market Directive (DSMD)

The EU Council’s text of 25 May 2018 follows the pathway of the European Commission’s Proposal but with a few thorny amendments on board.⁴⁶⁹

Firstly, Article 13 of the EU Council’s compromised text deviates from the definition of hosting ISSPs.⁴⁷⁰ Instead, it uses the term online content sharing service providers

⁴⁶⁷ G. Sartori, “Providers liability: From the ECD to the Future: In depth analysis for the IMCO Committee” (2017) IMCO Committee 14 is available at <[http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA\(2017\)614179_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf)> last accessed 27 December 2019.

⁴⁶⁸ U. Carsten, “Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective” (2017) 8 Journal of Intellectual Property, Information Technology and E-Commerce Law 116; E. Bonadio, “File Sharing, Copyright and Freedom of Speech” (2011) 33 E. I. P. R 628 where E. Bonadio argues that “the “transformation” of ISPs into copyright enforcement agents is probably a consequence of a quid pro quo strategy. There are signals that ISPs act as entertainment industry enforcement agents in exchange for them acquiring the right to transmit copyright holders’ programmes over their internet networks” in; at US level, A. Bridy, “Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement” (2010) 89 *Oregon Law Review* 101 where Bridy found that “In 2005, the same year the Eighth Circuit decided *Charter*, Verizon entered into an agreement with Disney to forward notices of infringement, in return for which it received the right to transmit certain Disney programming over its network” in; See also N. Anderson, “Verizon to forward RIAA warning letters (but that’s all) Verizon looks set to forward RIAA copyright infringement notices to its ...” (Arstechnica, 13 November 2009) is available at <<https://arstechnica.com/tech-policy/2009/11/verizon-to-forward-riaa-warning-letters-but-thats-all/>> last accessed on 27 December 2019.

⁴⁶⁹ For the full text of Article 13 of the EU Council text for the Copyright in the Digital Single Market Directive see Appendix II.

⁴⁷⁰ For the full EU Council text on DSMD see Appendix II.

(OCSSPs).⁴⁷¹ Such a term, however, is a novelty for the online world and marks a shift from the definition of hosting providers which is enshrined in the ECD. As per the ECD, hosting ISSPs are online marketplaces, social networks and blogs, and are, broadly speaking, all those providers who offer hosting services to users' content. However, under the definition of content sharing providers, only those providers who store and provide access to content are included. Such providers are those profit-based providers such as Facebook, YouTube and Google. In contrast, Wikipedia and other non-profit websites are excluded from the scope of online content sharing providers.⁴⁷²

Further, the EU Council's text endorses primary liability rules for online content sharing providers. This is because, it notes that "Member States shall provide that an online content sharing service provider performs an act of communication to the public or an act of making available to the public when it gives the public access to copyright protected works or other protected subject matter uploaded by its users." This means that OCSSPs will be liable for any infringing material their users' upload without having the defense of knowledge. This is because knowledge is a requirement for establishing secondary liability and not primary liability. Yet, as a corollary to the introduction of primary liability rules, a paradox might emerge. Two different regimes occur, which might create confusion to the parties involved. For instance, consider when a right holder initiates legal proceedings against an OCSSP for copyright infringement within its platform. On the one hand, OCSSPs might argue that under the e-commerce framework they were exonerated from liability since they did not have knowledge of the illicit activity while right holders under the DSMD might argue that online content sharing providers are still liable since knowledge is not requirement for primary liability.⁴⁷³

However, in order to avoid primary liability, OCSSPs must take authorisation from right holders. By taking this authorisation through the conclusion of agreements, users would benefit since their activities would not amount to copyright infringement anymore. However, as already discussed in the European Commission Proposal, taking authorisation for all copyrighted works seems impossible. This is because rights clearance

⁴⁷¹ Hereinafter OCSSPs.

⁴⁷² V. Moscon, "The Council Negotiating Position on Article 13: Warning, Creators are also Part of the Game!!!" (Kluwer copyright blog, 4 July 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/07/04/council-negotiating-position-article-13-warning-creators-also-part-game/>> last accessed on 27 December 2019.

⁴⁷³ G. Frosio, "Filter or not to filter? That is the question in EU Copyright Reform" (2018) 36 *Cardozo Arts and Entertainment Law Journal* 352.

licenses provided by collecting societies cover only works from their members and not those works from non-members. In this sense, there would always be an option for holding OCSSPs liable since the license cannot cover all types of content users upload on their platforms.⁴⁷⁴

If no such authorisation is given, the EU Council's text notes that OCSSPs can escape liability if they fulfil the following requirement. They must demonstrate either that they made the best efforts to prevent the availability of infringing works within their platforms or they have acted expeditiously and remove it upon being notified. However, when it comes to the interpretation of the term "best efforts", one might wonder what constitutes "best efforts" and in particular, what kind of measures OCSSPs must deploy.

Further, Article 13 of the EU Council text specifies that the measures which must be deployed shall be effective and proportionate. In order for the measures to be effective and proportionate, a number of factors must be taken into consideration. In particular, "the size and the nature of the services" provided by the online content sharing provider, "the amount and type of uploaded works" and "the availability and costs. While this understanding seems reasonable, it is can only be assessed case by case. For this reason, legal uncertainty may arise.

What is more, the provision notes that such measures shall be defined by right holders and OCSSPs so that they function effectively. However, as already discussed in the EU Commission Proposal, the cooperation between OCSSPs might result to one sided methods, thus subordinating the rights of internet users. This understanding is aggravated by the fact that the measures will be economically affordable for the OCSSPs and effective. This provision might lead to the use of cheap and limited efficiency filtering technology that might be prone to a high margin of errors and thus lead to over blocking of lawful content.

In order to appeal the blocking of legitimate content, users can resort to the complaints and redress mechanisms offered by the OCSSPs. Following the line of the EU Commission's Proposal, the EU Council's text encourages the establishment of complaints and redress mechanisms as well.⁴⁷⁵ Yet, here it could be argued that self-regulatory

⁴⁷⁴ M. Senftleben, "Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market" (2019) Vrije Universitat 3.

⁴⁷⁵ See Appendix II.

measures do not always guarantee the fundamental rights of users. For instance, it has been found that YouTube's complaints dispute procedure can last up to one month, thus leaving users in legal uncertainty about their rights.⁴⁷⁶

Finally, the EU Council's text suggests the establishment of independent bodies. Such independent bodies will be in charge of evaluating complaints with regard to the measures online content sharing providers have deployed in order to prevent the availability of infringing material within their platforms. However, while the creation of an independent authority would welcome, this shift from judicial control to administrative control might prompt reflections on the legitimacy and accountability of this authority since the principles under which the authority functions are not clearly carved out.

C. EU Parliament's compromised text for the Copyright in the Digital Single Market Directive

In similar fashion, the EU Parliament's compromised Text adopts the same approach with the EU Council, without great amendments.⁴⁷⁷ After being rejected in the first vote in July 2018, the EU Parliament voted again in September 2018 in the plenary session in Strasbourg. This time 438 MEPS voted in favour of the DSMD against 226.⁴⁷⁸

Thus, EU Parliament's text redeploys the language of the EU Council's text and notes that OCSSPs perform an action of communication and therefore they should conclude licensing agreements. Bringing forward again primary liability rules, the EU Parliament confirms the seismic shift from secondary liability norms to primary liability rules for hosting ISSPs' activities, as this has been observed in the EU Council's text as well.

The EU Parliament's text continues by noting that if online content sharing service providers do not wish to conclude licensing agreements with rights holders, then they shall cooperate with right holders to prevent the availability of unauthorized works within their networks.⁴⁷⁹ In order to do so, they shall decide methods which must be compatible

⁴⁷⁶ A. Bridy and D. Keller, "U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry" (30 March 2016) 18 is available at <<http://cyberlaw.stanford.edu/publications/us-copyright-office-section-512-study-comments-response-notice-inquiry>> last accessed 27 December 2019.

⁴⁷⁷ For the full text of Article 17 of the EU Parliament for a Copyright Directive in the Digital Single Market see Appendix III, IV.

⁴⁷⁸ N. Bernal, "EU Parliament approves sweeping digital copyright reforms" (The Telegraph, 12 September 2018) is available at <<https://www.telegraph.co.uk/technology/2018/09/12/eu-parliament-approves-sweeping-copyright-reforms-reshape-internet/>> last accessed 7 January 2020.

⁴⁷⁹ See Appendix III, IV, V.

with fundamental rights, do not restrict lawful content from being available and avoid the use of automated blocking mechanisms. Yet, one might wonder what practices will be decided between rights holders and online content sharing services so as to tackle the circulation of infringing material within their networks. As explained earlier in EU Council's text, practices defined between industry representatives and online content sharing providers might be biased towards the interests of rights holders and providers, thus undermining users' interests.

Moreover, following the EU Council's text, the EU Parliament's text encourages a self-regulatory approach by addressing the establishment of effective redress mechanisms where users can submit their complaints in case their content has been unreasonably removed. Such complaints will be dealt with without delay and be subject to human review. Here, however, it is possible to add that the review of all complaints by users will require a high number of employees with expertise knowledge in copyright law, which in turn will give rise to the transaction costs of online service providers. Yet, this review of complaints will be in accordance with the General Data Protection Regulation (GDPR)⁴⁸⁰ that prohibits any inaccurate and non-proportionate processing of personal data.⁴⁸¹

Finally, Member states shall establish an independent body for disputes as well as provide an alternative resolution mechanism for users whose rights have been violated by the measures adopted by online content sharing providers. However, as already observed, it is crucial to specify the principles under which this independent body will operate with a view to enhance the legitimacy of its decisions. Otherwise, such an independent body will lack legitimacy.

Hence, it seems that the EU Parliament's text of the DSMD includes the problematic features that have already been identified in the previous texts of the EU Commission and the EU Council.

⁴⁸⁰ Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) OJ L 119 (hereinafter GDPR).

⁴⁸¹ G. Buttarelli, "Comments of the European Data Protection Supervisor on Article 13 of the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market" (3 July 2018) is available at https://edps.europa.eu/sites/edp/files/publication/18-07-03_cover_letter_comments_copyright_en.pdf last accessed 28 December 2019.

Yet, in order to finalize the final text of the DSMD, the following step in the legislative process are the dialogues between the three main European Institutions, EU Commission, EU Parliament and the EU Council. So, after the vote of the EU Parliament for its compromised text in September 2018, dialogues started. However, due to the severe controversy that revolved around this Directive, instead of them lasting for 4 months, which was the initial plan, they lasted until March. It was on the 26th of March 2019 where three main European Institutions compromised and finalized the final draft of the DSMD which was passed by the EU Parliament in the plenary session in Strasbourg with 348 EU Parliamentarians in favour and 274 against.

Overall, it could be extrapolated that the EU Commission's Proposal, and the EU Council's and the EU Parliament's texts have raised problematic aspects. Such problematic aspects are relating to the introduction of primary liability rules for OCSSPs, the creation of a specific category of hosting ISSPs, the imposition of monitoring obligations, licensing requirements, and the creation of self-redress mechanisms operated by OCSSPs in case of complaints by their users. Unsurprisingly, as demonstrated below, many of these problematic aspects are to be found in the final draft of Article 17 of the DSMD. These problematic aspects that are critically assessed in the following section so as to underline the need for a legal reform that is presented in Part II of this thesis. This examination provides a discussion of the flaws of Article 17 of the DSMD that addresses OCSSPs' liability for copyright infringements.

III. Article 17 of the DSMD: Problematic features

Recital 64 of the DSMD notes that "It is appropriate to clarify in this Directive that online content-sharing service providers perform an act of communication to the public or of making available to the public when they give the public access to copyright protected works or other protected subject matter uploaded by their users." This means that one of the underlying objectives of Article 17 of the DSMD⁴⁸² is to provide clarifications to the existing *EU acquis* that deals with ISSPs' liability. However, instead of clarifying the law, Article 17 makes fundamental amendments to the law. Indeed, Bridy points out that the DSMD "changes the rules of the game."⁴⁸³

⁴⁸² For the full text of Article 17 of the DSMD see Appendix VI.

⁴⁸³ A. Bridy, "EU Copyright Reform: Grappling with the Google Effect" (2019) *Vanderbilt Journal of Entertainment & Technology Law* 26.

This is because Article 17 deviates from the existing liability regime of ISSPs and introduces not only new liability rules but also an array of amendments that create legal uncertainties and are highly controversial. As demonstrated below, the final text of Article 17 (previously named Article 13 in the EU Commission's Proposal, EU Council's and EU Parliament's texts) follows the same rationale of the compromised texts. In particular, in some stances it adopts the same wording while other controversial aspects that have been identified in the compromised texts have been lowered due to the high controversy that revolved around them.

In this light, the following section aims to identify and critically assesses the problematic aspects of Article 17 of the DSMD. Those problematic features include the new definition of online content-sharing service providers, the introduction of primary liability rules, the option of online content-sharing service providers to conclude a license agreement with right holders, the option of online content-sharing service providers to demonstrate that they made the best efforts to terminate any illicit activity within their networks, the provision addressing the prohibition for general monitoring obligations and the creation of redress mechanisms for online disputes with regard to copyright infringements.

A. The new definition of Online Content-Sharing Service Providers (OCSSPs)

The first problematic feature of Article 17 of the DSMD is that it introduces a new definition for hosting ISSPs that host copyright content online into the regulatory framework of ISSPs. Following the definition that has been used in the EU Council's and EU Parliament's texts and abandoning the definition which has been adopted in the EC's Proposal, this new type of hosting ISSP is called online content-sharing service provider (OCSSP) and seems to be a sub-set of hosting ISSPs as set forth in Article 14 of the ECD. Under the scope of OCSSPs fall popular music-exchange platforms such as YouTube, Vimeo, Dailymotion and Instagram as well as any platform where users can upload content online. This understanding has been clearly illustrated in Recital 62 of the DSMD which narrows the scope of the OCSSPs to those whose services are "to store and enable users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit therefrom, either directly or indirectly, by organizing it and

promoting it in order to attract a larger audience, including by categorizing it and using targeted promotion within it.”⁴⁸⁴

This of course does not mean that all online platforms that host content fall within the scope of Recital 62. Rather, certain platforms are excluded from the scope of OCSSPs. Indeed, non-profit platforms, online marketplaces, cloud services are not within the scope of the Directive. Thus, as per Article 2 (6) of the DSMD “Providers of services, such as not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and sharing platforms, electronic communication service providers as defined in Directive (EU) 2018/1972, online marketplaces, business-to-business cloud services and cloud services that allow users to upload content for their own use, are not ‘online content-sharing service providers’ within the meaning of this Directive.”⁴⁸⁵

Otherwise, Article 17 would include all the hosting providers that fall under the scope of Article 14 of the ECD and in this sense two provisions at the European level would regulate the same types of hosting ISSPs with a different legal system.⁴⁸⁶ What is more, the non-exclusion of certain hosting ISSPs from the scope of Article 17 would supersede the aim of the DSMD, which is to close the value gap between creators and hosting ISSPs.⁴⁸⁷ This would imply that hosting ISSPs that are not connected with the music or film industry sector would fall into the regime of Article 17 and thus, this would pose serious threats to their business model. For instance, if Wikipedia, a non-profit platform, fell into the scope of Article 17, it would be forced to shut down its business since it would be impossible for a non-profit platform to have the resources to prevent the posting of unlawful content, while at the same time it would be impossible to pay damages to the relevant right holders.

Interestingly, whilst the exclusion from the scope of OCSSPs non-profit platforms such as Wikipedia and open source software platforms seems sensible,⁴⁸⁸ it raises the question as

⁴⁸⁴ Recital 62 of Council 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.

⁴⁸⁵ Council 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.

⁴⁸⁶ A. Bridy, “EU Copyright Reform: Grappling with the Google Effect” (2019) *Vanderbilt Journal of Entertainment & Technology Law* 22.

⁴⁸⁷ G. Frosio and S. Mendis, “Monitoring and Filtering: European Reform or Global Trend” (2019) *Center for International Intellectual Property Studies Research Paper* 21.

⁴⁸⁸ See Concluding remarks of Part I.

to why cyber lockers, online marketplaces and cloud services do not fall into the scope of online content sharing service providers since they also give access to copyrighted content. For example, online marketplaces such as Amazon or eBay offer tangible as well as non-tangible goods to their online consumers. Non-tangible goods are understood as Kindles or other DVDs which are offered by online marketplaces and can be viewed as YouTube videos.⁴⁸⁹ In addition, with regard to cloud services, although the main function of cloud service providers is to store material online, they can also give access to copyright-protected content by providing links via Dropbox files.⁴⁹⁰

Finally, the need for introducing the new definition of OCSPs could be questioned since there has not been criticism or concerns raised regarding the definition of hosting ISSPs as set forth in Article 14 of the ECD. For instance, to my knowledge, the outcomes of the European Commission's Public Consultation on the Review of European Copyright rules raised problematic issues that revolve around online regulation, but it seems that the relevant stakeholders did not argue that a need for a new definition for hosting ISSPs was required.⁴⁹¹ Likewise, the outcomes of the Public Consultation on e-commerce did not demonstrate any need for amending or introducing a new definition for hosting ISSPs.⁴⁹² In contrast, they focused on the need for a legal reform with regard to liability rules that regulate ISSPs' online activities by noting that "liability regime introduced in Section IV of the ECD (Articles 12-15) has proven not fit for purpose or has negatively affected market level playing field."⁴⁹³ Finally, the summary of the outcomes of the Public Consultation on the modernization of IPR enforcement did not include the importance for a new definition for ISSPs.⁴⁹⁴ In contrast, many stakeholders argued that the introduction of a new definition for ISSPs might create inconsistency with the definition that is set forth in Article 14 of the ECD and thus lead to legal uncertainty.

⁴⁸⁹ M. Husovec, "Compromising (on) the Digital Single Market? A Quick Look at the Estonian Presidency Proposal(s) on Art 13" (Kluwer copyright blog, 8 September 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/09/08/compromising-digital-single-market-quick-look-estonian-presidency-proposals-art-13/>> last accessed 28 December 2019.

⁴⁹⁰ Ibid.

⁴⁹¹ EU Commission, "Report on the responses to the Public Consultation on the Review of the EU Copyright Rules", Directorate General Internal Market and Services, Directorate D – Intellectual property, D1 – Copyright (July 2014).

⁴⁹² Ibid.

⁴⁹³ EU Commission, "Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC)" (2010).

⁴⁹⁴ EU Commission, "Public Consultation on the evaluation and modernization of the legal framework for the enforcement of intellectual property rights: Summary of responses" (2016).

Therefore, the introduction of a new type of hosting ISSPs, namely online content-sharing service providers might prompt reflections among right holders and hosting ISSPs as to which hosting ISSPs fall into its scope, what would happen if a hosting ISSP does not qualify as an OCSSP but its services fall into the scope of Article 17 of the DSMD well as the practical necessity for introducing this new type of hosting ISSPs.

B. The introduction of primary liability rules

Another problematic feature of Article 17 of the DSMD is the introduction of primary liability rules for this new type of hosting ISSPs, the so called OCSSPs. Following the EU Commission's and EU Parliament's compromised texts, this understanding was reiterated in the final text of the DSMD. So, Article 17 of the DSMD confirms the departure from secondary to primary liability rules by noting that "Member States shall provide that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users."⁴⁹⁵ As per Article 3 of the InfoSoc Directive, communication to the public constitutes primary infringement.⁴⁹⁶ Therefore, OCSSPs commit a primary infringement by carrying out acts of communication to the public.

This new provision signals a landmark shift from the traditional legal regime for hosting ISSPs which is dictated under Article 14 of the ECD. As per Article 14, hosting ISSPs can escape liability if they are now aware of the illicit activity or upon being made aware of this illicit activity, they are required to expeditiously remove the infringing content. This means that knowledge is a requisite element in order to attribute liability rules to hosting ISSPs. In contrast, primary liability rules, which are now endorsed in Article 17 of the DSMD do not require the element of knowledge. So, under Article 17 OCSSPs are held liable for any copyright infringement that might take place on their networks without being aware of them.

The new liability regime under Article 17, however, conflicts with secondary tortious liability theories which are the legal basis upon which ISSPs' regulatory framework has been developed. Given that OCSSPs are a sub-set of hosting ISSPs, this conflict applies to

⁴⁹⁵ 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.

⁴⁹⁶ Council Directive (EC) 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (2001) O.J. L 167 (Hereinafter InfoSoc Directive).

hosting ISSPs as well. Secondary tortious liability theories, as presented in chapter 2, are the main theoretical underpinnings for ascribing liability rules to hosting ISSPs for the actions of their users. Such theories support that for moral or utilitarian reasons,⁴⁹⁷ hosting ISSPs might be held liable for enabling the circulation of infringing content within their networks. However, secondary liability rules might arise only if hosting ISSPs are aware of the infringing content that is disseminated within their networks. What is more, these theories constitute the main tool that offers a safe harbor to hosting ISSPs and boosts e-commerce in its infancy.⁴⁹⁸ Without secondary liability rules, it would be doubtful as to how European hosting ISSPs could compete with their American rivals since the relevant legislative tool, the DMCA, dictates that only under specific conditions of having knowledge of the infringing content online, can OCSSPs be held liable.

Nevertheless, while primary liability rules seem to contradict with secondary tortious liability upon which the rationale of hosting ISSPs' regulatory framework has been developed, there is a line of case law that reiterates the trend towards primary liability rules for ISSPs. Indeed, at European as well as national level, a number of courts imposed primary liability to ISSPs for hyperlinking unauthorized content.⁴⁹⁹ Interestingly, although the line of case law addresses hyperlinking cases, the trend towards primary liability rules could be applied more broadly. To put it more clearly, the trend towards primary liability can be equally applied to cases where material is circulated within online platforms without the permission of the creators.

At European level, this judicial trend has started in the *Svensson*⁵⁰⁰ case in 2014 and continued with the *GS Media*⁵⁰¹ case in 2016 and in the *Brein v Ziggo*⁵⁰² case in 2017 accordingly.⁵⁰³ In all three cases, under the umbrella of communication to the public as

⁴⁹⁷ See chapter 2 II A 1, 2.

⁴⁹⁸ G. Frosio and S. Mendis, "Monitoring and Filtering: European Reform or Global Trend" (2019) Center for International Intellectual Property Studies Research Paper No. 2019-05 5.

⁴⁹⁹ J. P. Quintais, "Untangling the hyperlinking web: In search of the online right of communication to the public" (2018) *The Journal of World Intellectual Property* 408.

⁵⁰⁰ Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB* (2014) EU:C:2014:76.

⁵⁰¹ Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644.

⁵⁰² Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456.

⁵⁰³ Meticulous analysis of the three cases in chapter 2 IV. A; see also E. Papadaki, "Hyperlinking, making available and copyright infringement: lessons from European national courts" (2017) *8 European Journal of Law and Technology* 2-14.

per Article 3 of the InfoSoc Directive,⁵⁰⁴ the CJEU endorsed primary liability rules for hosting ISSPs which redirect users via hyperlinks to unauthorized content.

In particular, the *Svensson* case,⁵⁰⁵ which was a referral from the Stockholm District Court, addressed a dispute between Retriever Sverige, which was a website that redirected its users via links to articles that were published in the websites of journals and a number of journalists. The thorny question that the CJEU was asked to examine was whether hyperlinking constitutes an act of communication to the public within the meaning of Article 3 (1) of the InfoSoc Directive. After a careful examination of the facts, CJEU concluded that hyperlinking constitutes communication to the public if two requirements are fulfilled, namely if there is an act of communication and if there is a new public. The concept of a new public, as the CJEU noted, addresses to the public that the right holder has not included in the initial transmission of her work. Therefore, if those two cumulative requirements are to be fulfilled, a hosting ISSP can be held primarily liable for copyright infringement.

Such a stance was maintained in the *GS Media* ruling⁵⁰⁶ where the CJEU went two steps further by adding two more requirements in order to find a hosting ISSP primarily liable for providing hyperlinks with unauthorized content. This case was about a dispute between Sanoma, the publisher of Playboy Magazine and GS Media, a lifestyle website which contained hyperlinks that redirected Internet users to third parties' websites where nude pictures of a Dutch celebrity had been placed prior to their official release on the Playboy Magazine. In this case as well, the thorny question was whether hyperlinking constitutes an act of communication to the public. Following *Svensson's* ruling,⁵⁰⁷ the CJEU responded in a positive way but added two further requirements. According to the Court's reasoning, hyperlinking constitutes an act of communication to the public if it is an act of communication to a new public and the hosting ISSP knows the illegal nature of the link if it operates on a commercial basis.⁵⁰⁸

⁵⁰⁴ Council Directive (EC) 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (2001) O.J. L 167.

⁵⁰⁵ Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB* (2014) EU:C:2014:76; A. Ohly, "The broad concept of "communication to the public" in recent CJEU judgements and the liability of intermediaries: primary, secondary or unitary liability?" (2018) 13 *Journal of Intellectual Property Law and Practice* 670.

⁵⁰⁶ *GS Media BV v Sanoma Media Netherlands BV and Others*, C-160/15, EU:C:2016:644.

⁵⁰⁷ *Nils Svensson and Others v Retriever Sverige AB*, C-466/12, EU:C:2014:76.

⁵⁰⁸ T. Rendas, "How Playboy Photos Compromised EU Copyright Law: The GS Media Judgment" (2017) 20 *Journal of Internet Law* 11; E. Rosati, "GS Media and Its Implications for the Construction of the Right of Communication to the Public within EU Copyright Architecture" (2017) 54 *Common Market Law Review* 1242.

This outcome implies that the profit-making motive plays a fundamental role as to whether the link provider is primarily liable for hyperlinking unauthorized content. Therefore, if the link provider does not run on a commercial basis, knowledge of the illicit activity is not presumed.⁵⁰⁹ This means that linking is not a primary infringement and thus the link provider is not liable for a primary copyright infringement.

A contrario, if the posting of hyperlinks is carried out for profit, it can be expected that the link provider knows the possible lack of consent of the right holder and thus this amounts to act to communicate to the public. This is because the CJEU noted that if the posting of links pursues financial gains, then the link provider “should carry out the checks necessary to ensure that the work concerned is not illegally published. Therefore, it must be presumed that that posting has been done with the full knowledge of the protected nature of the work and of the possible lack of the copyright holder’s consent to publication on the internet.”⁵¹⁰ Hence, in this case, hyperlinking amounts to unauthorized act of communication to the public unless the lifestyle website can prove that it does not pursue financial gains.

In similar fashion, the CJEU in the *Brein v Ziggo* case confirmed the requirements set out in the *GS Media* case.⁵¹¹ This case, a referral from the Dutch Supreme Court, was about a dispute between an anti-piracy association Stichting Brein that brought legal proceedings against Ziggo, is an internet access service provider, requesting to block access to Pirate Bay. Here again, the thorny question that the CJEU had to examine was whether hyperlinking constitutes an act of communication to the public within the meaning of Article 3 (1) of the InfoSoc Directive. Following the line of reasoning of the *Svensson* and *GS Media* cases, the CJEU held that hyperlinking constitutes an act of communication to the public and thus, the operators of Pirate Bay might be held primarily liable since “by making that platform available and managing it, provide their users with access to the

⁵⁰⁹ Case C-160/15, *GS Media V Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644, para. 47-48; E. Rosati “GS Media and its implications for the construction of the right of communication to the public within EU copyright architecture” (2017) 54 Common Market Law Review 1229.

⁵¹⁰ Case C-160/15, *GS Media V Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644, para. 51.

⁵¹¹ C. Angelopoulos, “CJEU Decision on Ziggo: The Pirate Bay Communicates Works to the Public” (Kluwer copyright blog, 30 June 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/06/30/cjeu-decision-ziggo-pirate-bay-communicates-works-public/>> last accessed 28 December 2019; C. Angelopoulos, “AG Szpunar in Stichting Brein v Ziggo: An Indirect Harmonisation of Indirect Liability” (Kluwer copyright blog, 23 March 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/03/23/ag-szpunar-stichting-brein-v-ziggo-indirect-harmonisation-indirect-liability/>> last accessed 28 December 2019.

works concerned. They can therefore be regarded as playing an essential role in making the works in question available.”⁵¹²

Unsurprisingly, all three rulings have been the subject of heated debate. Many commentators have argued that the rulings are controversial. This is because they not only give a new interpretation to hyperlinking since they equate the act of linking to the act of communication to the public,⁵¹³ but also because they introduce primary liability rules for hyperlinking that can also be applicable to any copyright infringement online. The latter concerns, which are relevant to the core of this thesis, have been confirmed with the DSMD that endorses a primary liability regime for OCSSPs for copyright infringements committed by their users.

Here, it is worth to mention that the ascription of primary liability rules to OCSSPs for copyright violations within their networks has affected the trade mark context as well. In particular, Advocate General Campos Sanchez- Bordona has opined in *Coty v Germany*⁵¹⁴ that Amazon can be held primary liable for trade mark violations within its networks. This is because Amazon is involved in the distribution of fake goods since it offers its auspices for storing them. For this reason, the online market place, as the Advocate General points out, is reasonably expected to identify the pirated goods and prevent their circulation.⁵¹⁵ While the final ruling is expected and seems unsure whether the CJEU will follow the opinion of the Advocate General, this opinion gives us a hint of the potential impact of the new DSMD in trade mark infringements which are ruled under the ECD, as already discussed in chapter 2 of this thesis.⁵¹⁶

What is more, this new type of liability rules for OCSSPs have raised long term discussions among prominent scholars. These discussions surround the legal uncertainties that

⁵¹² Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456, para. 37.

⁵¹³ Case C-160/15, *GS Media V Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644, para. 45: “In that regard, it should be noted that the internet is in fact of particular importance to freedom of expression and of information, safeguarded by Article 11 of the Charter, and that hyperlinks contribute to its sound operation as well as to the exchange of opinions and information in that network characterised by the availability of immense amounts of information.”; E Rosati “GS Media and its implications for the construction of the right of communication to the public within EU copyright architecture” (2017) 54 *Common Market Law Review* 1229; see also M. Leistner, “Intermediary liability in a global world” in T. Synodinou (ed.), *Pluralism and Universalism in international copyright law* (Kluwer Law International 2019) 488 where he argues that this controversy has restricted the spread of the presumption of knowledge at national level and gives the example of Germany where “accordingly, the German Federal Court of Justice has refused to apply the presumption to frame links containing Google’s image search function, since the social utility of such search services as well as their automated, passive mass character precluded a presumption of specific knowledge.”

⁵¹⁴ C- 567/18, *Coty Germany v Amazon*, Opinion of the Advocate General (2019) ECLI:EU:C:2019:1031.

⁵¹⁵ *Ibid*, para. 84.

⁵¹⁶ Article 14 of the ECD addresses the liability of hosting ISSPs in the form of secondary liability rules.

revolve around the introduction of primary liability rules for OCSSPs and their parallel force to the secondary liability regime as set forth in Article 14 of the ECD. In this vein, many scholars argue that Article 17 of the DSMD is considered a *lex specialis* for Article 14 of the ECD.⁵¹⁷ This means that if Article 17 of the DSMD does not apply, for instance, because the hosting ISSP is an online market retailer, Article 14 of the ECD continues to apply. Therefore, Article 14 of the ECD is the general rule and covers a wide spectrum of ISSPs that host and store content online. Should the hosting ISSPs provide services similar to those that are provided by YouTube, Dailymotion or Vevo and are not those that are explicitly excluded pursuant to Article 2 (6) of the DSMD,⁵¹⁸ then Article 17 of the DSMD applies.

Further, other scholars argue that Article 17 of the DSMD constitutes a *sui generis* communication to the public right.⁵¹⁹ This means that Article 17 introduces a new communication to the public right that does not share common elements with the right to communication to the public as enshrined in Article 3 of the InfoSoc Directive. Indeed, Husovec points out that “the newly constituted exclusive right is a communication to the public right only in name.”⁵²⁰

This is because pursuant to Article 3 of the InfoSoc Directive, “Member States shall provide authors with the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access them from a place and at a time individually chosen by them.”⁵²¹ This means that the alleged infringer may be held primarily liable if she broadcasts the work and makes the work available to the public who can access the work at a specific place and time chosen by them.

By contrast, communication to the public under Article 17 of the DSMD does not require the completion of two distinct acts, namely to broadcast the work and make the work it

⁵¹⁷ J. Quintais, “The New Copyright Directive: A tour d’horizon- Part II (of press publishers, upload filters and the real value gap) (Kluwer Copyright Blog, 17 June 2019) is available at < <http://copyrightblog.kluweriplaw.com/2019/06/17/the-new-copyright-directive-a-tour-dhorizon-part-ii-of-press-publishers-upload-filters-and-the-real-value-gap/>> last accessed 27 December 2019.

⁵¹⁸ Council 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.

⁵¹⁹ M. Husovec, “How Europe wants to redefine global online copyright enforcement” in T. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer Law International 2019) 536.

⁵²⁰ Ibid.

⁵²¹ Council Directive (EC) 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (2001) O.J. L 167.

available to the public. Rather, the communication to the public under Article 17 of the DSMD is fulfilled “by the legal presumption of the provision.”⁵²² This means that an infringement of communication to the public takes place if this act is committed by an OCSSP. Therefore, this implies that OCSSPs are subject to primary liability rules which are triggered from a new communication to the public right that applies in parallel with the right of communication to the public under Article 3 of the InfoSoc Directive.⁵²³

However, in order to lower the criticism that revolves around the introduction of primary liability rules for OCSSPs, Article 17 of DSMD provides two possibilities for OCSSPs to avoid primary liability. As per Article 17 (2) (3) OCSSPs must either seek the authorisation of right holders by concluding licensing agreements with them with regard to the use of their works or make the best efforts to terminate the dissemination of unlawful content within their networks. Both requirements, which are discussed below, seem to be contested areas as to how they should be construed in order for OCSSPs to avoid liability for the copyright infringements that their users have committed within their networks.

C. The possibility for OCSSPs to conclude a license

Following the wording of the EU Commission’s Proposal as well as EU Council’s and EU Parliament’s texts, the final text of Article 17 of the DSMD envisages the introduction of a licensing system. This constitutes another problematic feature of Article 17 which places licensing as a default rule for hosting ISSPs so as to exonerate them from liability for copyright infringements that accrue within their platforms. More specifically, Article 17 (2) notes that “Member states shall provide that when an authorisation has been obtained, including via a licensing agreement, by an online content sharing service provider, this authorisation shall also cover acts carried out by users of the services falling within Article 3 of the Directive 2001/29/EC when they are not acting on a commercial basis or their activity does not generate significant revenues.” This implies that a licensing system constitutes the main way for OCSSPs and thus OCSSPs must adapt it to their business model. Lack of licensing content that is disseminated via their networks might result in the liability of OCSSPs.⁵²⁴

⁵²² M. Husovec, “How Europe wants to redefine global online copyright enforcement” in T. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer law 2019) 536.

⁵²³ *Ibid.*

⁵²⁴ A. Bridy, “EU Copyright Reform: Grappling with the Google Effect” (2019) *Vanderbilt Journal of Entertainment & Technology Law* 22.

However, this emphasis on licensing system might be complex⁵²⁵ as it seems difficult to license all material that is disseminated online.⁵²⁶ Indeed, as Senftleben points out that, it burdens OCSSPs with a clearance rights task which cannot be fulfilled.⁵²⁷ The full licensing of the circulated content can only be achieved via umbrella licenses. However, such extended collective licenses that are issued by collective societies cover only works of their members⁵²⁸ and they do not extend to works of right holders who are not their members. In this sense, the dissemination of works of authors without their prior permission might automatically amount to the primary liability of hosting ISSPs despite the fact that they concluded licensing agreements with collective societies.⁵²⁹

What is more, at European level, there is no uniform approach with regard to the extended collective licenses or, as more commonly referred to, umbrella licenses.⁵³⁰ This means that even if OCSSPs decide to resort to collective licenses, they would face a vast array of different licenses from each jurisdiction. This is because the licensing system has not been harmonized so far at European level. For instance, while Article 12 of the DSMD offers a hint of harmonisation for extended collective licensing schemes,⁵³¹ it is unclear how this provision will be transposed in each of the 27 European member states and whether a desirable level of harmonisation would be achieved.⁵³² What is more, the possibility of a pan-European license is limited since a pan-European license issued by collective societies is restricted to works within a specific jurisdiction and does not cover works within other jurisdictions.⁵³³

⁵²⁵ M. Husovec, "How Europe wants to redefine global online copyright enforcement" in T. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer Law International 2019) 531; See also for an opposite view in M. Husovec and J. Quintais, "How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms" (1 October 2019) is available <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011> last accessed 27 December 2019.

⁵²⁶ J. Reda, "The text of Article 13 and the EU Copyright Directive has just been finalised" (Reda's website, 13 February 2019) is available at <<https://juliareda.eu/2019/02/eu-copyright-final-text/>> last accessed 27 December 2019.

⁵²⁷ M. Senftleben, "Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market" (2019) University of Amsterdam 3.

⁵²⁸ J. P. Quintais, "The New Copyright in the Digital Single Market Directive: A Critical Look" (2019) 1 European Intellectual Property Review 18.

⁵²⁹ M. Husovec, "How Europe wants to redefine global online copyright enforcement" in T. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer Law International 2019) 535.

⁵³⁰ M. Senftleben, "Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market" (2019) University of Amsterdam 4.

⁵³¹ *Ibid.*, 4.

⁵³² *Ibid.*, 4; the transposition of the DSMD is still ongoing.

⁵³³ *Ibid.*, 4.

Finally, the conclusion of licensing agreements seems to be rejected by the intellectual property holders themselves. Although the aim of European policy makers to introduce the option of licensing copyrighted content was to safeguard intellectual property holders' rights. The licensing of copyright content would bridge the value gap between right holders' revenues and the dissemination of content online. However, although the rationale of licensing was to protect their rights, right holders seem to disagree with this option. Indeed, right holders have expressed their opposition to conclude licensing agreements with the OCSSPs in the stakeholders meeting that has been organized by the European Commission on the 15th October 2019.⁵³⁴ This is because, as they argue, the experience of collective licensing with ISSPs so far is not appealing. For instance, a number of issues arise with regard to functioning tools that hosting ISSPs deploy in order to identify the allegedly infringing content. Such tools are mainly sound-recording and thus do not prevent the dissemination of infringing content online. Further, many right holders argue that collective licensing agreements are not transparent with relation to the monetization of authors as well as they lack accuracy in reporting the usage of works and the revenues of ISSPs when they enable the circulation of copyrighted content online.⁵³⁵

It is this disagreement that comes to accentuate the problematic feature of concluding licensing agreements as set forth in Article 17 (2) of the DSMD.

Therefore, it seems that concluding licensing agreements would turn to be a very difficult task for OCSSPs. This of course might imply that in order to avoid liability, OCSSPs are forced to resort to the second possibility as envisaged in Article 17 (4) of the DSMD. This possibility, which is analyzed in the following section, addresses the duty for OCSSPs to make the best efforts to either conclude authorisation from copyright holders to use their works or to prevent the dissemination of unauthorized content within their platforms.

D. The possibility for OCSSPs to demonstrate the best efforts

The second possibility for OCSSPs to be exonerated from liability is to demonstrate that they made best efforts to seek authorisation from copyright holders or made best efforts

⁵³⁴ EU Commission, "Press release on first meeting of the Stakeholder Dialogue on Art 17 of the Directive on Copyright in the Digital Single Market" (15 October 2019) is available at <<https://ec.europa.eu/digital-single-market/en/news/first-meeting-stakeholder-dialogue-art-17-directive-copyright-digital-single-market>> last accessed 28 December 2019.

⁵³⁵ Copyright Stakeholders dialogue (15 October 2019) is available at <<https://webcast.ec.europa.eu/copyright-stakeholder-dialogues>> last accessed 7 January 2020.

to impede the circulation of unauthorized content online. More specifically, Article 17 (4) of the DSMD reads as following:

“ (a) made best efforts to obtain an authorisation, and (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the right holders have provided the service providers with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the right holders, to disable access to, or to remove from their websites, the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).”

Similar to the previous paragraphs of Article 17 of the DSMD, this paragraph seems problematic as well for many reasons.

Firstly, as per Article 17 (4), OCSSPs must prove that they made best efforts to gain the permission of right holders for the dissemination of their works. In this way, the impetus to seek authorisation is placed on OCSSPs. Yet, it could be asked what is the level of diligence that must be demonstrated by OCSSPs.⁵³⁶ However, a clear understanding of the level of diligence is missing. As Erikson notes, there is only one unsuccessful attempt to define the concept of diligence in the Orphan Works Directive but at the end it seemed that it had not been fruitful.⁵³⁷

Secondly, as per Article 17 (4) b of the DSMD, such best efforts must be in accordance with industry practices. At the outset, it seems that this paragraph has been agreed in order to minimize the negative criticism that the European Commission’s Proposal has received with the introduction of the concept of “content effective recognition technologies.”⁵³⁸ This concept has drawn severe criticism from academics, who, with a number of public signed statements, were against the imposition of filtering-based technologies and accentuated its negative implications for internet users’ fundamental

⁵³⁶ K. Erikson, “The EU copyright directive creates new legal uncertainties” (LSE Blog, 6 April 2019) is available at <https://blogs.lse.ac.uk/businessreview/2019/04/06/the-eu-copyright-directive-creates-new-legal-uncertainties/> last accessed 28 December 2019.

⁵³⁷ Ibid.

⁵³⁸ Article 13 of the Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM/2016/0593 final - 2016/0280 (COD).

rights.⁵³⁹ So, instead of using this term, the final text of the DSMD used the concept of “industry standards of professional diligence” while at the end it refers to the vague concept of “suitable and effective means”.⁵⁴⁰ Undoubtedly, these wordings seem problematic.

Insofar as industry practices are concerned, a number of examples provide evidence that OCSSPs can conclude agreements with right holders that undermine the rights of internet users and thus lead to censorship. Moreover, with regard to suitable and effective means, this wording can entail a number of tools that could prove efficient to identify the unlawful content and block it. Such tools have already been developed by a number of OCSSPs.⁵⁴¹

Thirdly, Article 17 (4) of the DSMD states that the OCSSPs must make best efforts and not only terminate the dissemination of unlawful content but also prevent the emergence of these infringements in the future. Following the pathway of the EU Commission’s, and the EU Council’s and EU Parliament’s texts,⁵⁴² the final draft of the DSMD introduces a notice and stay down scheme that obliges OCSSPs to stop infringements from reappearing. Yet, this notice and stay down scheme, as already explained in Section II. A, has prompted mounting concerns for its compatibility with the *EU acquis* and, in particular, with existing EU legal provisions and case law. For example, a notice and stay down scheme would require the imposition of filtering-based technological tools that would identify the allegedly infringing content and thus prevent it from reappearing. While European policy makers attempted to eliminate the criticism by endorsing in paragraph 7 that notice and stay down schemes shall take into consideration copyright exceptions such as parody, caricature,⁵⁴³ it is doubtful whether the notice and stay down is not in conflict with the prohibition of general monitoring as envisaged in Article 15 of the ECD as well as with Articles 8, 11 and 16 of the EU Charter of Fundamental Rights that safeguards users’ personal data, right to conduct business and right to information.

⁵³⁹ CREATE, “The Copyright Directive: Articles 11 and 13 must go – Statement from European Academics in advance of the Plenary Vote on 26 March 2019” (CREATE blog, 24 March 2019) is available at < <https://www.create.ac.uk/blog/2019/03/24/the-copyright-directive-articles-11-and-13-must-go-statement-from-european-academics-in-advance-of-the-plenary-vote-on-26-march-2019/> > last accessed 19 September 2019.

⁵⁴⁰ See also A. Bridy, “EU Copyright Reform: Grappling with the Google Effect” (2019) *Vanderbilt Journal of Entertainment & Technology Law* 22-23.

⁵⁴¹ See Chapter 2. IV.C.ii.

⁵⁴² See Appendix II, III and IV.

⁵⁴³ See Appendix VI.

With regard to Article 15 of the ECD, it has been argued that the imposition of content identification technologies seems to be in conflict with Article 15 of the ECD, which is about the prohibition of imposing general monitoring obligations on hosting ISSPs.⁵⁴⁴ In particular Article 15 (1) reads as follows “Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.” This has been considered as the bottleneck of the hosting ISSPs’ regulatory framework since it prevents hosting ISSPs from policing the digital world.⁵⁴⁵

Undoubtedly, a notice and stay down might lead to the use of content identification technology which is all about general monitoring. By general monitoring is meant, as Riordan notes, “a systematic arrangement requiring random or universal inspection.”⁵⁴⁶ The use of such technology will make hosting ISSPs examine their platforms and remove any unlawful material. Therefore, content identification measures are in clear contrast with the prohibition of general monitoring.

The prohibition of general monitoring has been clearly outlined by the CJEU in a number of landmark cases. One of the landmark cases is to be found in the *Scarlet v Sabam*,⁵⁴⁷ Sabam, the Belgian association for authors, requested a filtering injunction against Scarlet, an internet service provider, alleging copyright infringement. Sabam argued that Scarlet’s subscribers used its network in order to file-share unauthorized material via peer to peer. However, the Court refused to issue an injunction under the reasoning that the imposition of a filtering obligation would “oblige it to actively monitor all the data relating to each of its customers in order to prevent any future infringement of intellectual-property rights. It follows that that injunction would require the ISP to carry out general monitoring, something which is prohibited by Article 15(1) of Directive 2000/31.”⁵⁴⁸ This

⁵⁴⁴ Council Directive (EC) 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.

⁵⁴⁵ G. Frosio, “To Filter or Not to Filter? That Is the Question in EU Copyright Reform” (2017) 36 *Cardozo Arts & Entertainment Law Journal* 332.

⁵⁴⁶ J. Riordan, *The liability of internet intermediaries* (Oxford University Press 2016) 421.

⁵⁴⁷ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

⁵⁴⁸ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 36.

means that the adoption of a filtering mechanism would contravene with the *EU acquis* that explicitly prohibits the obligations for general monitoring of a network.

The incompatibility of filtering technological tools with Article 15 of the ECD has been accentuated by a growing body of academic scholarship as well. For instance, a handful of scholars published an open letter entitled “The Recommendation on Measures to safeguard fundamental rights and open internet in the framework of the EU Copyright Reform.”⁵⁴⁹ In this open letter, they outlined the conflict with Article 15 of the ECD and urged the European Commission to reassess the imposition of monitoring obligations. Drawing their analysis from the CJEU case law, they outlined that Article 15 of the ECD applied to online platforms that host material and stated that the imposition of content identification technologies would come in direct conflict with Article 15 of the ECD. Such a stance has been maintained by Bourdillon, Rosati and others who have stressed that the imposition of content identification technologies will erode legal certainty of the *EU acquis*.⁵⁵⁰ For this, as they clearly point out, the need for ensuring the maintenance of filtering mechanisms is urgent for many reasons. Such reasons address the need for maintaining legal certainty, boosting innovation within the Digital Single Market and protecting Internet users’ fundamental rights.⁵⁵¹ Along similar lines, Senftleben stressed that filtering mechanisms will change the goals of copyright law.⁵⁵² This is because, as he notes, instead of being “an engine of free expression”,⁵⁵³ copyright turns to restrict the dissemination of content in the online world.⁵⁵⁴

However, it is not only a body of academics who have raised serious concerns towards the incompatibility of filtering technologies with Article 15 of the ECD. Indeed, a number of member states have submitted a series of questions to the legal service of the EU Council. More specifically, Belgium, Czech Republic, Finland, Hungary and The Netherlands have asked for clarification of the applicability of Article 15 of the ECD:

⁵⁴⁹ M. Senftleben and others, “The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform” (2017) 40 *European Intellectual Property Review* 149-163.

⁵⁵⁰ S. Stalla-Bourdillon and others, “Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society” (2016) 1-5.

⁵⁵¹ M. Senftleben, “Content censorship and Council carelessness – Why the Parliament must safeguard the open, participative web 2.01” (2018) 4 *AMI - tijdschrift voor auteurs-, media- en informatierecht* 139.

⁵⁵² *Ibid.*

⁵⁵³ *Ibid.*, 142.

⁵⁵⁴ *Ibid.*, 142.

“Is Article 15 of the Directive on electronic commerce to be understood that the prohibition for Member States to impose general monitoring obligations does not apply in the situation where Member States’ legislation would oblige certain platforms to apply technology that identifies and filters all the data of each of its users before the upload on the publically available services?”⁵⁵⁵

In the light of the above, it seems that a body of academic scholars, a handful of member states and CJEU’s court rulings reject the application of monitoring mechanisms on the hosting ISSPs, arguing that Article 17 of the DSMD contradicts Article 15 of the ECD. Interestingly, it has been argued that this conflict with Article 15 of the ECD might generate “systemic inconsistencies”⁵⁵⁶ with other provisions of the *EU acquis* such as Article 14 of the ECD that guarantees immunity from liability to hosting ISSPs under circumscribed conditions.

Another problematic aspect of Article 17 (4) of the DSMD revolves around how the best efforts that an OCSSP makes in order to seek authorisation from the right holders with regard to the legitimate use of their works online can be assessed. From a judicial perspective, the answer to this question could be found in Article 17 (5) of the DSMD which dictates that the principle of proportionality could examine the requirement of best efforts. Article 17 (5) of the DSMD notes “In determining whether the service provider has complied with its obligations under paragraph 4, and in light of the principle of proportionality, the following elements, among others, shall be taken into account: (a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers.” This means that through the lens of proportionality the concept of best efforts shall be examined. The principle of proportionality has been one of the cornerstones.⁵⁵⁷ As Stone, Sweet and Matthews point out, the principle of proportionality is equally placed next to the principles of supremacy and direct effect at European level.⁵⁵⁸

⁵⁵⁵ M. Senftleben and others, “The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform” (2017) 40 *European Intellectual Property Review* 149-163.

⁵⁵⁶ G. Frosio, “To Filter or Not to Filter? That Is the Question in EU Copyright Reform” (2017) 36 *Cardozo Arts & Entertainment Law Journal* 352.

⁵⁵⁷ J. Schwarze, *European Administrative law* (2006) 677.

⁵⁵⁸ A. Stone Sweet and J. Matthews, “Proportionality Balancing and Global Constitutionalism” (2009) 47 *Columbia Journal of Transnational Law* 73.

The principle of proportionality was officially included for the first time in Article 52 of the EU Charter of Fundamental rights, which dictates that “any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.” This implies that proportionality is the most appropriate mechanism to warrant the limitation of fundamental rights and thus could serve as a legitimate basis to examine the best efforts of OCSSPs with regard to the termination of unauthorized content online.

Yet, discrepancies may be found in using the principle of proportionality to assess the best efforts of OCSSPs to prevent the circulation of unauthorized content online. Indeed, Stamatoudi describes the principle of proportionality as “an ambiguous oracle of Pythia: it says everything and nothing at the same time”⁵⁵⁹ while Riordan reports that the principle of proportionality is “a notoriously difficult test to apply.”⁵⁶⁰ This is mainly due to its nature.

Firstly, the concept of proportionality lacks clarity. This understanding has been illustrated in the different views expressed by academic scholarship that attempts to define ‘proportionality’. For instance, within the framework of intellectual property rights’ enforcement in the digital ecosystem,⁵⁶¹ Husovec suggests a cluster of guidelines in order to specify the elements of proportionality.⁵⁶² He notes that in order for the measures to be proportionate, the following elements should be met : 1) effectiveness, 2) method of implementation, 3) collateral damage to innovation, 4) operator’s right to fair trial, 5) abusive use, 6) legality of blocking (out-of-court private agreements), 7) degree of illegality, 8) subsidiarity and 9) shifting of costs. Lodder and Meulen consider the directness of the measure, the effectiveness of the measure, the costs of the measure,

⁵⁵⁹ I. Stamatoudi, “Data Protection, Secrecy of Communications and Copyright: Conflict and Convergences – The Example of Promusicae v. Telefonica” in I. Stamatoudi (ed.), *Copyright enforcement and the Internet* (Kluwer Law International 2010) 231; M. Mercedes Frabboni, File-sharing and the role of intermediaries in the marketplace” in I. Stamatoudi (ed.), *Copyright enforcement and the Internet* (Kluwer Law International 2010) 133 where she criticizes the principle of proportionality “Interpretation of the meaning of proportionality is problematic and could hardly be seen to have established a common ground for the rules existing in each of the Member states.”

⁵⁶⁰ J. Riordan, *The liability of internet intermediaries* (Oxford University Press 2016) 98.

⁵⁶¹ J. Schwarze, *European administrative law* (Sweet & Maxwell London 2006) 664-665.

⁵⁶² M. Husovec, “Injunctions against Innocent Third Parties: The Case of Website Blocking” (2013) 4 JIPITEC 116.

cooperation in the past for the hosting ISSP, time element and adequate safeguards to be taken.⁵⁶³ Finally, a more widely accepted definition of the elements of proportionality has been put by Savola who submitted five interrelated criteria to evaluate proportionality,⁵⁶⁴ namely the legal basis of blocking, effectiveness of the measure, not burdening the hosting ISSPs, subsidiarity, and avoiding collateral damage.

Secondly, it has been argued that the principle of proportionality that the principle of proportionality has been construed in different ways depending on the jurisdiction. Indeed, Finnish courts balance the different interests at stake without first considering the suitability or necessity of the measures to be ordered.⁵⁶⁵ German courts preclude from the suitability test only the most irrelevant measures while limitations that restrict in a mild way the exercise of the right are considered sufficient on the condition that the legislative objective is accomplished.⁵⁶⁶ This vague nature of proportionality may lead to ambiguity, thus erode its applicability when national judges include it in their reasoning, and lead to conflicting outcomes from jurisdiction to jurisdiction as to whether OCSSPs have undertaken best efforts to seek authorisation from right holders with regard to the use of their works.

Therefore, it seems that the principle of proportionality might not be suitable to assess whether the OCSSPs have fulfilled the requirement of best efforts and thus avoid liability.

What is more, the concept of “suitable and effective” is vague and gives the right to OCSSPs to deploy any measure they think it could identify online infringements. It might entail a number of tools that could prove efficient to identify the unlawful content and block it. Such tools have already been developed by a number of ISSPs. The most prominent examples are the Content ID system of YouTube⁵⁶⁷ and the Copyright Match of Vimeo⁵⁶⁸ which are filtering-based technologies and enable right holders to file their works in a database.

⁵⁶³ A. Lodder and N. van der Meulen, “Evaluation of the Role of Access Providers: Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time” (2013) 4 JIPITEC 130.

⁵⁶⁴ P. Savola, “Proportionality of Website blocking: Internet Connectivity Providers as Copyright Enforcers” (2014) 5 JIPITEC 116.

⁵⁶⁵ P. Savola, “Proportionality in Fundamental Rights Conflicts in National Measures Implementing EU Law” (2014) is available at <<http://dx.doi.org/10.2139/ssrn.2432260>> last accessed 28 December 2019.

⁵⁶⁶ Ibid.

⁵⁶⁷ <https://support.google.com/youtube/answer/3244015?hl=en>

⁵⁶⁸ <https://vimeo.com/help/guidelines>

Nevertheless, it could be argued that not all OCSSPs own the appropriate resources to prevent the dissemination of infringing content. Indeed, in order to counter-balance the criticism expressed in the EU Commission's Proposal, and the EU Council's and EU Parliament's compromised texts, the requirement of best efforts does not apply to all OCSSPs indiscriminately. Article 17 (6) of the DSMD excludes a number of OCSSPs with regard to the requirement of best efforts. This limitation entails those OCSSPs whose services "have been available to the public in the Union for less than three years and an annual turnover of 10 million euros." Those OCSSPs that fulfil those criteria do not have to demonstrate best efforts with regard to the prevention of unlawful from reappearing. Rather, they must comply only with Article 17 (4) (a) and (b) which state that OCSSPs must demonstrate best efforts to seek authorisation from right holders and act expeditiously upon receiving notification of the allegedly infringing content.

Yet, while this paragraph has its own merits, since the rationale behind it is to dispel with the burden of OCSSPs to undertake the appropriate measures to seek authorisation or prevent the dissemination of infringing content, it is problematic. This is because there is a lack of evidence that could justify those limitations.⁵⁶⁹ To my knowledge, there are no empirical studies so far that conclude that OCSSPs with less than 3 years operation of business could take advantage of this exclusion or, even better, whether OCSSPs with annual turnover could benefit from this exclusion. What is more, this paragraph might trigger more complicated questions rather than offer solid answers. For instance, it is not clear from how long ago these OCSSPs would benefit from this limitation of liability,⁵⁷⁰ or whether the threshold of 5 million users per month is too low.⁵⁷¹ It is worth pointing out that, within 2 years, YouTube managed to increase its traffic and reach 72 million users monthly.⁵⁷² It may even be that the threshold of the annual turnover of 10 million euros is too high. Hence, it seems that the thresholds for OCSSPs are subject to different interpretations and do not clarify which OCSSPs would be entitled to a limited liability regime.

⁵⁶⁹ J. P. Quintais, "The New Copyright Directive: A tour d'horizon- Part II (of press publishers, upload filters and the real value gap)" (Kluwer copyright blog, 17 June 2019) is available at < <http://copyrightblog.kluweriplaw.com/2019/06/17/the-new-copyright-directive-a-tour-dhorizon-part-ii-of-press-publishers-upload-filters-and-the-real-value-gap/> > last accessed 28 December 2019.

⁵⁷⁰ J. P. Quintais describes this paragraph "window dressing" in J. P. Quintais, "The New Copyright in the Digital Single Market Directive: A Critical Look" (2020) 1 European Intellectual Property Review 19.

⁵⁷¹ Ibid.

⁵⁷² BBC News, "Google buys YouTube for \$1.65bn" (bbc news, 10 October 2006) is available at < <http://news.bbc.co.uk/1/hi/business/6034577.stm> > last accessed 20 September 2019.

Finally, another problematic aspect of the term ‘best efforts’ is that it could be subject to interpretation by national jurisdictions. So, in the course of the transposition of the DSMD to the national legal systems of the 27 EU member states, the translation of the term ‘best efforts’ might substantially differ from national jurisdiction to national jurisdiction. Indeed, there is evidence that in Spain the term ‘best efforts’ translates to ‘greater efforts’, in Italy it amounts to ‘greatest efforts’ while in Germany it is construed as ‘all efforts’.⁵⁷³ It is this divergence in the interpretation of the term that could lead to conflicting outcomes with regard to court rulings and accentuate legal uncertainty among OCSSPs and right holders. For instance, whereas in Spain if an OCSSP demonstrates that it undertook greater efforts to prevent the circulation of infringing content, it would be exonerated from liability. By contrast, if in Italy an OCSSP proves that made greater efforts to tackle the online dissemination of illicit content, it runs the risk of being held for committing copyright infringements. Undoubtedly, the translation of various terms that are enshrined in Directive and Regulations in one of the 28 EU national languages is not a novelty. Yet, this problematic aspect confirms the stance of this thesis that a harmonisation of the liability of OCSSPs seems to be far from reality.

E. No general monitoring: a void provision

To mitigate any criticism that could emerge from the requirement of best efforts to prevent the reappearance of infringing content, Article 17 (8) of the DSMD outlines the prohibition of general monitoring obligations. In particular, it states that “the application of this Article shall not lead to any general monitoring obligation.”

In this way, European policymakers want to be in compliance with the *EU acquis* and EU case law. More specifically, Article 17(8) is in compliance with Article 15 of the ECD that prohibits general monitoring. Article 15 of the ECD is considered one of the cornerstones of e-commerce since it takes from hosting ISSPs any obligation to develop technological tools in order to identify any illicit activity within their networks. Therefore, hosting ISSPs continue their business operation without disruption and without investing in content-identification technologies.

⁵⁷³ “DSM Directive Series #5: Does the DSM Directive mean the same thing in all language versions? The case of ‘best efforts’ in Article 17(4)(a)” (IPKat blog, 22 May 2019) is available at <<https://ipkitten.blogspot.com/2019/05/dsm-directive-series-5-does-dsm.html>> last accessed 28 December 2019.

With regard to EU case law, Article 17 (8) is in accordance with a number of EU rulings that reinforce the importance of not having general monitoring duties for the OCSSPs.⁵⁷⁴

However, this paragraph is void. Its existence seems to be only for aesthetical reasons. This is because it seems impossible to satisfy the requirement of best efforts to seek to terminate the circulation of infringing content or prevent the reappearance of infringing content within the OCSSPs' networks, without deploying monitoring obligations.

This understanding has been reiterated in the words of European and national policymakers. After the final vote of the DSMD in Strasbourg, the French Minister stated that "I also announce that the Higher Council of Literary and Artistic Property, the HADOPI and the CNC will jointly launch in the coming days a "Mission to promote and supervise content recognition technologies."⁵⁷⁵ Likewise, the former Commissioner for Digital Affairs admitted that Article 17 of the DSMD implies the imposition of filtering obligations to OCSSPs by noting that "As things stand, upload filters cannot be completely avoided."⁵⁷⁶ These statements illustrate the rationale of the DSMD and reinforce the suggestion that the use of filtering technologies would be an essential part of the new European e-commerce legislation.⁵⁷⁷

Therefore, it seems that Article 17 (8) of the DSMD turns void since its application in practice is problematic.

⁵⁷⁴ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959; Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85; Case C-484/14 - *Mc Fadden* (2016) ECLI:EU:C:2016:689.

⁵⁷⁵ M. Maschnik, "After Insisting That EU Copyright Directive Didn't Require Filters, France Immediately Starts Promoting Filters" (techdirt, 28 March 2019) is available at <<https://www.techdirt.com/articles/20190327/17141241885/after-insisting-that-eu-copyright-directive-didnt-require-filters-france-immediately-starts-promoting-filters.shtml>> last accessed 27 December 2019.

⁵⁷⁶ M. Maschnik, "EU Commissioner Gunther Oettinger Admits: Sites Need Filters To Comply With Article 13" (techdirt, 3 April 2019) is available at <<https://www.techdirt.com/articles/20190329/15501341902/eu-commissioner-gunther-oettinger-admits-sites-need-filters-to-comply-with-article-13.shtml>> last accessed 27 December 2019.

⁵⁷⁷ Interestingly, companies that develop content identification technologies already advertise their technical tools in relation to Article 17 of the DSMD, see for instance audible magic's website where it states that "Article 17 impacts most social networks in existence today. The clock is ticking, and companies need to put in place technical measures to comply", is available at <<https://www.audiblemagic.com/article-17/>> last accessed 23 December 2019

F. Redress mechanisms and out of court mechanisms: non legitimate without safeguards?

Another problematic feature of Article 17 of the DSMD is to be found in Article 17 (9) of the DSMD. Following the EU Commission's and EU Parliament's compromised texts, the final text of the DSMD in paragraph 9 states that "OCSSPs must put in place an effective and expeditious complaint and redress mechanism that is available to users of their services."

Undoubtedly, this paragraph's role is to decrease the negative criticism that could emerge from the requirement of best efforts to prevent the circulation of infringing content. However, this mechanism might give rise to concerns around the legitimacy of this mechanism and whether it fulfils its aim, to offer access to justice to internet users whose material has erroneously been removed. This is because there have been many examples that outline the inefficiency of such a mechanism operated by hosting ISSPs. For instance, YouTube rejected a counter-notification from a user on the basis of existing contractual relations with right holders.⁵⁷⁸ Another example that outlines the inefficiency of this kind of mechanism is the long process that might be needed in order to examine the counter-notifications. For example, it has been found that the process can take more than a month and during this period, and until the decision, internet users' accounts are blocked so that they do not upload any new content.⁵⁷⁹ It is this long process that encroaches upon the access to justice since, as Husovec points out, "justice delayed is justice denied".⁵⁸⁰ This implies that while this redress mechanism has been designed to offer access to justice for internet users, the long process to examine the content might have the opposite effects and take this right from end-users.

What is more, Article 17 (9) fails to specify which entity would examine the counter-notices of internet users. For instance, one might wonder if the right holders would examine the counter-notices of end-users and under what conditions? Or would it be the

⁵⁷⁸ M. Perel and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 Stanford Technology Law Review 496.

⁵⁷⁹ S. Wodinsky, "YouTube's copyright strikes have become a tool for extortion- Scammers are threatening to shut down channels — unless the owner pays up" (The Verge, 11 February 2019) is available at <<https://www.theverge.com/2019/2/11/18220032/youtube-copystrike-blackmail-three-strikes-copyright-violation>> last accessed 23 September 2019.

⁵⁸⁰ M. Husovec, "Why There Is No Due Process Online?: New Controversies in Intermediary Liability Law" (Balkan.com, 7 June 2019) is available at <<https://balkin.blogspot.com/2019/06/why-there-is-no-due-process-online.html>> last accessed 23 September 2019.

OCSSPs that would assess the validity of the counter-notices and decide whether the content will be reinstated. In any case, this article lacks clarity and gives rise to legal uncertainty.

Finally, another problematic issue of the DSMD revolves around the creation of an impartial body that deals with complaints of users whose material has erroneously been removed by OCSSPs. As Article 17 (9) para. 2 states “Member states shall ensure that out-of-court redress mechanism are available for the settlement of disputes. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the users of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies.” This means that an alternative dispute resolution mechanism will be offered to internet users in order to protect their fundamental rights, namely the freedom of expression. Although this initiative has its own merits, the lack of identifying the criteria under which this mechanism would operate might turn void this initiative. This is because, as discussed in chapter 6 IV and V, it is crucial to specify the principles that shape this impartial body with regard to the validity of the issued decisions. A lack of accountability, legitimacy or proportionality might erode the mission of this impartial body and thus fail to safeguard the fundamental rights of internet users.

In the light of the above, it is possible to observe that the Copyright in the Digital Single Market Directive entails a vast array of problematic features that could not only undermine OCSSPs’ right to conduct business but also interfere with internet users’ fundamental rights and right holders’ rights.

However, it is not only Article 17 of the DSMD itself that has problematic features and thus its application might trigger legal uncertainties. Indeed, it is important to keep in mind that Article 17 of the DSMD is in parallel force with the provisions of the ECD. Both legislative tools regulate the liability of ISSPs and OCSSPs for trade mark and copyright infringements within their networks respectively. Crucially, as demonstrated below, it is this intersection between the DSMD and the ECD that might be problematic and might accentuate the existing legal uncertainties.

IV. Problematic intersection between Article 17 of the DSMD and Article 14 of the ECD

Article 17 of the DSMD addresses the liability of OCSSPs for copyright infringements within their networks. Given that OCSSPs seem to be a sub-category to the hosting ISSPs, this provision acts as a *lex specialis* to Article 14 of the ECD whose scope has been limited to regulate the liability of hosting ISSPs for trade mark infringements.

However, as noted in this chapter in Section III. B., Article 17 of the DSMD introduces primary liability rules for OCSPs and marks a shift from a secondary to primary liability regime. Yet, as explored in chapter 2, the ECD, which is still in force, offers a secondary liability regime for those ISSPs who are aware of the infringing content or who do not act expeditiously to remove it upon being notified.

This understanding implies that there is a dual liability regime, i.e. one set forth in Article 17 of the DSMD and Article 14 of the ECD. Such a dual liability regime, however, might trigger legal uncertainties and might trigger fragmentation at European level since copyright protected works are not only disseminated on YouTube, Facebook, Twitter or Instagram.⁵⁸¹ In fact, they also disseminated on Amazon, by 3d printing files and Cloud service providers via Dropbox files that offer links to material.

In this respect, this dual liability regime might split the existing case law. Consider, for instance, the case where the ISSP falls outside the scope of the definition of Article 17 of the DSMD but the services they provide fall within the scope of Article 17 of the DSMD. A representative example of this line of thinking is eBay. As discussed in Section III. A of this chapter, eBay offers tangible as well as non-tangible goods to its online consumers. Tangible goods amount to anything that is tangible. Non-tangible goods amount Kindles or other pictures which can be viewed as YouTube videos.⁵⁸² In this way, Kindles or pictures that are viewed as video via music video exchange platforms such as Dailymotion fall within the meaning of copyrighted content and thus under the scope of Article 17 of the DSMD. Accordingly, if a brand owner brings legal proceedings against an online

⁵⁸¹ EU Commission, "EU study on the New rules for a new age? Legal analysis of a Single Market for the Information Society 6. Liability of online intermediaries" (2009)

⁵⁸² M. Husovec, "Compromising (on) the Digital Single Market? A Quick Look at the Estonian Presidency Proposal(s) on Art 13" (Kluwer copyright blog, 8 September 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/09/08/compromising-digital-single-market-quick-look-estonian-presidency-proposals-art-13/>> last accessed 27 December 2019.

marketplace alleging trade mark infringement, the principle of the diligent economic operator. More specifically, following the *L’Oreal v Ebay* case,⁵⁸³ to attribute liability to the online marketplace, the Court shall examine whether the online marketplace is “aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1) (b) of Directive 2000/31.”⁵⁸⁴ In contrast, it is questionable which principle would be applicable if a right holder brings legal suit against an online marketplace for copyright infringements that accrue within its platform.⁵⁸⁵ Whether the principle of diligent economic operator would be applicable in the case where the online marketplace offers copyrighted content would be open to discussion. In any case, the stance of this thesis is that given the novelty of the DSMD, further guidance in the following years from the CJEU would be very much expected.

What is more, this dual liability regime could lead to a fragmented enforcement of copyright law since there would be a dual regime in locating the burden of proof. Consider, for instance, that within the copyright framework, as a default a right holder must prove that their rights have been violated. This rationale has been followed by the ECD which under Article 14 intellectual property holders would need to prove the copyright violations. More specifically, under Article 14 of the ECD, right holders must prove that they identified the infringing content and they sent a valid notification for the allegedly infringing content to ISSPs. By contrast, under Article 17 of the DSMD that sets forth a notice and stay down regime, OCSSPs must demonstrate that they undertook all the precautionary measures to terminate the unauthorized content and prevent its reappearance in the future. Thus, for OCSSPs such as YouTube, Facebook and Instagram, the right holder does not need to prove a copyright infringement in order to seek redress for the violations of her rights. Therefore, a copyright law of two velocities would incur and thus amend the existing harmonized practices in copyright law.

Finally, this dual liability regime might act as a deterrent for innovation in the Digital Single Market. This is because a dual liability regime, depending on the services that hosting ISSPs provide might pose a strict limitation for hosting ISSPs that may wish to offer

⁵⁸³ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011.

⁵⁸⁴ Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) E.C.R. I-6011, para. 120.

⁵⁸⁵ C. Angelopoulos and J.P. Quintais, “Fixing copyright reform: a better solution to online infringement” (2019) 10 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 153.

copyrighted content as well as goods that hosting ISSPs wish to offer both services, it must comply with different obligations, thus placing an additional burden to its business model. For instance, a hosting ISSP may wish to combine different services in its business model. When it gives access to copyrighted material, its activities fall under the scope of Article 17 of the DSMD. This means that in order to be exonerated from liability, a hosting ISSP must conclude licensing agreements with right holders. If a hosting ISSP decides not to license the material that users upload within its networks, it must provide evidence that it made the best efforts either to acquire the permission of creators for the material that is circulated on the platform or prevent the availability of infringing material within the platform. The latter, as many scholars have pointed out, amounts to the use of filtering technology that prevents the emergence of online infringements. In parallel with this, a hosting ISSP who might also wish to engage to online retail must comply with Article 14 of the ECD. This implies that in order to be exonerated from liability, a hosting ISSP must expeditiously remove, upon being notified, the allegedly infringing material. Therefore, excessive costs might arise for hosting ISSPs who wish to commercially operate in both services.

This dual liability regime might lead to the creation of a monopoly in the field of OCSSPs that disseminate content. For instance, the role of OCSSPs such as YouTube and Instagram would be empowered in the market since they already own a highly sophisticated technology to identify infringements. Given that the burden of proof is lighter in the case of notice and take down, many hosting ISSPs would prefer to invest in online retailer markets whose schemes to avoid liability does not place an impetus on hosting ISSPs. As a corollary, the DSMD might erode the main aim of the ECD, namely to facilitate e-commerce players.

Therefore, it seems that the intersection between the ECD and DSMD is also problematic. This is because, firstly, the imposition of a dual liability regime, might contradict with the rationale of the ECD which has been introduced with the aim to offer to ISSPs a friendlier environment for innovation within the European Digital Single Market. Secondly, it might give rise to a fragmented enforcement of copyright rules or as I have discussed to a copyright framework of two velocities. Thirdly, the intersection between the ECD and DSMD might lead to a monopolistic market and pose serious impediments to innovation.

V. Conclusion

This chapter hitherto has critically discussed Article 17 of the DSMD that was finalized on the 17th of April 2019 and addressed the liability of OCSSPs for copyright infringements within their networks. Although the DSMD is a new Directive and has not been tested yet in the courts across the EU borders, this chapter has identified a number of problematic aspects that might give rise to legal uncertainties.

Firstly, it was noted that a problematic feature of Article 17 of the DSMD is what appears to be a new sub-type of hosting ISSPs, the OCSSPs. Under the definition of OCSSPs fall those platforms that store and enable users to upload copyright protected content while, as per Recital 62, providers of business-to business cloud services and cloud services, cyber lockers and online marketplaces are excluded. It is questionable as to why online marketplaces; cloud services and cyber lockers do not fall within the definition of OCSSPs since they also give access to public-protected content. This understanding might lead to limitations of innovative business ideas such as new online platforms that could offer a multiple of services to their users that combine the provision of copyright content and the sale of goods.

Secondly, another problematic feature of Article 17 of the DSMD is the introduction of primary liability rules. In particular, Article 17 (1) states that an OCSSP performs an act of communication to the public or an act of making available to the public. This means that, when a copyright infringement takes place, OCSSPs are primarily liable. However, primary liability rules go against the rationale of secondary liability regime as set forth in Article 14 of the ECD. This is because, as discussed in this chapter, as per Article 14 of the ECD, hosting ISSPs can escape liability if they are aware of the illicit activity or upon them being made aware of this illicit activity, by expeditiously removing the infringing content. The imposition of primary liability rules goes against the rationale of secondary liability theories that have been the cornerstone of e-commerce for more than 20 years and that have safeguarded the operation of business for many hosting ISSPs since the defense of knowledge enabled them to be exonerated from liability in cases where intellectual property holders initiated proceedings against them. In contrast, primary liability rules, which are now endorsed in Article 17 of the DSMD, do not require the element of knowledge and thus OCSSPs would be held liable once the copyright violation takes place within their networks.

In order to evade primary liability for copyright infringements, OCSSPs must fulfil two requirements. As per Article 17 (4) of the DSMD, OCSSPs must either make best efforts to seek concluding licensing agreements or to terminate the dissemination as well as prevent the reappearance of copyright infringements. However, both requirements do not come without criticism. As discussed in this chapter, given that OCSSPs operate within a primary liability regime, this implies that the burden of evidence is now placed on them. This means that OCSSPs have to prove that they took all the necessary precautions in order to avoid the dissemination of unlawful material. In contrast, under the secondary liability regime which is set forth in Article 14 of the ECD, right holders have to prove that they notified hosting ISSPs for infringing material within their network. Further, it promotes the one-sided agreements between right holders and OCSSPs since it states that the best efforts that OCSSPs must undertake must be in compliance with “high industry standards of professional diligence.” Such practices might prompt reflections as to whether they take into consideration users’ rights and thus guarantee the dissemination of content online. For this reason, Ramahlo concludes that the current framework “is partly industry-orientated.”⁵⁸⁶

Thirdly, this paragraph endorses a notice and stay down mechanism without defining its limits. On the one hand, it could be assumed that the notice and stay down system requires the implementation of filtering technology. For sure, the prevention of reappearance of infringements cannot rest on human review and technological tools are needed. Otherwise, OCSSPs would have to hire a huge number of reviewers in order to examine the infringements case by case. On the other hand, it is extremely urgent to clarify whether this notice and stay down mechanism shall address the emergence of copyright infringements of the same nature or copyright infringements by the same user or copyright infringements of the same nature by different users or copyright infringements of the same nature by the same user.⁵⁸⁷ Otherwise, notice and stay down would be the subject of different interpretations and thus inconsistencies.

What is more, another problematic aspect revolves around Article 17 (8) of the DSMD which explicitly prohibits general monitoring obligations. As discussed in this chapter, this paragraph seems problematic too since it might be subject to different interpretations.

⁵⁸⁶ A. Ramahlo, “Copyright law-making in the EU: what lies under the ‘internal market’ mask?” (2014) 9 *Journal of Intellectual Property Law & Practice* 224.

⁵⁸⁷ This is the so called *Kerntheorie* and has been discussed in chapter 2 IV. B. 1; see also in *Case C-494/15 - Tommy Hilfiger Licensing* (2016) ECLI:EU:C: 2016:528, para. 34.

On the one hand, it could be argued that this paragraph is void because Article 17 (4) of the DSMD requires from OCSSPs to prevent the dissemination of infringing content. The only understandable way to follow this requirement is to deploy filtering mechanisms. On the other hand, it could be argued that the explicit prohibition of general monitoring obligations imply that specific filtering obligations are allowed under the DSMD. If this is the case, however, does this mean that filtering is allowed only in specific cases as already set forth Recitals 47 and 48 of the ECD and if so, how those specific cases shall be examined.

Finally, the problematic framework of Article 17 of the DSMD is aggravated by the establishment of a redress mechanism which would be operated by OCSSPs as well as the creation of an out of court mechanism that would deal with the disputes between OCSSPs and internet users. This is because, as explained in this chapter, if those self and out of court mechanisms come without safeguards, the principles of due process and the right to access to justice for internet users would be in peril.

Overall, it appears that the attempts to offer more harmonisation in terms of hosting ISSPs' liability have not been fruitful. While Article 17 of the DSMD offers a definition for OCSSPs by noting that OCSSPs commit an act of communication to public by giving the public access to copyright protected works, the rationale behind this definition and the constituents of this new regulatory framework for OCSSPs, which is a sub-type of hosting ISSPs, appear to be problematic. In particular, this definition does not only come into conflict with the secondary liability doctrine that has served as the foundation for e-commerce within the EU, but it also might have a detrimental effect to the interests of OCSSPs and internet users' fundamental rights.

However, as the findings of this thesis indicate, what is even more troublesome with Article 17 of the DSMD is the fact that it does not only entail problematic features. Rather, it also performs a problematic intersection with the existing *EU acquis* and in particular with Article 14 of the ECD. As discussed, this intersection reveals the existence of a dual liability regime under the ECD and DSMD respectively. This dual liability regime might lead to a monopolistic market with big OCSSPs prevailing since the new hosting ISSPs might find the secondary liability regime more appealing and develop services such as cloud services, cyber lockers and online market retailers. The creation of such a monopolistic market might lead to the erosion of Web 2.0 whose main aim is the dissemination of

diverse information to which the direct involvement of internet users is required. Finally, a dual liability regime might create confusion to OCSSPs and ISSPs as, in order to avoid liability rules, they may over-remove material that might be lawful. In this way, internet users' right to freedom of expression and information would be violated.

In addition, there is a dual scheme for hosting ISSPs and OCSSPs in order to avoid primary and secondary liability. Within the scope of Article 17 of the DSMD, OCSSPs must undertake best efforts not only to terminate the infringement but also to prevent its future reappearance. In contrast, pursuant to Article 14 of the ECD, ISSPs must remove the infringing content upon being notified. Any obligation to prevent the reemergence of content is not stated in the ECD. However, this dual scheme for avoiding liability might create confusion to hosting ISSPs, OCSSPs and right holders. This is because, the burden of proof is different in each scheme. For instance, under Article 14 of the ECD, right holders must prove that they identified the infringing content and sent a valid notification for the allegedly infringing content to hosting ISSPs. In contrast, under Article 17 of the DSMD OCSSPs must demonstrate that they deployed preventive mechanism in order to stop the violation online as well as impede its reappearance.

Hence, it seems that the DSMD fails to offer a solid answer to the OCSSPs' liability conundrum. Although it remains to be seen in the following years how this Directive would be transposed in the national legal systems of the 27 EU member states, it is undeniable that Article 17 of the DSMD attempted to provide a uniform aspect to the OCSSPs' liability. Yet, its problematic features seem to erode this aspect. This makes this Directive, along with the ECD, which offers an outdated approach to hosting ISSPs' liability, two legislative tools that do not meet the needs of the parties at stake. In contrast, the outdated approach of the ECD and the problematic aspects of the ECD might pose serious risks to ISSPs business operations and interfere with internet users' fundamental rights.

In the light of the above and in order to examine the legal consequences of the approaches adopted by the ECD and DSMD respectively, the following section offers a number of concluding remarks with regard to the implications of liability rules under the ECD and the DSMD to hosting ISSPs', right holders' and internet users' rights. This illustrates the impact of these two legislative tools on the parties involved as well as offers a strong normative justification for a legal reform with a cluster of recommendations,

which follow in Part II of this thesis. It is worth to mention here that given OCSSPs appear to be a new sub-type of hosting ISSPs, for the sake of convenience and to avoid repetitions, I will use the umbrella term of hosting ISSPs in order to critically examine the implications of the current regulatory framework under the ECD and DSMD to the rights of intellectual property holders, internet users and hosting ISSPs and OCSSPs. Yet, I will use the term OCCSPs when the specific implications emerge from the DSMD.

VI. Concluding remarks for PART I: Critical evaluation of the implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD

A. *Implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD on hosting ISSPs and OCSSPs*

The main rationale of liability rules on ISSPs and OCSSPs is to safeguard the rights of trade mark owners and copyright holders respectively. However, as the findings indicate in chapters 2 and 3, the outdated and problematic framework under Article 14 of the ECD and Article 17 of the DSMD respectively for ISSPs and OCSSPs' liability might cause a level of legal uncertainty to ISSPs and OCSSPs.

The need to ascribe clear legal rules has been expressed by private stakeholders, academic scholars and policymakers. With regard to private stakeholders, a report conducted by Oxera on behalf of Google demonstrates that clear rules may reduce the transaction costs of hosting ISSPs. This is because hosting ISSPs would be aware of the level of enforcement and the processes they need to follow in order to avoid liability.⁵⁸⁸ Clear legal rules could have a positive impact in cases where the notification sent to ISSPs lacks clarity, but hosting ISSPs would still prefer to remove the allegedly infringing material without further investigation with the aim to avoid liability.⁵⁸⁹ An example of this is the case of the Liberty

⁵⁸⁸ Oxera report on behalf of Google, "The economic impact of safe harbors on Internet intermediary start-ups" (2015) 10 is available at <<https://www.oxera.com/getmedia/cba1e897-be95-4a04-8ac3-869570df07b1/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.aspx?ext=.pdf>> last accessed 27 December 2019.

⁵⁸⁹ D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 86; Lecture by Sjoera Nas, Bits of Freedom, "The Multatuli Project ISP Notice & take down" (2004) is available at <<https://www-old.bof.nl/docs/researchpaperSANE.pdf>> last accessed 27 December 2019; C. Ahlert, C. Marsden and C. Yung, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation" (2014) is available at <<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>> last accessed 27 December 2019; D Kiat Boon Seng, "The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices" (2014) 18 *Virginia Journal of Law and*

project.⁵⁹⁰ In this case, the researchers submitted a complaint for a legitimate content to an UK and a US ISSP that offered internet access. The content at stake was part of the book of John Stuart Mill which belonged in the public domain since it was published in 1869. While researchers submitted the same complaint to both ISSPs offering access to internet, the responses differed. In particular, the US ISSP that offered internet access responded to this notice with a list of questions regarding the claims of copyright ownership, while the UK ISSP expeditiously removed the legitimate material without any further investigation of the claim.

Therefore, with the adoption of clear legal rules, hosting ISSPs would be urged to follow a specific process in order to investigate the notices that they receive and thus take down the allegedly infringing material. Otherwise, this ambiguity may result in over-removal of lawful content or additional costs for hosting ISSPs. This is because ISSPs might undertake expensive precautionary measures in order to avoid liability, thus increasing their transaction costs. Such measures would amount to the use of highly sophisticated technology that could detect infringing material online or the hire of experienced employees that could monitor the traffic within the networks.

In line with this, the Council of Europe's recommendation on cyberspace stresses the need for a clear legal framework. In order to promote the public value of the internet, the Council of Europe points out a number of recommendations for Member States with the aim to carve out "the boundaries of the roles and responsibilities of all key stakeholders within a clear legal framework.." as well as establish legislation between cyberspace entities and public authorities that has "...a clear legal basis and respects privacy regulations."⁵⁹¹ This is warranted because internet and all relevant digital technologies have high public service value and must promote the respect of human rights and other fundamental rights within the online environment.

Technology 369; D. Keller, "DMCA classic, DMCA turbo: major new empirical research on notice and takedown operations" (The Center for Internet and Society, 20 April 2016) is available at <<http://cyberlaw.stanford.edu/blog/2016/04/dmca-classic-dmca-turbo-major-new-empirical-research-notice-and-takedown-operations>> last accessed 27 December 2019.

⁵⁹⁰ C. Ahlert, C. Marsden and C. Yung, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation" (2014) is available at <<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>> last accessed 27 December 2019.

⁵⁹¹ Committee of Ministers, "Recommendation to member states on measures to promote the public service value of the Internet" CM/ Rec (2007) 16 is available at <<https://wcd.coe.int/ViewDoc.jsp?id=1207291>> last accessed 27 December 2019.

Along similar lines, the Public Consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights outlines the need for legal certainty.⁵⁹² The majority of respondents supported the introduction of specific requirements that would prevent the dissemination of unlawful content along with a uniform level of enforcement of intellectual property rights at European level. Such requirements could promote legal certainty among right holders.

Likewise, prominent scholars lean in favour of clear legal rules. For example, Garstka argues that legal certainty is directly related with the “quality of a desirable system of regulation.”⁵⁹³ This implies that a legislative framework that aims to balance the interests involved must set out clear legal rules. Another scholar, Jones, stresses that our understanding of legal consequences is contingent upon clear legal provisions.⁵⁹⁴ In order to support his argument, he explores the ruling of *Neij and Sunde Kolmisoppi v Sweden*⁵⁹⁵ where the founders of Pirate Bay were prosecuted for infringing copyright on a commercial basis.⁵⁹⁶ In this case, the CJEU weighed up the right to freedom of expression with the rights of content industries and outlined that the criteria which are used for the balancing act need to be specifically and clearly written. Otherwise, as Jones points out “our predictability will be jeopardized.”⁵⁹⁷

In addition, Angelopoulos outlined the need for legal certainty at European level.⁵⁹⁸ She argues that the current legal framework triggers legal uncertainty. This is because the non-uniform approach of liability rules at European level might create legal uncertainty to hosting ISSPs, right holders and internet users. Likewise, Stalla-Bourdillon stresses the need for legal certainty with regard to hosting ISSPs’ regulatory framework.⁵⁹⁹ She argues that the diverse interpretations of legal provisions in the ECD, along with their inconsistent

⁵⁹² EU Commission, “Public Consultation on the evaluation and modernization of the legal framework for the enforcement of intellectual property rights: summary of responses” (2016) 37.

⁵⁹³ K. Garstka, “Looking above and beyond the blunt expectation: specified request as the recommended approach to intermediary liability in cyberspace” (2016) 7 *European Journal of Law and Technology*

⁵⁹⁴ J. Jones, “Internet pirates walk the plank with article 10 kept at bay: *Neij and Sunde Kolmisoppi v Sweden*” (2013) 35 *European Intellectual Property Review* 698.

⁵⁹⁵ *Neij and Sunde Kolmisoppi v. Sweden* (19 February 2013) Application no. 40397.

⁵⁹⁶ A. Murray, *Information Technology Law: The law and society* (2019) 250.

⁵⁹⁷ J. Jones, “Internet pirates walk the plank with article 10 kept at bay: *Neij and Sunde Kolmisoppi v Sweden*” (2013) 35 *European Intellectual Property Review* 698.

⁵⁹⁸ C. Angelopoulos “Beyond the safe harbors: harmonizing substantive intermediary liability for copyright infringement in Europe” (2013) 3 *Intellectual Property Quarterly* 254.

⁵⁹⁹ S. Stalla-Bourdillon, “Sometimes one is not enough! Securing freedom of expression, encouraging private regulation, or subsidizing Internet intermediaries or all three at the same time: the dilemma of Internet intermediaries’ liability” (2012) 7 *Journal of International Commercial Law and Technology* 154.

application, would turn hosting ISSPs into key players of content regulation while at the same time users' freedom of expression would be subordinated.

Without clear legal rules, a great degree of confusion would have a detrimental effect on hosting ISSPs. For instance, legal uncertainty might lead to excessive removal of content from hosting ISSPs as hosting ISSPs would be unaware of the level of enforcement and would tend to take down material in order to avoid liability. In this way, hosting ISSPs might turn into censorship machines that would violate users' fundamental rights in order to preserve their business operation.⁶⁰⁰

Moreover, legal uncertainty created by the outdated and problematic approach under the ECD and the DSMD might pose serious interference to the legitimate uses of hosting ISSPs and thus threaten their business model. While OCSSPs, a sub-type of hosting ISSPs, such as Pirate Bay focus on the dissemination of unauthorized material, many hosting ISSPs offer legitimate services to users. This is the case of dual use technologies which can "be used to violate third parties' rights as well as promote social beneficial uses."⁶⁰¹ This understanding might undermine their business models since hosting ISSPs may be unsure in which cases they would be subject to liability. So, in order to avoid any risk of liability, hosting ISSPs may undertake proactive measures with the aim to mitigate the dissemination of infringing content within their platforms and thus be exonerated from liability. This scenario has been illustrated by Landes and Lichtman. They refer to the case of a flea market.⁶⁰² In order to battle counterfeit goods, flea market organizers might use technology in order to screen the goods that are displayed.⁶⁰³ Yet, whereas the use of technology might protect sellers from liability, it might increase the costs of operating a flea market and thus impede sellers of goods to participate in the flea market.⁶⁰⁴

⁶⁰⁰ D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 86.

⁶⁰¹ G. Frosio, "Why keep a dog and bark yourself? From intermediary liability to responsibility" (2017) Centre for International Intellectual Property Studies 8.

⁶⁰² W. M. Landes and D. Lichtman, "Indirect Liability for Copyright Infringement: An Economic Perspective" (2003) 16 *Harvard Journal of Law and Technology* 409.

⁶⁰³ W. M. Landes and D. Lichtman, "Indirect Liability for Copyright Infringement: Napster and Beyond" (2003) 16 *The Journal of Economic Perspectives* 20; W. M. Landes and D. Lichtman, "Indirect Liability for Copyright Infringement: An Economic Perspective" (2003) 16 *Harvard Journal of Law and Technology* 404-405.

⁶⁰⁴ W. M. Landes and D. Lichtman, "Indirect Liability for Copyright Infringement: An Economic Perspective" (2003) 16 *Harvard Journal of Law and Technology* 409; M. Daly, "Life after Grokster: analysis of US and European approaches to file-sharing" (2007) *European Intellectual Property Review* 2; T. Hays, "The evolution and decentralisation of secondary liability for infringements of copyright-protected works: Part 1" (2006) 3 *European Intellectual Property Review* 617 where Hays notes that from a judicial perspective, this understanding has been exemplified in the Sony case which was the first ruling that has preoccupied the courts and shed light on whether dual-uses technologies should be held liable for copyright infringements or not. In the case at hand, Universal City Studios have brought legal proceedings against Sony Betamax because

However, this outdated framework of Article 14 of the ECD and the problematic approach set forth in Article 17 of the DSMD do not have a negative impact only on hosting ISSPs. Indeed, new tech companies may be hesitant to enter the Digital Single Market. In light of legal uncertainty, new hosting ISSPs under Article 14 of the ECD and OCSSPs under Article 17 of the DSMD may be forced to adopt expensive proactive measures in order to avoid liability.

Within the context of a digital ecosystem, consider for instance the case of YouTube. Being uncertain of the level of enforcement, YouTube may be encouraged to use filtering technology in order to curb the illicit content that accrues within its platform. At the same time, the adoption of filtering technology would increase the transaction costs and thus act as a deterrent for new OCSSPs with similar services to enter the market. This dual effect has been criticized by Lichtman who argues that:

“...the best reason to impose liability on YouTube is that it is in an enormously good position to filter for and in other ways discourage online infringement. The best reason to decline is that there will be some cost associated with filtering, and that cost might discourage future technologists from experimenting with similar products...”⁶⁰⁵

This means that legal uncertainty on the level of enforcement might impede innovation in the Digital Single Market. This because the development of sophisticated technology would require high resources from new hosting ISSPs and OCSSPs, which they would not possess. Lacking resources, new hosting ISSPs and new OCSSPs may be hesitant to enter the market. Therefore, one of the substantial elements of the Digital Single Market (DSM), innovation,⁶⁰⁶ would be under threat at supranational and national level.

Finally, with regard to the DSMD, new OCSSPs might be willing to enter into licensing agreements with content owners in order to avoid liability. Given that enforcement rules

Sony manufactured home video recorders which were used by its users also for unlawful copying of films. Having found that Sony's products can commercially contribute to the home video industry while at the same time home video recorders' main aim was non-infringing uses, the Court refrained from imposing liability to Sony Betamax. Otherwise, if Sony was held liable for the infringing actions of its users, piracy might be decreased but the whole market of home video recording will be disrupted; *Sony Corp of Am. v Universal City Studios, Inc* 464 U.S. 417, 220 U.S.P.Q. (BNA) 665 (1984).

⁶⁰⁵ D. Lichtman, "Copyright as Information Policy: Google Book Search from a Law and Economics Perspective" in J. Lerner and S. Stern (eds.), *Innovation Policy and The Economy* (2008) 19

⁶⁰⁶ J. Scott Marcus, G. Petropoulos and T. Yeung, "Contribution to Growth: The European Digital Single Market Delivering economic benefits for citizens and businesses" (2019) IMCO Committee 11 is available at <[http://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU\(2019\)631044_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU(2019)631044_EN.pdf)> last accessed 27 December 2019; EU Commission, "A Digital Single Market Strategy for Europe COM (2015) 192 final 3.

are not clear to right holders and hosting ISSPs and OCSSPs, both parties might adopt a more cautious approach in the course of the negotiations of licensing agreements. This is what Coase describes as a “prisoner’s dilemma.”⁶⁰⁷ This describes the difference in the behavior of the prisoners in prison when they live in separate cells and when they live all together. According to this dilemma, if prisoners were not restricted in separate cells, they would have more chances to contact each other and negotiate in a more liberal way. As they live in separate cells they follow a more personal way of making contact with other prisoners.⁶⁰⁸ This understanding could be applied in the context of hosting ISSPs and right holders. Given that OCSSPs and intellectual property holders are not aware of the level of enforcement, they might act with more precautions than necessary. It is this precautionary approach that might lead to the cancellation of the negotiations for licensing agreements between intellectual property holders and new tech companies.⁶⁰⁹

Nevertheless, this outdated and problematic framework under Article 14 of the ECD and Article 17 of the DSMD that revolves around the regulatory regime of ISSPs might prove harmful not only for hosting ISSPs and OCSSPs. Indeed, it could also have a detrimental effect on internet users’ fundamental rights. For this reason, a critical evaluation of the implication of liability rules on users’ rights follows.

B. Implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD on internet users’ rights

The outdated and problematic approaches under Article 14 of the ECD and Article 17 of the DSMD might restrict users’ freedom of expression as per Article 11 of the EU Charter of Fundamental rights, namely the right to freedom of expression that encompasses the right to receive and impart information. To hold hosting ISSPs under the uncertainty of whether or not to impose on the liability rules, as Zittrain argues, could lead to paradoxical scenarios.⁶¹⁰ For instance, while hosting ISSPs are forced to function as gatekeepers by

⁶⁰⁷ F. E. Guerra-Pujol and O. Martínez-García, “Does the Prisoner’s Dilemma Refute the Coase Theorem?” (2013) 47 *John Marshall Law Review* 1290.

⁶⁰⁸ *Ibid.*

⁶⁰⁹ J. Blevins, “Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms” (2013) 34 *Cardozo Law Review* 1829; see also M. A. Carrier, “Copyright and Innovation: The Untold Story” (2012) 2012 *Wisconsin Law Review* 914 where Carrier notes that “VCs are Venture capitalists (VCs) provide money and play an active role in the company’s operations, typically occupying a position on the board of directors” in Carrier stresses that legal uncertainty forced VCs to adopt a more cautious approach towards the new entrants in the markets and thus led to a “loss of new disruptive technologies that deliver content to people”; M. Husovec, “Accountable, Not Liable: Injunctions Against Intermediaries” (2016) TILEC Discussion Paper 33.

⁶¹⁰ J. Zittrain, “A History of Online Gatekeeping” (2006) 19 *Harvard Journal of Law and Technology* 253.

policymakers, they have a lack of expertise and judiciary duties.⁶¹¹ In this regard, under the threat of sanctions, they may act as “overzealous police officers.”⁶¹² Subsequently, this could lead to an overzealous notice and take down or even an intensive blocking of websites without prior consideration of their illicit activities. This would reduce the amount of content available on public and deprive Internet users from obtaining information.

A representative example of this line of thinking can be found in a handful of empirical studies where notice and take down mechanisms were eroded. For instance, in a study conducted in the Netherlands,⁶¹³ it was found that the ISSP that offered internet and was located in the UK removed the allegedly infringing material upon notification without verifying the validity of the claim. In this case, the claim was fake since the allegedly infringing material belonged to the public domain. In this regard, one might assume that other ISSPs might adopt the same stance in order to avoid liability. This understanding seems persuasive since, if an ISSP unreasonably or unjustifiably removes a content, it is not liable. In contrast, the non-expeditious removal of allegedly infringing content upon notification might trigger the liability of hosting ISSPs.

With regard to users’ right to impart information, legal uncertainty could have a negative impact too. For instance, it could cause disincentives for the hosting ISSPs’ side. This concerns the concept of collateral censorship which occurs “when a (private) intermediary suppresses the speech of others in order to avoid liability that otherwise might be imposed on it as a result of that speech.”⁶¹⁴ In order to be exonerated from liability, hosting ISSPs could unreasonably restrain the sphere of action of internet users, prohibiting legal activities and lawful content which has been placed or exchanged by the users.⁶¹⁵ In this way, whereas online infringements could be curbed, lawful activities of internet users

⁶¹¹ D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 86.

⁶¹² *Ibid*, 87.

⁶¹³ Lecture by Sjoera Nas, Bits of Freedom “The Multatuli Project ISP Notice & take down” (2004) is available at <<https://www-old.bof.nl/docs/researchpaperSANE.pdf>> last accessed 1 March 2019.

⁶¹⁴ F. T. Wu, “Collateral Censorship and the Limits of Intermediary Immunity” (2011) 87 *Notre Dame Law Review* 295-296; The concept of collateral censorship has been first developed in Balkin’s writings; see J. Balkin, “Old School/ new School speech regulation” (2014) 127 *Harvard Law Review* 2309.

⁶¹⁵ G. Sartor, “Providers Liability: From the e-commerce Directive to the future” (2017) IMCO Committee 12; A. Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards* (Intersentia 2018) 96-97 where she argues that “legal uncertainty is problematic because vague rules can push intermediaries to adopt overly cautious behaviour. When not sure about their legal situation, they may prefer to err on the side of caution, which means that they eliminate disputed content, even if it is actually legitimate.”

would be restricted. Therefore, the benefit of terminating illicit activities online could not outweigh the negative effect of restricting lawful activities online.

A telling example can be found in the *Lenz v Universal* case.⁶¹⁶ In this case, a video with a baby dancing under the rhythms of the Prince's song "Let's go crazy" has been removed by YouTube for copyright purposes. Likewise, a video from NASA that was about the landing of the first human in Mars has been removed for copyright violation.⁶¹⁷ Therefore, under the reasoning of copyright infringement, users are deprived from expressing themselves by uploading videos with parodies or videos with educational purposes.

What is more, the legal uncertainty with regard to the level of enforcement of rights would underestimate the internet users' rights in the online public domain. This is because, as Advocate General Poiares Maduro in joined cases C-236/08, C-237/08 and C-238/08 of *Google France/Inc. v. Louis Vuitton Malletier*⁶¹⁸ pointed out, "the aim of Directive 2000/31 is to create a free and open public domain on the internet." This means that internet users should be able to exchange and receive information online. Yet, if the dissemination of content is restricted online due to the legal uncertainty that revolves around the level of enforcement of rights, one of the main objectives of the ECD would be placed in peril.

However, the negative implications of the liability rules under Article 14 of the ECD and Article 17 of the DSMD might not be limited to internet users and hosting ISSPs' and OCSSPs' business models. Indeed, they can also extend to right holders themselves.

C. Implications of liability rules under Article 14 of the ECD and Article 17 of the DSMD on the rights of right holders

With regard to the rights of intellectual property holders, the outdated framework under the ECD and the problematic approach as set forth in DSMD create legal uncertainty. As already discussed in chapter 2, Article 14 of the ECD does not provide a definition for hosting ISSPs. Rather, it entails a set of defences for hosting ISSPs in order for them to be exonerated from liability. For this reason, in order to define liability for hosting ISSPs,

⁶¹⁶ *Lenz v. Universal Music Corp.* (9th Cir. Mar. 17, 2016)

⁶¹⁷ J. Reda, "When filters fail: These cases show we can't trust algorithms to clean up the internet" (Reda's website, 28 September 2017) is available at <<https://juliareda.eu/2017/09/when-filters-fail/>> last accessed 29 December 2019.

⁶¹⁸ C-236/08, C-237/08 and C-238/08 of *Google France/Inc. v. Louis Vuitton Malletier* (2009) ECLI:EU:C:2009:569, para. 142.

national courts resort to secondary liability rules. Given the lack of harmonisation on secondary liability rules, each legal jurisdiction offers its own legal rules. The result is a patchwork of miscellaneous tortious secondary liability doctrines among the EU member states with different criteria to claim legal protection. In addition, as discussed in chapter 3, Article 17 of the DSMD provides a definition for OCSSPs, which is a sub-type of ISSPs, but entails an array of problematic features that accentuate the existing legal uncertainty for copyright holders. As discussed in chapter 3 Section IV., it is questionable under which liability regime copyright holders could seek redress if their copyrighted content has been violated within the platform of an online marketplace. A representative example of this line of thinking is to be found on eBay. In this case, eBay offers tangible as well as non-tangible goods to its online consumers. For instance, tangible goods amount to anything that is tangible such as bags, watches, furniture while non-tangible goods could amount to Kindles or other pictures which can be viewed as YouTube videos.⁶¹⁹ With regard to non-tangible goods, this means that Kindles or pictures that are viewed as video via music video exchange platforms such as Dailymotion fall within the meaning of copyrighted content and thus under the scope of Article 17 of the DSMD. However, if a copyright holder brings legal proceedings against an online marketplace, which is considered a hosting ISSP under Article 14 of the ECD, alleging copyright violation, one might wonder under which liability regime would her lawsuit fall and how she will protect her copyright?

Therefore, neither legislative frameworks can guarantee the protection of the rights of creators or brand owners. Whether or not a hosting ISSP is liable for copyright or trademark infringements that accrue within their networks is subject to a case by case assessment and might differ from jurisdiction to jurisdiction depending on the courts' examination.

Further, apart from the legal uncertainty that might arise among right holders, the imposition of liability rules may not be a panacea for the intellectual property holders. This is because, even if the courts find hosting ISSPs liable, this does not automatically guarantee that right holders will be compensated. Consider, for instance, the case of *The Pirate Bay*.⁶²⁰ In 2009, the Stockholm District Court found *Pirate Bay* liable and thus

⁶¹⁹ M. Husovec, "Compromising (on) the Digital Single Market? A Quick Look at the Estonian Presidency Proposal(s) on Art 13" (Kluwer copyright blog, 8 September 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/09/08/compromising-digital-single-market-quick-look-estonian-presidency-proposals-art-13/>> last accessed 27 December 2019.

⁶²⁰ A. Murray, *Information Technology Law: The law and society* (2009) 250.

ordered it to pay damages up to 30 million kronor. However, when the right holders requested the damages, it was found that Pirate Bay did not have the necessary assets to satisfy the pecuniary orders of the court.⁶²¹ Therefore, the right holders could not collect the award of damages and thus be compensated for the massive infringement of their rights. Hence, in such cases it appears that liability rules cannot provide adequate protection to the right holders.

Finally, the problematic approach under the DSMD might give rise to negative publicity for intellectual property holders. Although the aim of the DSMD was to bridge the value gap between right holders' revenues and the dissemination of their content online, it might have an opposite effect for right holders. This is because it presents right holders as the main threat for users to access copyrighted content online and for OCSSPs to disruptively continue the operation of their business model. For example, it urges OCSSPs to license the content that is disseminated online. Given that it seems impossible to license all the content available online, internet users would be deprived of content that could not license. What is more, the introduction of primary liability rules, as presented in chapter 3 Section III. B, would act as a threat for the operation of OCSSPs since they would be subject to damages once a copyright infringement takes place within their networks.

Overall, one might conclude that the current legislative tools that regulate hosting ISSP's and OCSSPs' liability undermine their business models, and internet users' and right holders' rights. While the CJEU outlined in the *Scarlet Extended*⁶²² ruling that "in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures",⁶²³ the findings presented in this thesis indicate that the ECD and DSMD fail to provide a regulatory framework that could take into consideration all the rights at stake. For this reason, a legal reform is imperative in order to suggest legislative amendments so as to balance the

⁶²¹ N. Anderson "Swedish court rules TPB admins too broke to pay damages" (Arstechnica, 24 August 2009) is available at <<https://arstechnica.com/tech-policy/2009/08/swedish-court-rules-tpb-admins-too-broke-to-pay-damages>> last accessed 27 December 2019; M. Manner, T. Siniketo and U. Polland, "The Pirate Bay ruling" (2009) 20 Entertainment Law Review 198.

⁶²² Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

⁶²³ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 45.

interests of the parties involved. These suggestions will be thoroughly discussed in the following Part of this thesis.

Part II: Recommendations

Chapter 4: Towards a responsibility framework for hosting ISSPs based on co-regulatory approach

I. Introduction

As discussed in Part I of this thesis, the current legislative landscape that regulates hosting ISSPs' and OCSSPs', which is a sub-type of hosting ISSPs, liability for trade mark and copyright infringements respectively fails to strike a fair balance between the interests of hosting ISSPs, intellectual property holders and internet users. Firstly, the legal framework under Article 14 of the ECD is outdated. As already presented, Article 14 of the ECD endorses a secondary liability regime for hosting ISSPs. This means that hosting ISSPs could only be held liable for the infringements committed by their users only if they are aware of the illicit activity within their networks. However, Article 14 of the ECD fails to define hosting ISSPs' liability. Instead of defining hosting ISSPs' liability, it offers a set of defences to hosting ISSPs. Unfortunately, the national transposition of the ECD to EU member states fails to offer a solid answer to hosting ISSPs' liability conundrum as well. What is more, national courts resort to their tortious secondary liability doctrines to define the secondary liability of hosting ISSPs. Yet, while secondary liability rules could define hosting ISSPs' liability, this solution does not seem ideal. The findings suggest this is mainly due to two reasons. Firstly, it seems that national courts have difficulties in applying tortious secondary liability rules within the online context. Secondly, these tortious secondary liabilities differ from each other. As corollary, a puzzle of miscellaneous secondary liability doctrines has emerged and aggravated the existing legal uncertainty among the parties involved.

Likewise, the DSMD seems to favor the interests of intellectual property holders while at the same time it undermines the rights of OCSSPs and internet users. More specifically, Article 17 of the DSMD has attempted to define OCSSPs' liability⁶²⁴ with regard to copyright infringements but with limited success. While it offers a definition of OCSSPs' liability, it endorses a primary liability regime for them. This means that OCSSPs are held liable if a copyright infringement takes place within their network. The defense of knowledge cannot be used since it does not constitute a requisite for primary liability. This

⁶²⁴ Council Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the DSM and amending Directives 96/9/EC and 2001/29/EC (hereinafter DSMD).

understanding comes against the rationale upon which internet infrastructure has been developed and which is based on the ideal of secondary liability rules. What is more, Article 17 of the DSMD is misaligned with Article 14 of the ECD as it introduces a dual liability regime that might accentuate the existing legal uncertainty.

These findings offer normative reasons to justify the need for a legal reform with regard to hosting ISSPs' regulatory regime. In this vein, Part II of this thesis explores an array of legal amendments on hosting ISSPs' liability with a view to balance the interests of hosting ISSPs, intellectual property holders and internet users. In order to propose the amendments, this chapter draws upon the establishment of a responsibility framework for hosting ISSPs based on co-regulatory approach. This means that hosting ISSPs would undertake a number of responsibilities and the state would step in the EU regulatory framework with the establishment of a proposed hosting ISSP supervisory authority. In other words, hosting ISSPs would be assigned to a set of responsibilities through which they would be accountable to a proposed hosting ISSP supervisory authority. In this light, this chapter considers the normative and theoretical underpinnings upon which a set of responsibilities of hosting ISSPs could lie. Finally, this chapter explores one of the constituents of this responsibility framework, namely the duty of care of hosting ISSPs towards the infringements that might occur within their networks.

II. Normative justifications for establishing a responsibility framework for hosting ISSPs based on co-regulatory approach

With the advent of Web 2.0, there has been a plethora of arguments that might warrant the ascription of a responsibility framework for hosting ISSPs. The underlying basis of these arguments is the new role of hosting ISSPs. Such a role does not represent hosting ISSPs as mere conduit platforms anymore. Rather, this role depicts hosting ISSPs as controllers of the information that passes through their networks, implementers of public policies and enforcers of rights in the digital ecosystem. However, this new role also comes with challenges for internet users/ online consumers, intellectual property holders and hosting ISSPs.

A. *Hosting ISSPs as information gatekeepers*

Firstly, hosting ISSPs are now considered *information gatekeepers*.⁶²⁵ This is because the great majority of internet users are informed by hosting ISSPs. Indeed, a number of policy documents and reports reinforces that new role of hosting ISSPs. For instance, the Digital Single Market Strategy outlines that one of the main social functions of hosting ISSPs nowadays is to inform internet users.⁶²⁶ A study conducted by the Digital News Oxford's Reuters Institute in 2019 indicates that 52% of the respondents between 25-34 years old reported that Facebook is the main source of information while at the same time 32% of the respondents between 18-24 years old rely on YouTube for their news.⁶²⁷ Hosting ISSPs are now compared with the public squares where citizens express and exchange views.⁶²⁸

However, what is critical about hosting ISSPs as information gatekeepers is that they can decide which information reaches the end-users. As Mansell pointed out, hosting ISSPs "have the power to influence what ideas citizens are able to find easily."⁶²⁹ An example of this is the removal of a political video on YouTube.⁶³⁰ This video concerned the speech of a Member of the EU Parliament who advocated the termination of selling trade goods that are used for tortures and death penalties. The video has been removed under the justification of violating the community guidelines of the online music-exchange platform. However, the removal of this video has deprived EU citizens from obtaining knowledge of

⁶²⁵ E. Laidlaw, "Private Power, Public Interest: An Examination of Search engine accountability" (2009) 17 *International Journal and Information Technology* 114.

⁶²⁶ EU Commission, "A Digital Single Market Strategy for Europe" COM (2015) 192 final where it states that hosting ISSPs have "an ever more central role in social and economic life: they enable consumers to find online information..."

⁶²⁷ Reuters Institute for the Study of Journalism, "Reuters Institute Digital News Report" (2019) 56; Reuters Institute for the Study of Journalism, "Reuters Institute Digital News Report 2016" (2016) 176 is available at <<http://media.digitalnewsreport.org/wp-content/uploads/2018/11/Digital-News-Report-2016.pdf?x89475>> last accessed 27 December 2019; "We increasingly get our news on social media (44 percent of the overall U.S. population accesses news on Facebook), shop on e-commerce platforms (Amazon accounts for 43% of US online retail sales) stream videos on YouTube (80% of European internet users had used the digital video platform within the past month)".

⁶²⁸ A. Starzak, "When the Internet (Officially) Became the Public Square" (Cloudflare, 21 June 2017) is available at <<https://blog.cloudflare.com/internet-became-public-square/>> last accessed 27 December 2019; the US Supreme Court has held that access to social media is a constitutional right, see US Supreme Court of United States, *Packingham v. North Carolina* 582 U.S. (2017); In addition, a Costa Rican ruling confirmed that access to internet is a fundamental right, see A. Guadamuz, "Text of the Costa Rican ruling declaring internet as a fundamental right" (TechnoLlama, 23 April 2012) is available at <<https://www.technollama.co.uk/text-of-the-costa-rican-ruling-declaring-internet-as-a-fundamental-right>> last accessed 27 December 2019.

⁶²⁹ R. Mansell, "Platforms of power" (2015) 43 *Intermedia* 20-24.

⁶³⁰ J. Reda, "When filters fail: These cases show we can't trust algorithms to clean up the internet" (Reda's website, 28 September 2017) is available at <<https://juliareda.eu/2017/09/when-filters-fail/>> last accessed 27 December 2019.

a highly important discussion topic.⁶³¹ In this sense, the music exchange platform could control the information received by its users through the take down of a video. Likewise, Perel and Elkin-Koren argue that hosting ISSPs can decide which information reaches the end-users. For instance, the mere removal of videos by YouTube or the blocking of a link of a website by Google denies users from obtaining useful information which otherwise would have been accessible by the public.⁶³² Subsequently, a level of censorship is performed by hosting ISSPs that restrict internet users' fundamental right to obtain information which is a constituent of freedom of expression as set forth in Article 11 of the EU Charter of Fundamental Rights.

B. Hosting ISSPs as policymakers

Furthermore, given that hosting ISSPs control the flow of information,⁶³³ they could also shape public policy. From a normative perspective, the impact that hosting ISSPs might have on public sphere and the influence as to how policies can be implemented in practice might warrant the ascription of a set of responsibilities to hosting ISSPs. Although they are not political or public institutions, they contribute to the development of public policies such as copyright and trade mark policies.⁶³⁴ This is illustrated by the example of YouTube, which carves out copyright policies through the provisions in their Terms of Service and in particular through Content ID system and the Copyright School tutorial. Content ID system is a software that entails a database where copyright holders have submitted files of their works and that scans any video that is uploaded by internet users

⁶³¹ Marietjschaake's website is available at <<https://marietjschaake.eu/en/mep-trade-in-torture-goods-must-stop>> last accessed 27 December 2019.

⁶³² M. Perel and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 *Stanford Technology Law Review* 483.

⁶³³ D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 85-86.

⁶³⁴ An example with regard to privacy issues can be found in the right to be forgotten case. More specifically, given that Google is the most popular search engine worldwide, it contributed to the imposition of the right to be forgotten pursuant to the ruling of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* by enabling the users in the 28 EU member states to request the deletion of their personal data. Case 131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECR I-000; see also O. Lynskey "Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez" (2015) 78 *Modern Law Review* 522-534; In this case, a Spanish citizen Mario Costeja González sent a formal notice to the Spanish Data Protection Agency requesting from a Spanish newspaper and Google Spain to remove information about his social security debts which were not overdue anymore. While the Spanish Data Protection Agency rejected Costeja's arguments against the newspaper, it tilted in favor of his claims against Google. In this regard, Google appealed to the Spanish Court of Appeal which subsequently made a referral of three questions to the CJEU; See also O. Fischman Afori, "Universal measures in the service of global challenges: proportionality, blocking orders, and online intermediaries as hybrid bodies" in T. Synodinou, *Pluralism or Universalism in international copyright law* (Kluwer Law International 2019) 663 where the author describes hosting ISSPs as "hybrid private/public bodies"; E. Lee, "Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten" (2016) 49 *U.C. Davis Law Review* 1066 where Lee argues that Google is "a private administrative agency administering the right to be forgotten".

within this music exchange platform.⁶³⁵ Within the context of Content ID system, YouTube amends the main copyright law principle which states that the owner of a work is the author of the work. This is because copyright holders do not own their works anymore. Rather, they are subject to the options that YouTube offers them in case this advanced software identifies a copyright infringement.⁶³⁶ More specifically, once a piece of work, which is uploaded, matches a copyrighted work that is already in the database of the Content ID system, the copyright owner is notified and provided with specific options with regard to the unauthorized video such as the blocking of the whole video, the monetization of the video by running ads before its viewing, share revenues with the user that uploaded the video.⁶³⁷

Further, another example of role of hosting ISSPs to curtail copyright policies can be found in the Copyright School tutorials offered by YouTube and in which users are educated as to how they shall comply with copyright law.⁶³⁸ So, users who upload material that has been blocked are encouraged to attend YouTube's Copyright School. In this tutorial, the video stresses the negative consequences for the users if they upload infringing material on the platform. Such consequences may vary from taking the infringer-users to court or suspending users' accounts for an unlimited period of time. In this way, users are educated to comply with copyright policies and be cautious before uploading any material regardless of the fact that it may have been legitimately obtained by third parties.⁶³⁹ However, what is critical about shaping copyright policies is that hosting ISSPs are not state authorities and thus they are not granted any legitimacy to curtail policies on copyright or trade mark issues. This role belongs to the national authorities and not to private entities with business interests. What is more, it might be the case that the

⁶³⁵ Youtube , "How to manage your copyrights in Youtube" is available at <<https://support.google.com/youtube/answer/2797370?hl=en-GB>> last accessed 10 November 2019.

⁶³⁶ L. Edwards, "With Great Power Comes Great Responsibility? The Rise of Platform Liability" in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 276.

⁶³⁷ <https://support.google.com/youtube/answer/2797370?hl=en>; In addition, it is worth mentioning that since mid-September 2019 YouTube has changed its policy in its manual claiming tool for copyright holders with regard to the monetization of the videos. In particular, the new terms and conditions state that copyright holders cannot monetize videos that entail "very short or unintentional uses unclaimed". Without defining these concepts, this might result, as commentators observe, to a high degree of blocking videos. In other words, copyright holders would be in favor of blocking the video entirely since they do not have the option of monetizing it if the video entails only short uses of their copyright protected works in H. Boscher, "YouTube takes copyright law into their own hands with new policy on music infringement" (IPKat, 2 September 2019) is available at <<http://ipkitten.blogspot.com/2019/09/youtube-takes-copyright-law-into-their.html>> last accessed 27 December 2019.

⁶³⁸ https://www.youtube.com/copyright_school

⁶³⁹ L. Belli, P. Augusto Francisco and N. Zingales, "Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018) 57.

copyright policies that hosting ISSPs adopt are one-sided and thus a risk to remove lawful content, such as fair use content, might occur.⁶⁴⁰ As corollary, an over-enforcement of copyright law may emerge and therefore impinge upon the rights of users, such as the right of freedom of expression, and violate the rights of the authors of fair use works.

C. *Hosting ISSPs as enforcers of intellectual property rights online*

Moreover, the growing power of hosting ISSPs due to their function as information gatekeepers and implementers of public policies is increased when their role as enforcers of intellectual property rights in the digital ecosystem is added. It is this role of enforcers of intellectual property rights online that could also justify the ascription of a set of responsibilities to them. Under the guise of indirect regulation of the online behavior of the users,⁶⁴¹ hosting ISSPs now filter, block or remove allegedly infringing material that harms the rights of the content industries or trade mark holders.⁶⁴² However, what is critical about their role as enforcers of rights is that it is not limited to the enforcement of rights but is also extended to adjudication needs. As Huszti-Orban notes, “the end decision is ultimately delegated to private entities who are thereby effectively given law enforcement and quasi-adjudicative responsibilities.”⁶⁴³ This means that hosting ISSPs are those entities that take the last decision to leave or remove any allegedly unwelcome content that is uploaded on their networks. In this respect, they turn to be “the judge and the jury” in the same case.⁶⁴⁴

Yet, it is worth questioning whether this dual role of hosting ISSPs acts against the rule of Law and in particular whether it is legitimate to engage concomitantly a private entity

⁶⁴⁰ M. Perel and N. Elkin-Koren, “Accountability in Algorithmic Copyright Enforcement” (2016) 19 *Stanford Technology Law Review* 491: An example is the removal of the campaign video of a candidate for the US Presidential Elections in 2008 on the basis that it included snippets from popular TV Programs, although the use of snippets is considered fair use is found in A. Marsoof, “Notice and take down: a copyright perspective” (2015) 5 *Queen Mary Journal of Intellectual Property Law* 19; W. Seltzer, “Free speech unmoored in copyright’s safe harbour: chilling effects of the DMCA on the first Amendment” (2010) 24 *Harvard Journal of Law & Technology* 172.

⁶⁴¹ L. Lessig, *Code and other laws of cyberspace* (1999) 85; M. Schruers, “Copyright, Intermediaries and Architecture” in F. Mesiani, D. Cogburn, L. Denandis and N. Levinson (eds.), *The turn to infrastructure in internet governance* (2016) 108.

⁶⁴² N. Tusikov, *Chokepoints: Global private regulation on the Internet* (2017) 49-50.

⁶⁴³ K. Huszti-Orban, “Countering Terrorism and Violent Extremism Online: What Role for Social Media Platforms?” in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018) 202; European Digital Rights (EDRI), “The Slide from “Self-Regulation” to “Corporate Censorship” is available at <https://edri.org/files/EDRI_selfreg_final_20110124> last accessed 27 December 2017.

⁶⁴⁴ M. Warmann, “Google is the ‘judge and jury’ in the right to be forgotten” (The Telegraph, 14 July 2014) is available at <<https://www.telegraph.co.uk/technology/google/10967211/Google-is-the-judge-and-jury-in-the-right-to-be-forgotten.html>> last accessed on 27 December 2019.

such as a hosting ISSP with enforcement and judicial demands. For this reason, Elkin-Koren criticizes this dual role of hosting ISSPs and argues that enforcement and judicial duties have a public interest and shall be assigned to government institutions and authorities.⁶⁴⁵ Otherwise, this dual role of hosting ISSPs could prompt reflections on the legitimacy of the decision of hosting ISSPs to remove material depending on their judgement while at the same time they lack any authority to adjudicate.

This concern about the dual role of hosting ISSPs could be aggravated by the fact that they are private entities that might need to adjust their business interests with their enforcement and adjudication duties.⁶⁴⁶ In particular, it could be argued that hosting ISSPs might abuse the power they enjoy and favor their own interests or the interests of their business partners, which could threaten competition and innovation within the Digital Single Market (DSM). Insofar as the interests of the hosting ISSPs are concerned, consider, for example, Google which has been accused and fined by the European Commission by virtue of abuse of its dominant position.⁶⁴⁷ In this case, Google placed its own shopping services on higher ranking in the search listings while at the same time downgrading rival services. However, while market dominance is acceptable under European competition rules, it is forbidden to take advantage of the dominant position in the market and restrict competition.⁶⁴⁸ On this basis, European Commissioner for Competition Affairs, Margaret Vestager acutely pointed out that “what Google has done is illegal under European antitrust rules. It denied other companies the chance to compete on the merits and to innovate. And most importantly, it denied European consumers a genuine choice of services and the full benefits of innovation.”⁶⁴⁹ This means that by giving preference to its own services, Google did not only undermine the services provided by its competitors.

⁶⁴⁵ M. Perel and N. Elkin-Koren, “Accountability in Algorithmic Copyright Enforcement” (2016) 19 Stanford Technology Law Review 485.

⁶⁴⁶ *Ibid.*

⁶⁴⁷ R. Price “Google has been hit with a record-breaking €2.4 billion fine by the EU over its antitrust case” (UK Business Insider, June 2017) available at <<http://uk.businessinsider.com/eu-fines-google-record-breaking-antitrust-shopping-case-2017-6>> last accessed 27 December 2019; EU Commission, “Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service”(27 June 2017) is available at< http://europa.eu/rapid/press-release_IP-17-1784_en.htm> last accessed 21 November 2017.

⁶⁴⁸ EU Commission, “Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service” (27 June 2017) is available at <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> last accessed 21 November 2017; K. von Blanckenburg, “Google search abuses dominant position to illegally favour Google Shopping: an economic review of the EU decision”(2018) 20 Digital Policy, Regulation and Governance 211.

⁶⁴⁹ *Ibid.*

Rather, it also deprived internet users of a number of choices in terms of comparative shopping services.

Drawing further insights, due to their growing power⁶⁵⁰ hosting ISSPs might not only favour their own interests and violate competition rules. Rather, they may also favour their business partners' interests. Indeed, the Communication of 2015 that accompanied the Digital Single Market Strategy stated that "some online platforms have evolved to become players competing in many sectors of the economy and the way they use their market power raises a number of issues..."⁶⁵¹ This implies that hosting ISSPs may give priority to their business partners' interests and disregard their users' rights and the interests of other business players in the market. This was illustrated in the case of an American singer who uploaded a parody video on YouTube.⁶⁵² Due to the fact that the video included a number of lyrics from popular songs, YouTube removed the video on the basis of copyright infringement. In order to respond to the removal, the singer submitted a counter-notice highlighting that he uploaded the video for fair use. Despite his legitimate claims for the fair use purposes, YouTube refused to reload the video under the justification that it had a contractual agreement with the specific copyright holders and thus the counter-notification that has been submitted cannot be further processed and examined. Therefore, the video that has been removed cannot be reinstated to the platform.⁶⁵³ This response reveals that YouTube gives priority to rights holders with whom the video-music platform has concluded agreements.⁶⁵⁴ Indeed, having a closer look at YouTube's policies, it appears that counter notification processes are not available if the work belongs to music copyright owners who have entered into agreements with YouTube with regard to the use of their music.⁶⁵⁵

⁶⁵⁰ O. Lynskey, "Regulating "Platform Power" (2017) LSE Law, Society and Economy Working Papers 3; J. Cohen, "The Regulatory State in the Information Age" (2016) 17 Theoretical Inquiries in Law 6 where Cohen names it "platform power".

⁶⁵¹ EU Commission, "A DSM Strategy for Europe" COM (2015) 192 final 12.

⁶⁵² M. Perel and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 Stanford Technology Law Review 507.

⁶⁵³ "YouTube's Deal with Universal Blocks DMCA Counter Notices" (Torrentfreak, 5 April 2013) is available at <<https://torrentfreak.com/youtube-deal-with-universal-blocks-dmca-counter-notices-130405/>> last accessed 27 December 2017.

⁶⁵⁴ M. Perel and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 Stanford Technology Law Review 507.

⁶⁵⁵ YouTube, "Videos removed or blocked due to YouTube's contractual obligations" is available at <<https://support.google.com/youtube/answer/3045545?hl=en>> last accessed 27 December 2019.

A similar example where hosting ISSPs gave priority to the interests of their business partners can be found to the android's Google Play application store.⁶⁵⁶ While Google is considered a search engine and do not fall within the scope of the hosting ISSPs, this example could be equally applied to hosting ISSPs as well. In this case, Google play app store did not include in its store the Disconnect's application which was about a software that prevents third parties tracing Android users' data when they use applications on their mobile devices. The exclusion of this app in its store was achieved under the guise that this specific application was in conflict with existing applications by diminishing the functionality of the existing applications or forcing them to amend their business model.⁶⁵⁷ In this way, Google can exert control over which information reaches end-users and thus might deprive users of important content to them.

D. Hosting ISSPs as architects of e-commerce infrastructure

Further, within the context of e-commerce, hosting ISSPs play a pivotal role. Their function is not limited anymore to acting as middlemen between information and internet users.⁶⁵⁸ Rather they are architects of the e-commerce infrastructure. This means that they design their business model in such a way that allows them to be aware of the material that is hosted and in particular the value of the goods as well as their demand among consumers.⁶⁵⁹ In this way, they can grasp the needs of the consumers and distribute material that is appealing to the internet users, thus turning themselves into "critical market access points."⁶⁶⁰ This means that they are the main entities that consider which content shall be circulated within the digital ecosystem.

⁶⁵⁶ O. Lynskey, "Regulation by Platforms: The Impact on Fundamental Rights" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018) 90.

⁶⁵⁷ F.Y. Chee, "Privacy app maker files EU antitrust complaint against Google" (Reuters, 2 June 2015) is available at <<https://www.reuters.com/article/us-eu-google-antitrust/privacy-app-maker-files-eu-antitrust-complaint-against-google-idUSKBN00I1Z220150602>> last accessed 27 December 2019; In the words of Google's spokesperson "Our Google Play policies have long prohibited apps that interfere with other apps - such as altering their functionality or removing their way of making money. We apply this policy uniformly and Android developers strongly support it."

⁶⁵⁸ As OECD describes "internet intermediaries bring together or facilitate transactions between third parties on the internet. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet-based services to third parties" in OECD, "Report on the economic and social role of internet intermediaries" (2010) 9.

⁶⁵⁹ M. Tessier, J. Herzog and L. Madzou, "Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018) 178.

⁶⁵⁹ *Ibid*, 179.

⁶⁶⁰ *Ibid*, 178.

However, if counterfeit goods are displayed on hosting ISSPs and are sold to innocent consumers, the trust of consumers will be lost. Given that e-commerce's primary aim is to gain trust from consumers when they interact with online auction platforms via the transactions,⁶⁶¹ a lack of trust could not only restrict the growth of the e-commerce business models and prevent new players to enter the market. It could also drive back internet users from using their services.

E. Hosting ISSPs as inducers of illicit activity online

Finally, another reason that warrants the ascription of a set of responsibilities to hosting ISSPs is the fact that their power could induce illegal activity on the part of internet users. A representative example of this line of thinking can be found in autocomplete suggestions that search engines offer to their users.⁶⁶² Whereas search engines do not fall into the scope of hosting ISSPs, this example can be equally applied to hosting ISSPs. This is because hosting ISSPs might offer a search list to their users in order to navigate themselves better within their websites.⁶⁶³ Autocomplete suggestions concern the

⁶⁶¹ See C. Riefa, *Consumer Protection and Online Auction Platforms: Towards a Safer Legal Framework* (Ashgate 2015) 67-123 where Riefa elaborates on the control of pre-contractual information in online auctions and the right of consumers to withdraw from online auctions; I. Lianos and K. Botwright, "Five ways to increase trust in e-commerce" (World Economic Forum, 22 March 2019) is available at <<https://www.weforum.org/agenda/2019/03/five-ways-to-restore-trust-in-e-commerce/>> last accessed 27 December 2019; World Economic Forum, "White Paper on The Global Governance of Online Consumer Protection and E-commerce Building Trust" (22 March 2019) is available at <http://www3.weforum.org/docs/WEF_consumer_protection.pdf> last accessed 27 December 2019.

⁶⁶² S. Karapapa and M. Borghi, "Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm" (2015) 23 *International Journal of Law and Information Technology* 261-289.

⁶⁶³ Another important reason addresses that hosting ISSPs' power has political dimensions. There are cases where hosting ISSPs do not exert their power within the limits of a business corporation. Rather, they manage to influence the public with regard to political issues such as the national elections or important Referendums. With regard to national elections, an outstanding example is the Cambridge Analytica scandal. Cambridge Analytica is a UK data profiling organization that uses a number of psychological tools in order to predict the outcome of important political events based on voters' personal profiles. In light of the US elections in 2016, Facebook gave access to Cambridge Analytica's experts so that they collect via an app its users' data within the US jurisdiction and create psychological profiles for each of them. After collecting users' data and without their permission, Cambridge Analytica offered this database to Trump's campaigners with the aim to influence voters' choices at the day of the US elections. In this way, despite Zuckerberg's refusal, Facebook has enabled the manipulation of US voters through the non-authorized use of its users' personal data. Hence, it seems that major political outcomes could be influenced by hosting ISSPs' services; A documentary on Netflix with the title "The Great Hack" explores allegations of Facebook selling its users' data without their consensus to Brexit campaigners ahead of the Brexit Referendum; "The Cambridge Analytical files: key stories" (The Guardian) is available at <<https://www.theguardian.com/news/series/cambridge-analytica-files>> last accessed 11 November 2019; L. Edwards, "Privacy and Data Protection" in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 56-57; I. Lapowsky, "How Cambridge Analytica Sparked the Great Privacy Awakening Repercussions from the scandal swirling around the data analytics firm continue to be felt across the tech industry" (Wired, 17 March 2019) is available at <<https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/>> last accessed 11 November 2019; For instance, the free Basics service aimed to launch an initiative in India in order to offer free services to low-income citizens. The service enabled the user to access the internet via their mobile phones after entering Facebook's website. With this service, Facebook's CEO's claimed that they fight social inclusion and the digital divide. However, this initiative has been subjected to severe criticism. Its opponents argue that the Free Basics program is a walled garden

suggestions that are provided in the search bar lists once the internet user starts typing a term. In that case, the French Supreme Court has found that the use of the terms Rapidshare and Megaupload that showed up next to suggested websites of the search results 'systematically orients internet users'⁶⁶⁴ towards the commission of illicit activities.⁶⁶⁵ In this way, search engines could induce internet users to commit infringing acts such as the download of unauthorized films or songs. Likewise, in *LUSH* case,⁶⁶⁶ the English Court of Appeal has found that Amazon's search list that offered a number of competitive products once the online consumer started typing LUSH violates the function of the trade mark and thus it might trigger confusion to the average consumer.⁶⁶⁷ Hence, the suggestion of competitive goods by the autocomplete function could lead to the violation of trade marks online.

In the light of the above, one may conclude that the ascription of a responsibility framework is justified due to the emerging role of hosting ISSPs. Such a role, in contrast with the role of hosting ISSPs as perceived in the ECD in 2000, represents hosting ISSPs as powerful market players that control information flow,⁶⁶⁸ shape public and political discourse as well as enforce and adjudicate rights online. Yet, whilst hosting ISSPs are entitled to enforcement and adjudication duties, this does not mean that they should subordinate their business interests. However, those business interests may lead them to undermine the rights of their less powerful individual- users and rights holders and

whose function is directly manipulated by Facebook. Subsequent to these allegations, the Indian Government decided to ban this initiative. Yet, Facebook invoked the status of an international actor that contributes to the development of lower-income countries and put pressure on the Indian government by sending emails and stressing the importance of the right to connectivity. Thus, it appears that hosting ISSPs can exercise influence to a certain degree on political governments and participate in the discussion of seminal agendas such as the international economic and social developments of the poorer countries; More see in D. Broeders and L. Taylor, "Does Great Power Come with Great Responsibility? The Need to Talk About Corporate Political Responsibility" in M. Taddeo and L. Floridi (eds.), *The responsibilities of online service providers* (Springer 2017) 319; J. Kiss, "Mark Zuckerberg defends Facebook's motives in free internet project in India" (The Guardian, 28 December 2015) is available at <<https://www.theguardian.com/technology/2015/dec/28/mark-zuckerberg-facebook-india-internet-free-basics>> last accessed 27 December 2019; J. Hempel, "Zuckerberg to the UN: The Internet Belongs to Everyone" Wired Business (Wired, 28 September 2015) is available at <www.wired.com/2015/09/zuckenber-to-un-internet-belongs-to-everyone/> last accessed 27 December 2019.

⁶⁶⁴ S. Karapapa and M. Borghi, "Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm" (2015) 23 *International Journal of Law and Information Technology* 282.

⁶⁶⁵ *Syndicat National de l'Édition Phonographique (SNEP)/Google*, Cour de Cassation, 12 July 2012 (France)

⁶⁶⁶ *Cosmetic Warriors Ltd v Amazon.co.uk Ltd* [2014] EWHC 181 (Ch).

⁶⁶⁷ *Ibid.*

⁶⁶⁸ As Revolidis has rightfully summarized "the activities of internet intermediaries constitute the basic backbone of current internet technology" in I. Revolidis, "Internet intermediaries and copyright enforcement in the EU: In search of a balanced approach" in M. Corrales, M. Fenwick and N. Forgó (eds.), *New Technology, Big Data and the Law* (Springer 2017) 224.

therefore adopt a “lowest common denominator”⁶⁶⁹ for the protection of their rights. For this reason, the establishment of a responsibility framework for hosting ISSPs might offer a greater degree of protection for the rights of internet users and right holders respectively.

However, the introduction of a handful of responsibilities for hosting ISSPs does not only relate to the new role they exercise in the Web 2.0 era. Indeed, it is also backed up by a strong theoretical framework that stems from internet co-regulatory theories expressed by Reidenberg and Lessig. The following section explores these theoretical approaches that reinforce the imposition of a responsibility framework based on co-regulation on the hosting ISSPs.

III. Theoretical underpinnings of the responsibility framework for hosting ISSPs: internet co-regulatory theories

The section below addresses two internet regulatory theories as expressed by Reidenberg and Lessig respectively.

A. *Reidenberg’s Lex Informatica theory*

The proposed responsibility framework based on co-regulation can be influenced by Reidenberg’s theory. Drawing parallels with *Lex Mercatoria*, which was the prevailing law during medieval times, Reidenberg introduced the *Lex Informatica* theory.⁶⁷⁰ This theory is based upon the idea of networks’ decentralization, within which the state can influence the regulation of internet infrastructure through ISSPs.⁶⁷¹ This means that hosting ISSPs would not be the sole entities to undertake the role of the enforcer of rights online. Rather, governmental authorities would be able to regulate online activities with the cooperation of hosting ISSPs. Therefore, a regulatory framework for hosting ISSPs could be built through public oversight, namely through the state as an external regulator.⁶⁷²

In practice, this could mean that hosting ISSPs’ would be assigned with a set of responsibilities with regard to the dissemination of unlawful content. These

⁶⁶⁹ In other words, a lower standard; see O. Lysnkey, “Regulation by Platforms: The Impact on Fundamental Rights” in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018) 92.

⁶⁷⁰ J. Reidenberg, “Governing Networks and Rule-Making in Cyberspace” (1996) 45 *Emory Law Journal* 911.

⁶⁷¹ J. Reidenberg, “Lex Informatica: The formulation of Information Policy Rules through Technology” (1997) 76 *Texas Law Review* 577.

⁶⁷² A. Murray, *Information Technology Law: The Law and Society* (Oxford University Press 2019) 60.

responsibilities would be subject to a hosting ISSP supervisory authority, which would be government based. Indicative examples can be found in the context of a number of European member states that have introduced supervisory authorities that deal with the blocking of websites with infringing content and the imposition of fines in cases of non-compliance with the legal rules. For instance, in Greece,⁶⁷³ Italy,⁶⁷⁴ Spain⁶⁷⁵ and the UK,⁶⁷⁶ intellectual property holders could resort to supervisory authorities in order to seek redress for the infringements of their rights online. This recommended hosting ISSP supervisory authority is discussed in chapter 6 of this thesis.

Yet, it is worth mentioning that the limits of this responsibility regime based on co-regulation should be clearly carved out in order to avoid any shift from co-regulation to state regulation. Indeed, Reidenberg acutely warns that “state governments cannot and should not attempt to expropriate all regulatory power from network communities.”⁶⁷⁷ This is because the threat of a state regulation could impede the boost of e-commerce since state regulation rules “become outdated shortly thereafter.”⁶⁷⁸ This means that the intervention of state regulation might act as a deterrent for innovation since legal rules cannot efficiently follow the rapid progress of technological developments. What is more, lack of boundaries of the role of the state within the internet regulation might pose a serious threat to the flow of content online since there might be a risk of abuse and censorship. This has already been exemplified in a number of countries outside Europe, such as China, where the authorities have deployed special routers, known as The Great Firewall, to prohibit internet users from accessing banned websites.⁶⁷⁹ This means that if an internet user attempts to access a banned website, a network error message appears

⁶⁷³ General information on the Greek Committee on intellectual property violations is available at < <https://www.opi.gr/en/committee/general-information> > last accessed 11 April 2019.

⁶⁷⁴ Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 April 2003, No. 70 is available at < <https://www.agcom.it/documents/10179/0/Documento/b0410f3a-0586-449a-aa99-09ac8824c945> > last accessed 27 December 2019; in English is available at < <http://www.portolano.it/wp-content/uploads/2013/12/English-translation-of-the-IT-Regulation-on-the-copyright.pdf> > last accessed 27 December 2019.

⁶⁷⁵ Out of Laws News, “Spain legislates for out-of-court copyright enforcement” (Out of Law Blog, 29 November 2018) is available at < <https://www.out-law.com/en/articles/2018/november/spain-out-of-court-copyright-enforcement/> > last accessed 27 December 2019.

⁶⁷⁶ ISP Review, “UK Gov Aim to Make ISP Piracy Website Blocks Cheaper and Easier” (ISP review, 15 June 2018) is available at < <https://www.ispreview.co.uk/index.php/2018/06/uk-gov-to-make-isp-piracy-website-blocks-cheaper-and-easier.html> > last accessed 27 December 2019.

⁶⁷⁷ J. Reidenberg, “Governing Networks and Rule-Making in Cyberspace” (1996) 45 Emory Law Journal 929.

⁶⁷⁸ F. H. Easterbrook, “Cyberspace and the Law of the Horse” (1996) 1 University of Chicago Legal Forum 207.

⁶⁷⁹ A. Guadamuz, “Internet Regulation” in L. Edwards (ed.), *Law, policy and the internet* (Hart Publishing Oxford 2019) 20; J.L. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) 96-97 where the authors argue that China is using Internet as a tool of political control.

on her screen.⁶⁸⁰ Hence, without any clear clarification of the role of the state in the internet regulation, risks of information censorship might occur.

Interestingly, Reidenberg's theory has been further developed by Lessig in his seminal book *Code and other Laws of Cyberspace*.⁶⁸¹

B. Lessig's theory

Lessig's theory draws upon Reidenberg's *Lex Informatica* and further expands the concept of co-regulation within the internet infrastructure. Pursuant to Lessig's theory, internet can be regulated via four modalities, namely market, norms, code⁶⁸² and law.⁶⁸³ This means that those four modalities could influence internet users' activities and thus shape their online behavior. In the brick and mortar environment, those four modalities could restrict citizens' actions. For instance, consider the case of tobacco regulations.⁶⁸⁴ The state, under the threat of public health, aimed at reducing the consumption of tobacco packs and cigars. In order to achieve this policy, the state used some of the four modalities, as depicted in Lessig's theory. Therefore, the states have increased the price of tobacco products via the markets, prohibited the consumption of smoking in closed spaces and prohibited the advertisement of tobacco products via the media. In this way, the state achieved to influence the behavior of individuals.

Within the online context, Lessig's theory could enable the state to regulate hosting ISSPs' activities for copyright and trade mark infringements via these four modalities. Without undermining the power of the modalities of norms and market, this thesis argues that the appropriate modalities with regard to the research topic concern the modalities of law and code. So, firstly, given that this thesis adopts a legal approach, this could mean that legislation could be used by governmental authorities in order to regulate internet users' activities. Based on Lessig's theory, this means that the state can impose a set of

⁶⁸⁰ J.L. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006) 58.

⁶⁸¹ L. Lessig, *Code and other Laws of cyberspace* (1999) 43-44

⁶⁸² Ibid where Lessig argues that "even if it is hard to regulate behaviour given the Net as it is, it is not hard for the government to take steps to alter, or supplement, the architecture of the Net" and "if the government regulates the architecture of the Net, it could be regulated in the future"; A. Guadamuz, *Networks, Complexity and Internet Regulation: Scale Free Law* (Edward Elgar 2011) 86-89 where Guadamuz notes that "...several countries started redesigning the entry points into their national networks in order to impose screening mechanism that would allow them to filter out undesired content if necessary."

⁶⁸³ L. Lessig, *Code, version 2.0* (2006) 123.

⁶⁸⁴ M. Taddeo and L. Floridi, "The Debate on the Moral Responsibilities of Online Service Providers" (2016) 22 *Science and Engineering Ethics* 1575-1603.

responsibilities to hosting ISSPs with regard to the circulation of infringing content and counterfeit goods. Such responsibilities, which are discussed in Section IV of this chapter as well as in chapters 5 and 6, would be imposed by a legal reform and would aim to terminate the infringing content online as well as safeguard internet users' and consumers' rights. Secondly, on the basis of Lessig's theory, the state could endorse the establishment of a hosting ISSP supervisory authority. Without restricting access to judicial authorities for right holders and internet users/ consumers, the proposed hosting ISSP supervisory authority could impose liability on hosting ISSPs for the activities that might occur within their platforms.

Yet, while this theory has its own merits, it prompts reflections on the legitimacy of those authorities that would allocate liability to hosting ISSPs.⁶⁸⁵ For instance, the proposed hosting ISSP supervisory authority must entail an array of principles under which it would operate. These principles would act as a safeguard for all the parties at stake. This means that the proposed hosting ISSP supervisory authority would guarantee the rights of the intellectual property holders whose rights have been violated without undermining the rights of hosting ISSPs to conduct business and internet users to access content and goods online. Otherwise, a lack of legitimacy would erode the validity of its decisions, as discussed in chapter 6, and thus annul its own existence within the internet regulatory framework.

Accordingly, a responsibility framework based on co-regulation could draw upon Reidenberg's and Lessig's theories. Both theories argue that the state could restrict internet users' online activities via regulating the hosting ISSPs' services, namely either by the attribution of a set of responsibilities to hosting ISSPs or by holding them accountable to a hosting ISSP supervisory authority. Those theories may offer a solid theoretical underpinning for the creation of a new regulatory framework for hosting ISSPs that could balance the needs of the different parties at stake as well as deviate from the outdated and problematic approaches of the existing legislative tools that regulate hosting ISSPs' liability. In this respect, this brings us to the question of how such a framework, a thorough analysis of which will be discussed in the following section, shall be carved out.

⁶⁸⁵ V. Mayer-Schonberger, "Demystifying Lessig" (2008) 4 Wisconsin Law Review 713.

IV. How to construe a responsibility framework based on co-regulation for hosting ISSPs?

This section discusses a number of legislative and policy initiatives with regard to the imposition of a duty of care on hosting ISSPs, engages with criticism and counter-arguments for the imposition of a duty of care on hosting ISSPs, as documented by academic scholarship and then recommends how to shape a duty of care based on the legal principles that underlie the legal framework of hosting ISSPs and relevant case law. Finally, it discusses the limitations upon a duty of care, which would safeguard the business model of hosting ISSPs and the fundamental rights of internet users/ consumers.

A. A duty of care for hosting ISSPs at legislative and policy level

Within the context of online infringements, this thesis argues that hosting ISSPs need to take care in eliminating or terminating any misuse which arises on their networks and thus filter, scan or block any allegedly infringing content within their platforms.⁶⁸⁶ In other words, they should have a duty of care. This duty of care describes the proactive role that a hosting ISSP should adopt against the illicit material that is disseminated within its network.

The imposition of a duty of care on hosting ISSPs is not a novelty. Rather, its legal basis has been envisaged in Recitals 47 and 48 of the ECD.⁶⁸⁷ According to this provision, Member States may require from “service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities.”⁶⁸⁸ This means that hosting ISSPs might be forced to deploy preventive measures against the circulation of infringing material within their networks.

At policy level as well, the duty of care has been endorsed in a handful of several European policy documents that include recommendations on how hosting ISSPs would tackle the

⁶⁸⁶ G. Frosio describes the imposition of a duty of care as “ongoing move towards privatization of law enforcement” in G. Frosio and M. Husovec, “Accountability and Responsibility of Online Intermediaries” in G. Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press, forthcoming) 3.

⁶⁸⁷ Council Directive (EC) 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 (hereinafter ECD).

⁶⁸⁸ Recital 48 of the ECD.

increasing number of online intellectual property infringements within their networks.⁶⁸⁹ In these documents, hosting ISSPs are expected to adopt proactive measures in order to curb the dissemination of infringing material online. A duty of care has been for the first time endorsed in the DSM Strategy that addressed the steps to be taken in order to offer better enforcement of intellectual property rights in the online world. It has been noted that “the Commission will analyze the need for new measures to tackle illegal content on the internet, with due regard to their impact on the fundamental right to freedom of expression and information, such as rigorous procedures for removing illegal content while avoiding the take down of legal content, and whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems – a duty of care.”⁶⁹⁰ Likewise, after right holders’ requests for better enforcement of intellectual property rights online, the European Commission’s staff working document outlines the need for due diligence. More specifically, it notes that “another is whether to ask intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems.”⁶⁹¹ This demonstrates the need for a higher degree of responsibility of hosting ISSPs towards the dissemination of content within their networks.

Such a stance has been reinforced in the public consultation the EU Commission has conducted on the evaluation of the certain aspects of the Enforcement Directive.⁶⁹² More specifically, the right holders outlined that “a duty of care” for intermediaries at EU level

⁶⁸⁹ EU Commission, “A DSM Strategy for Europe” {SWD (2015) 100 final 12; EU Commission, “Recommendation on measures to effectively tackle illegal content online” (2018) 1177; see also HM Government, “Online Harms (White Paper)” (April 2019) 57; see also Theresa May’s speech on Davos where she announced the creation of a Digital Charter “The Digital Charter we are developing in the UK sets out the principles of our approach to agree the rights and responsibilities of the online world and to put them into practice” in World Economic Forum, Theresa’s May speech in Davos 2019 is available at <<https://www.weforum.org/agenda/2018/01/theresa-may-davos-address/>> last accessed 27 December 2019; A duty of care has already been applied in the context of terroristic content, hate speech and pornographic content; see EU Parliament, “Legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online” (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)); Council Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (2018) OJ L 303; EU Commission, “The EU Code of conduct on countering illegal hate speech online” is available at <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en> last accessed 27 December 2019.

⁶⁹⁰ EU Commission, “A DSM Strategy for Europe” {SWD (2015) 100 final 12.

⁶⁹¹ EU Commission, “A DSM Strategy for Europe - Analysis and Evidence {COM (2015) 192 final} 56-57.

⁶⁹² Council Directive (EC) 2004/48/EC on the enforcement of intellectual property rights (2004) O.J. L 157.

would be a step in the right direction and should extend to all intermediaries.”⁶⁹³ Further, the consultation notes that a number of respondents find that there is no balance between the interests at stake. In this light, they argue that hosting ISSPs must have a duty of care so as to prevent the circulation of infringing material within their networks.⁶⁹⁴ Likewise, the EU Commission’s citizens’ summary on EU action plan for enforcing intellectual property rights has stressed that the “idea is to encourage due diligence by all parties involved in these transactions -from suppliers and advertising agencies to payment service providers, even the rights-holders themselves.”⁶⁹⁵ Finally, the EU Commission Communication on a balanced intellectual property rights’ enforcement system warned about the negative impact of not imposing the concept of due diligence on hosting ISSPs. A lack of due diligence on hosting ISSPs would be detrimental for the e-commerce infrastructure since it would allow the circulation of counterfeit goods to a great extent, thus questioning the security of online purchases. Therefore, businesses and online consumers would be placed in a weak position.⁶⁹⁶

However, while the imposition of a duty of care is not only legally admissible but also encouraged at the policy level as well, many scholars have reflected on the ascription of a duty of care to hosting ISSPs.⁶⁹⁷ Firstly, scholars have debated the choice of a duty of care over existing mechanisms such as notice and take down mechanism or notice and notice mechanism. Secondly, they question the imposition of a duty of care on “neutral” hosting ISSPs. Thirdly, they express concerns on the conflict between Recital 48 of the ECD, which envisages a duty of care for hosting ISSPs and Article 15 of the ECD, which prohibits the imposition of general monitoring obligations on hosting ISSPs and has been a cornerstone for the development of the e-commerce infrastructure. An evaluation of these concerns follows.

⁶⁹³ EU Commission, “Public consultation on evaluation and modernisation of the legal framework for the enforcement of intellectual property rights” (2016) 52.

⁶⁹⁴ *Ibid*, 43.

⁶⁹⁵ EU Commission, “Citizens' summary EU action plan – enforcing intellectual property rights” is available at < <file:///C:/Users/krokida/Downloads/CS-EN.pdf> > last accessed 27 December 2019.

⁶⁹⁶ Commission, “A balanced IP enforcement system responding to today's societal challenges” {SWD (2017) 430 final} 9.

⁶⁹⁷ C. Angelopoulos and S. Smet, “Notice and Fair Balance: How to reach a compromise between fundamental rights in European Intermediary Liability” (2016) 8 *Journal Media of Law* 287-288; G. Frosio, “Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility” (2017) 25 *Oxford International Journal of Law and Information Technology* 5; D. Mac Sithigh, “The road to responsibilities: new attitudes towards internet intermediaries” (2019) *Information and Communications Technology Law* 18.

B. Criticism and counter-arguments for imposing a duty of care for hosting ISSPs

This section critically engages with the relevant criticism that has been flagged out and in particular addresses the choice of a duty of care against notice and take down and notice and notice mechanisms, its imposition to neutral hosting ISSPs and its conflict with the general prohibition of monitoring obligations as set forth in Article 15 of the ECD.

i. Duty of care vs notice and take-down mechanism and notice and notice mechanism

As discussed earlier, a duty of care on hosting ISSPs is envisaged at legislative and policy level. Yet, the majority of European member states have integrated the notice and take down system into their national legislations.⁶⁹⁸ For this reason, it is worth considering whether a notice and take down mechanism with the appropriate safeguards for users' rights could be recommended instead of imposing a duty of care. The majority of European member states have integrated the notice and take down system into their legislations.⁶⁹⁹ Pursuant to this system, a hosting ISSP can examine the validity of the claim and react either by rejecting the claim for removal of the content or taking down the content.⁷⁰⁰ For this reason, despite a number of empirical studies that demonstrate several flaws of the notice and take down system,⁷⁰¹ the introduction of this mechanism in 2000 has been warmly welcomed by scholars. As Van Eecke has pointed out, through the notice and take down system all the interests of the parties involved are taken into

⁶⁹⁸ A. Kuczerawy A, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards* (Intersentia 2018) 210.

⁶⁹⁹ Report of the Swiss Institute of Comparative Law commissioned by the Council of Europe, "Comparative study on filtering, blocking and take-down on illegal content on the internet" (2015); For an overview of EU member states that adopt the notice and take down process see A. Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards* (Intersentia 2018) 331-377.

⁷⁰⁰ P. Van Eecke, "Online service providers and Liability: A plea for a balanced approach" (2011) 48 *Common Market Law Review* 1455 where Van Eecke noted that "the notice-and-take-down procedure is one of the essential mechanisms through which the E-Commerce Directive achieves a balance between the interests of right holders, online intermediaries and users."

⁷⁰¹ C. Ahlert, C. Marsden and C. Yung, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation" (2014) is available at <<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>> last accessed 27 December 2019 ;_Lecture by Sjoera Nas, Bits of Freedom " The Multatuli Project ISP Notice & take down" (2004) is available at <<https://www-old.bof.nl/docs/researchpaperSANE.pdf>> last accessed 27 December 2019; It has been found that the number of notices might increase compliance costs as well as encroach upon the principle of due process in K. Erickson and M. Kretschmer, "Empirical approaches to intermediary liability" (2019) 6 CREATE Working Paper 6.

consideration.⁷⁰² This is because through the notice and take down system, the right holder sends a notice to the ISSP alleging copyright or trade mark violation. Upon examining the validity of the notice, the hosting ISSP reaches the decision whether to remove the allegedly infringing material or not. It is this examination on the part of the hosting ISSP that might protect internet users' fundamental rights to information and expression.

However, the imposition of a duty of care could have advantages over the notice and take down system. This is mainly because the aim of a duty of care is to prevent the emergence of the same infringement online. Conversely, with the notice and take down system, the same infringement might occur again "hydra-like" within the online platform.⁷⁰³ This is because while Hercules cut Lernean Hydra's one head, two heads emerged.⁷⁰⁴ In this sense, a notice and take down system might not impede the increasing number of infringements in the digital world since it is considered a "Sisyphean task".⁷⁰⁵

Further, it could be argued that a notice and notice system would be more preferable over the imposition of a duty of care. Policymakers should endorse a notice and notice mechanism with the appropriate safeguards for users' rights. This mechanism treats a hosting ISSP as an intermediary since, after being notified of the infringement, intermediary's duties are limited to sending a notification to the allegedly infringing user. As Angelopoulos notes, this mechanism "restricts intermediaries to their natural role as middlemen and returns the job of enforcing rights and obligations to the courts."⁷⁰⁶ This implies that hosting ISSPs would not be treated anymore as enforcers and adjudicators of intellectual property rights since judicial authorities would now decide on the illegal nature of the content and offer redress to the intellectual property holders.

However, this assumption can be misleading. This is because the crucial point here is not to give hosting ISSPs immunity for circulating infringing material. Rather, since their

⁷⁰² P. Van Eecke, "Online service providers and Liability: A plea for a balanced approach" (2011) 48 Common Market Law Review 1455.

⁷⁰³ J.C. Ginsburg, "Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs" (2008) 50 Arizona Law Review 591; A. Giannopoulou, "Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality" (2012) 3 European Journal for Law and Technology 1.

⁷⁰⁴ Hydra Greek Mythology (Encyclopedia Britannica) is available at <<https://www.britannica.com/topic/Hydra-Greek-mythology>> last accessed 24 April 2019.

⁷⁰⁵ L. Helman and G. Parchomovsky, "The best available technology standard" (2011) 111 Columbia Law Review 1204.

⁷⁰⁶ C. Angelopoulos and S. Smet, "Notice and Fair Balance: How to reach a compromise between fundamental rights in European Intermediary Liability" (2016) 8 Journal Media of Law 266.

services, as Friedmann notes, “shapes infringements”,⁷⁰⁷ hosting ISSPs should undertake in principle a higher degree of participation in the battle against online infringements. This is illustrated in the case of the Pirate Bay website. Due to its infrastructure, internet users are able to file exchange unauthorized files. Moreover, in order to increase traffic on its website and increase advertisement revenues, the website invited internet users to share their illegal files with each other. In this sense, the business model of Pirate Bay shaped the infringements through inducing its clients to exchange files via its peer to peer network.

ii. From neutral to active hosting ISSPs

Another concern to be addressed is the imposition of a duty of care to hosting ISSPs whose function does not address an active involvement in the dissemination of content online. In this respect, it could be questioned how plausible it is to ascribe a duty of care to those hosting ISSPs whose nature is neutral and whose services are limited to hosting and storing content uploaded by their users.

Hosting ISSPs are understood as neutral entities in view of the passive nature of the services they provide to the end-users.⁷⁰⁸ This understanding has been outlined in the *Google v Louis Vuitton case*⁷⁰⁹ where Louis Vuitton initiated legal proceedings against Google alleging trade mark violation via Google’s AdWords.⁷¹⁰ Google AdWords is a paid service which offers to advertisers the option to advertise their products when users enter specific search terms. In this case, Google AdWords offered advertisements of fake Louis Vuitton bags when users type the keywords Louis Vuitton in the search engine. After a careful consideration of the facts, the Court did not attribute liability to Google for trade mark infringement because it perceived its role as neutral. By neutral is understood, as the CJEU noted, the conduct that is “merely technical, automatic and passive, pointing to

⁷⁰⁷ D. Friedmann, “Sinking the Safe Harbour with the legal certainty of strict liability in sight” (2014) 9 *Journal of Intellectual Property Law and Practice* 148-155 where Friedmann gives the example of the algorithm “if one assumes that the algorithms of an OSP to optimise the transactions between a third party and internet users, were merely technical, automatic and passive, but have the result that they induce infringements, the OSP has the option to fix this problem in the algorithm under their control after it becomes aware of the problem.”

⁷⁰⁸ See discussion on the passive nature of hosting ISSPs in P. Jougoux, “The role of internet intermediaries in copyright law online enforcement” in T. Synodinou, P. Jougoux, C. Markou and T. Prastitiou (eds.) *EU Internet Law: Regulation and Enforcement* (Springer 2017) 273.

⁷⁰⁹ Case C-236/08 - *Google France and Google* (2010) ECLI:EU:C:2010:159.

⁷¹⁰ C. Volkmann, “Trademark Use and Liability of Referencing Service in Keyword Advertising – Google AdWords and Trademark Law” (2011) 3 *European Journal of Risk Regulation* 450.

a lack of knowledge or control of the data which it stores.”⁷¹¹ This means that the concept of neutrality amounts to the passive function of hosting ISSPs provided that they are deprived of knowledge and control of the content that is hosted via their platforms. Therefore, hosting ISSPs were treated as neutral entities since they did not engage with the circulation of content and goods within their platforms.

Nonetheless, while hosting ISSPs would have incentives to maintain the rhetoric of neutrality so as to evade any accountability,⁷¹² the concept of neutrality does not align with the technological developments of 2019. This is because this provision was drafted in 1999 when the hosting providers were related to forums and blogs.⁷¹³ Yet, with the advent of Web 2.0, hosting providers are not neutral anymore and thus do not limit their services to hosting content. Rather, they are seen as active entities that index material, decide which content reaches the end-users and circulate the content within their networks. As van der Sloot pointed out “in the modern internet landscape however, providers have become much more active, for example by providing the platform on which information is shared by users, by indexing this information, by making it searchable and by publishing and distributing the information over the internet.”⁷¹⁴ This means that following the technological evolution, the business model of hosting ISSPs has been transformed.

More specifically, hosting ISSPs nowadays govern a wide range of activities and are active towards the usage of the content⁷¹⁵ since they index it and choose which information

⁷¹¹ Case C-236/08 - *Google France and Google* (2010) ECLI:EU:C:2010:159, para. 114.

⁷¹² U. Kohl, “Google: The rise and Rise of online intermediaries in the Governance of the Internet and Beyond (Part 2)” (2013) 21 *International Journal of Law and Information Technology* 187.

⁷¹³ A. Lodder, “Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market” in A. Lodder and A. Murray (eds), *EU Regulation of E-Commerce: A commentary* (2017) 51; The French High Council for Literary and Artistic Property notes that “Although all parties noted that the above activities do not match the assumptions made by the European authorities in 2000 when the legislation was drafted,” in The French High Council for Literary and Artistic Property, “Mission to Link Directives 2000/31 and 2001/29 – Report and Proposals” (2016) 7 *Journal of Intellectual Property, Technology and E-Commerce* is available at <<https://www.jipitec.eu/issues/jipitec-7-2-2016/4436>> last accessed 27 December 2019.

⁷¹⁴ B. van der Sloot, “Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe” (2015) 6 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 212.

⁷¹⁵ Whilst the ECD provisions consider hosting ISSPs as passive entities and limit the scope of their functions into storing temporary data, transmitting information or offering space for users to upload content, see P. Van Eecke thinks that although mere conduit and caching providers have a neutral role, the hosting providers exercise greater involvement with their users. To explain his view, Van Eecke cites the following example “For example, when offering a website on which users can upload and store their personal photos or videos, the website operator must make available some tools to allow users to upload, categorize and display the information towards the usage of the content transmitted via their networks, the hosting providers exercise greater involvement in distributing the information” in P. van Eecke, “Online Service Providers and Liability: A Plea for a Balanced Approach” (2011) 48 *Common Market Law Review* 1483. However, Revolidis criticizes

reaches the end-users.⁷¹⁶ As Hurwitz notes “active intermediaries now are capable of using and manipulating user data in ways that were never before possible...”⁷¹⁷ For example, social network platforms or video sharing networks or digital auction platforms are not merely hosting the content posted by users or enabling sellers to display their goods within their networks. Rather, they are suggesting links to content which users may find more appealing on the basis of their preferences or make easier for users to search for their favorite material.⁷¹⁸ Hence, it appears that hosting ISSPs adopt a more dynamic role that is far from passivity and neutrality.

This active role of hosting ISSPs has been mirrored in a bedrock of court rulings where hosting ISSPs have been treated as active entities at the European level. For instance, in the cases of *Delfi*,⁷¹⁹ *Costeja*,⁷²⁰ *Stichting Brein v Ziggo*⁷²¹ and *GS Media*,⁷²² the CJEU endorsed an active role for hosting ISSPs since they are now more active in the dissemination of content throughout their platforms. Whereas the first two rulings addressed defamatory and privacy issues, it seems worth mentioning them since they were the first rulings that introduced the active role of hosting ISSPs. For example, in the *Delfi* ruling delivered by the European Court of Human Rights,⁷²³ an individual user requested that Delfi, a news portal with very high traffic in Estonia, remove offensive comments which also entailed threats against him. After a careful consideration of the facts, the Court did not find Delfi liable, but in light of the ‘comments’ section on the website, the Strasbourg Judges considered Delfi as an active entity. In particular, they noted that “[i]t is certainly true that the active intermediary can exercise control over the comments that appear on its site and it’s also true that by creating a space for comments, and inviting users to participate, it engages in an expressive activity that entails

this view and notes that “the neutral role of internet service providers is not to be measure only on their function per se, but it must also be projected on their participation in the production of information. It is the knowledge and the control of information that would take them out of the realm of intermediaries not the mere distribution of information that would take them out of the realm of intermediaries” in I. Revolidis, “Internet Intermediaries and Copyright Enforcement in the EU: In search of a Balanced Approach” in M. Corrales, M. Fenwick, N. Forgo (eds.) *New Technology, Big Data and the Law* (Springer 2017) 231; see also A. Kuczerawy, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards* (Intersentia 2018) 97-98.

⁷¹⁶ B. van der Sloot, “Welcome to the Jungle: The Liability of internet Intermediaries for Privacy Violations in Europe” (2015) 6 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 211.

⁷¹⁷ J. Hurwitz, “Trust and Online Interaction” (2013) 161 *University of Pennsylvania Law Review* 1593.

⁷¹⁸ C. Yoo, *The dynamic internet* (2012) Chapter 9.

⁷¹⁹ ECtHR, Grand Chamber, *Delfi AS v Estonia*, 16 June 2015, Application no. 64569, (2015) E.M.L.R

⁷²⁰ Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) ECLI:EU:C:2014:317.

⁷²¹ Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456.

⁷²² Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644.

⁷²³ ECtHR, Grand Chamber, *Delfi AS v Estonia*, 16 June 2015, Application no. 64569, (2015) E.M.L.R 26.

responsibility”⁷²⁴ and have concluded that with the comments’ part it offers to the users, Delfi’s role went “beyond that of a passive, purely technical service provider.”⁷²⁵

Further, in *Costeja* ruling⁷²⁶ the Court of Justice examined the dispute between a Spanish citizen and Google Spain which declined his request to take down search results that linked to a Spanish online newspaper. These search results were about a past social security debt that has been paid back and thus was not relevant anymore. At the outset, the Luxembourg judges outlined that Google’s search services play a seminal role in the spread of information online.⁷²⁷ Such dissemination could occur with the processing of personal data conducted by Google. For this reason, the Court explained that “it is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity...”⁷²⁸ This means that the courts perceive that search engines do not maintain a passive role towards the searching results. Rather, it is presumed that search engines adopt an active role since they process data with a view to provide a list of searching results.⁷²⁹ Although this conclusion has been applied to search engines, a similar stance could be equally applied to hosting ISSPs. This understanding has been reinforced in the following case at the European level.

Similar to the cases that deal with privacy and defamatory issues, the CJEU then endorsed an active role for hosting ISSPs with regard to copyright infringements in the *Stichting Brein v Ziggo BV and XS4All Internet BV* ruling. In this case, the CJEU examined the question of whether Pirate Bay’s activities which enable users to download files via a peer-to-peer software constitute communication to the public as per Article 3 of the InfoSoc Directive.⁷³⁰ This case was referred from the Dutch Court of Appeal where Stichting Brein, a Dutch foundation that protects the rights of creators requested a blocking injunction against Ziggo and XS4All Internet, two internet service providers, to terminate the access to their users to the Pirate Bay website. After careful consideration of the facts, the CJEU

⁷²⁴ Ibid.

⁷²⁵ ECtHR, Grand Chamber, *Delfi AS v Estonia*, 16 June 2015, Application no. 64569, (2015) E.M.L.R note 146.

⁷²⁶ Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) ECLI:EU:C:2014:317, para. 33.

⁷²⁷ ECtHR, Grand Chamber, *Delfi AS v Estonia*, 16 June 2015, Application no. 64569, (2015) E.M.L.R note 36

⁷²⁸ Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) ECLI:EU:C:2014:317, para. 33.

⁷²⁹ S. Stalla-Bourdillon, “Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well...” In M. Taddeo and L. Floridi (eds.) *The Responsibilities of Online Service Providers* (Springer 2017) 287.

⁷³⁰ Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456.

held that Pirate Bay's actions to redirect users to websites with unauthorized content amounts to communication to the public on the basis that The Pirate Bay is "a sharing platform which, by means of indexation of metadata relating to protected works and the provision of a search engine, allows users of the platform to locate those works..."⁷³¹ This means that to index files and enable users to find them via search engine service imply the active involvement of The Pirate Bay towards the circulation of unauthorized content. Therefore, while this ruling has been severely criticized since it attributes primary liability rules to The Pirate Bay,⁷³² it shows clearly that the Court treats hosting ISSPs with file-sharing function as active hosting ISSPs.

Finally, in the *GS Media* ruling, the active status of hosting ISSPs was confirmed. This case was a referral from the Dutch Supreme Court to the CJEU and it examined the liability of linking provider to unauthorized content, in this case the nude photos of a Dutch celebrity prior to their publication in a magazine. Upon assessing the facts, the CJEU held that since GS Media, as operator of the website *GeenStijl*, has a profit-gain aim, it must conduct the necessary control to ensure the legality of the material to which the users are redirected via the link that is provided.⁷³³ In this way, GS Media is assumed that it has knowledge over the illegal content and thus could be held liable for copyright infringements via hyperlinking.⁷³⁴ To counter the presumption of knowledge, the hosting ISPSS shall provide evidence that it carried out all the necessary controls in order to confirm the lawful nature of the content.⁷³⁵ Therefore, it appears that GS Media shall undertake an active role towards the dissemination of content online in order to escape liability.

⁷³¹ Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456, para .18.

⁷³² This ruling prompts reflections on the academic scholarship. J.B. Nordemann, "Liability of Online Service Providers for Copyrighted Content- Regulatory Action needed?" (2017) IMCO Committee notes that "the role of the Pirate Bay as a platform to connect users of the BitTorrent protocol for infringing activity was evaluated by the CJEU as primary liability for communication to the public." Angelopoulos states that "the result would be a judge-made harmonisation of indirect (i.e. accessory) copyright liability and one, moreover, that engulfs it within primary liability." in C. Angelopoulos, "AG Szpunar in *Stichting Brein v Ziggo*: An Indirect Harmonisation of Indirect Liability" (Kluwer copyright blog, 23 March 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/03/23/ag-szpunar-stichting-brein-v-ziggo-indirect-harmonisation-indirect-liability/>> last accessed 3 October 2019; Rosati as well "Further to the CJEU decision in The Pirate Bay situations like the one examined by the CJEU should be assessed by national courts under the lens of primary – rather than secondary – liability." In E. Rosati, "The CJEU Pirate Bay judgment and its impact on the liability of online platforms" (2017) 39 *European Intellectual Property Law Review* 12.

⁷³³ Case C-160/15, *GS Media BV v Sanoma Media Netherlands BV and Others* (2016) EU:C:2016:644, para. 51.

⁷³⁴ E. Papadaki, "Hyperlinking, making available and copyright infringement: lessons from European national courts" (2017) 8 *European Journal of Law and Technology* 12.

⁷³⁵ E. Rosati, "GS Media and Its Implications for the Construction of the Right of Communication to the Public within EU Copyright Architecture" (2017) 54 *Common Market Law Review* 1242.

Bearing in mind the above, there is an emergent trend in judicial rulings that confirm an active role for hosting ISSPs. These rulings dictate that hosting ISSPs are not neutral but are actively engaged in the distribution of goods and transmission of information that reaches the end-users. Therefore, the idea of hosting ISSPs as neutral entities seems to have been replaced by hosting ISSPs as entities who index content and make it subsequently available to the audience online. This understanding might offer a solid justification for the recommendation of this thesis for establishing a responsibility framework for hosting ISSPs based on co-regulation.

iii. Duty of care vs general monitoring: lack of clash

As discussed earlier, a duty of care has been envisaged in Recital 48 of the ECD. This provision dictates that hosting ISSPs might deploy preventive measures in order to prevent the emergence of online infringements. Yet, a number of commentators argue that the imposition of a duty of care might not be in accordance with the prohibition of general monitoring obligations as set forth in Article 15 of the ECD.⁷³⁶

Pursuant to Article 15 of the ECD the imposition of general monitoring obligations to hosting ISSPs is precluded. This means that hosting ISSPs are not obliged by law to deploy mechanisms in order to identify the allegedly infringing content online. Nonetheless, a growing body of academic scholarship argues that the prohibition of general monitoring shall not be construed as an absolute exclusion of filtering mechanisms by hosting ISSPs.

To restrict hosting ISSPs' reaction to mere removal of the infringing content upon being notified might be against the EU *acquis*. Firstly, it could be against Recital 47 of the ECD that allows the imposition of monitoring obligations to hosting ISSPs in specific cases. Indeed, Recital 47 states that "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and..." It is this conflict between a Recital and an Article that has generated mounting concerns as to which of the two prevails. However, this concern is but an illusion. This thesis argues that there is no conflict between a Recital and an Article of a Directive. This is because Recitals are

⁷³⁶ Council Directive (EC) 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 (hereinafter ECD).

considered “interpretative tools”⁷³⁷ of the provisions of the Directive. This interpretation takes into consideration the purpose of the Directive. Given that the overall purpose of the Directive is to curb the dissemination of infringing content within the online world, it is understood that proactive measures are allowed.

Indeed, this understanding has been reinforced at policy level. The Director General of the DG Internal Market stated that Article 15 is about “...certain duties of care which can be reasonably be expected from service providers and which are specified in national law. Such duties of care could for instance consist in making available of complaint-systems or in the operation of notice and take down procedures....”⁷³⁸ This implies that hosting ISSPs are expected to adopt a proactive stance towards the circulation of infringing content. Otherwise, the exclusion of all proactive measures would force hosting ISSPs merely to remove content.⁷³⁹

Secondly, it could be against the established line of CJEU case law that ascribes not only take down duties but also preventive duties on hosting ISSPs. A representative example can be found in the *L’Oreal v Ebay* case.⁷⁴⁰ In this case, the CJEU handed down that eBay shall prevent the displacement of counterfeit goods of L’Oreal on its platform, outlining that “the measures, procedures and remedies to be provided for should include prohibitory measures aimed at preventing further infringements of intellectual property rights”.⁷⁴¹ This means that eBay’s role would not amount only to the termination of the illicit activity but also to the prevention of future infringements.

In a similar fashion, in *Scarlet v Sabam*,⁷⁴² although the Court outlined the prohibition of general monitoring obligations, it explicitly noted that hosting ISSPs are allowed “to take measures aimed not only at bringing to an end infringement already committed against intellectual-property rights using their information-society services, but also at preventing

⁷³⁷ R. Baratta, “Complexity of EU Law in the domestic implementing process” (2014) 2 *The Theory and Practice of Legislation* 296.

⁷³⁸ Letter of Director of DG Internal Market J. Mogg to MEP Cederschild (13 June 2000) is available at <<https://www.asktheeu.org/en/request/2250/response/7914/attach/2/letter%20Mogg%20to%20MEP.pdf>> last accessed 27 December 2019.

⁷³⁹ J. B. Nordemann, “Are preventive duties on hosting service providers in line with EU law? Some comments from a legal perspective on Art. 13 Draft DSM Directive and “upload filters” (Kluwer Copyright blog, 28 June 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/06/28/preventive-duties-hosting-service-providers-line-eu-law-comments-legal-perspective-art-13-draft-dsm-directive-upload-filters/>> last accessed 27 December 2019.

⁷⁴⁰ Case C-324/09, *L’Oreal SA V eBay Int’l AG* [2011] E.C.R. I-6011.

⁷⁴¹ *Ibid.*

⁷⁴² Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

further infringements.”⁷⁴³ This implies that under certain conditions Scarlet shall exercise a proactive role and thus undertake any precautionary measures in order to prevent its customers from downloading unauthorized films.

Similarly, in the *UPC Telekabel* ruling, which was a referral from the Austrian Appeal Court,⁷⁴⁴ two film production companies requested the issue of a blocking injunction against UPC Telekabel, an ISSP that gave access to websites with unauthorized films. After careful consideration of the facts, the CJEU reinforced the compatibility of outcome injunctions with the European fundamental rights. This is because, as the Court noted, it does not violate the fundamental right of hosting ISSP to conduct business as per Article 16 of the EU Charter of Fundamental Rights while at the same time it enables the recipient of the injunction to undertake all reasonable measures to avoid liability.⁷⁴⁵ For the current narrative, the second explanation seems the most interesting. This is because the Court introduced the concept of reasonable measures that hosting ISSPs must have taken in order to exonerate liability.⁷⁴⁶ Such measures imply a proactive nature. This means that they should prevent the emergence of online infringement or at least to curb at a greater extent the online infringements. As the Court noted, the measures to adopt shall be effective in the sense that they must protect the fundamental right to property as enshrined in Article 11 of the European Charter of Fundamental Rights but also in the sense that they must prevent the access of internet users to unauthorized content that could place into peril the right of content owners and brand owners to safeguard their property.⁷⁴⁷ In this light, with this ruling the CJEU explicitly carved out the path for the imposition of obligations on hosting ISSPs by endorsing the concept of reasonable measures.

⁷⁴³ Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85, para. 18; see also L. Edwards, “With Great Power Comes Great Responsibility? The Rise of Platform Liability” in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 280 where Edwards notes that “Nonetheless, Scarlet still upheld the principle that a filtering injunction might be possible if properly tailored and constrained”.

⁷⁴⁴ Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (2014) ECLI:EU:C:2014:192, para. 51-52.

⁷⁴⁵ Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (2014) ECLI:EU:C:2014:192, para. 51-52.

⁷⁴⁶ Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (2014) ECLI:EU:C:2014:192, para. 53.

⁷⁴⁷ Case C-314/12, *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* (2014) ECLI:EU:C:2014:192, para. 62.

Finally, the most recent ruling in the line of the CJEU's case law that affirms the preventive duties of hosting ISSPs is the *Eva Glawischnig-Piesczek*.⁷⁴⁸ This case was a referral from the Austrian Supreme Court and was about the dispute of *Eva Glawischnig-Piesczek*, an internet user against Facebook with regard to the post of defamatory comments online. After careful consideration of the facts, the Court handed down that a hosting ISSP is obliged to prevent the reemergence of content that has already been declared unlawful. This means that in this case, the reposting of defamatory comments should have been removed by Facebook, without notifying the internet user. In this line of reasoning, the CJEU found that "EU law does not preclude a host provider such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared to be illegal."⁷⁴⁹ This means that the existing European Law does not exclude the order of a hosting ISSP to take down information that is stored within its network and whose illegality has already been declared given that the hosting ISSP does not need to take an independent examination to identify the illegal nature of the content.⁷⁵⁰

Therefore, it appears that a duty of care is allowed within the scope of the existing *EU acquis* since the rationale of Article 15 of the ECD is not to prohibit the imposition of all preventive measures in the battle against copyright and trade mark infringements.

Finally, a reason that could offer a counter-argument to those scholars who insist that the wording of Article 15 of the ECD prohibits the imposition of monitoring obligations to hosting ISSPs is the fact that Article 15 of the ECD is outdated. Article 15 of the ECD was drafted in the 1990s.⁷⁵¹ This means that European policymakers had in mind the limited technological capacities of filtering at that time. More specifically, it was around 1999-

⁷⁴⁸ Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (2019) ECLI:EU:C:2019:821.

⁷⁴⁹ Press release No. 128/19 on the Judgement of the C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, 3 October 2019.

⁷⁵⁰ Case C-18/18, *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (2019) ECLI:EU:C:2019:821, para. 55.; see also A. Kuczerawy, "General Monitoring obligations: a new cornerstone of Internet Regulation in the EU?" in KU Leuven Centre for IT and IP Law (ed.), *Rethinking IT and IP Law* (Intersentia 2019) 146 where she criticizes the Advocate's General decision on differentiating between software tools and sophisticated monitoring solutions. As she explains, the former do come in conflict with Article 15 of the ECD while the latter might encroach upon it.

⁷⁵¹ A. Lodder, "Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market" in A.Lodder and A.Murray (eds), *EU Regulation of E-Commerce: A commentary* (2017) 53; The French High Council for Literary and Artistic Property notes that "Although all parties noted that the above activities do not match the assumptions made by the European authorities in 2000 when the legislation was drafted," in The French High Council for Literary and Artistic Property, "Mission to Link Directives 2000/31 and 2001/29 – Report and Proposals" (2016) 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law* is available at <<https://www.jipitec.eu/issues/jipitec-7-2-2016/4436>> last accessed 27 December 2019.

2000 when scientists started developing filtering technology in laboratories around the world. Representative examples are the MIT Butterfly Project and the Information Retrieval and Information Systems in the Netherlands that reveal the development of applications and software on filtering information.⁷⁵² Given the premature stage of all these projects at the time, one might understand that such a nascent filtering technology could not distinguish between illegitimate and lawful material without a high margin of error.⁷⁵³ It is probably for this reason that the European policymakers endorsed Article 15 of the ECD and thus exempted hosting ISSPs from deploying ill-fitted filtering technologies in order to monitor their networks.

Yet, the current digital ecosystem is not similar to the “embryonic state of electronic commerce”⁷⁵⁴ of 2000. This is because, as Frosio notes, “the theoretical and market background against which the intermediary liability debate developed has changed considerably since the first appearance of online intermediaries almost two decades ago.”⁷⁵⁵ This means that hosting ISSPs’ business models, along with the environment in which they operate, have been transformed into a more complex digital ecosystem with myriad online services and risks as well.

So, in contrast to 2000 when the ECD was introduced, in 2019 it cannot be denied that existing filtering technologies are way more advanced and sophisticated.⁷⁵⁶ A telling example is the Content ID system of YouTube.⁷⁵⁷ This is a rights management system

⁷⁵² S. M. Bohte, W.B. Langdon and H. La Poutre, “Report on Current Technology for Information Filtering and User Profiling in Agent-Based Systems, Part I: A Perspective” (2000) 9 is available at < <http://www0.cs.ucl.ac.uk/staff/W.Langdon/TA/reports/profiling.pdf> > last accessed 27 December 2019.

⁷⁵³ Center for Democracy and Technology, “Mixed Messages? The Limits of Automated Social Media Content Analysis” (November 2017) 18 where it is noted that “Among studies using NLP to judge the meaning of text (including hate speech detection and sentiment analysis), the highest accuracy rates reported hover around 80%; in many studies, the highest accuracy rates reported were around 70 to 75%.”⁷³ These accuracy rates may represent impressive advancement in NLP research, but they should also serve as a strong caution to anyone considering the use of such tools in a decision-making process.”

⁷⁵⁴ A. Wyckoff and Al. Colecchia, “Report on the Economic and Social Impact of Electronic Commerce” (1992) 12 where he notes that “the embryonic state of electronic commerce, policies should be crafted with care and with due recognition of its fragile and evolving nature”.

⁷⁵⁵ G. Frosio, “Why keep a dog and bark yourself? From intermediary liability to responsibility” (2017) Centre for International Intellectual Property Studies Research Paper 3.

⁷⁵⁶ M. Schellekens, “Liability of Internet Intermediaries’ a slippery slope?” (2011) 8 SCRIPTed 154 where cites the examples of eBay’s Fraud Engine and VeRo-software; L. Edwards, “With Great Power Comes Great Responsibility? The Rise of Platform Liability” in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 258; In a study conducted by N. Koren and M. Perel it has been found that 25% of video-sharing websites and 10% of image-sharing websites adopt ex-filtering systems in order to identify unauthorized content online in N. Koren and M. Perel, “Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement” (2017) 69 Florida Law Review 181.

⁷⁵⁷ B. Boroughf, “The Next Great YouTube: Improving Content ID to foster creativity, cooperation and fair compensation” (2015) 25 Albany Law Journal Science and Technology 8; L. Helman and G. Parchomovsky,

based on digital fingerprinting technology, and its costs for its development were about US\$60 million.⁷⁵⁸ Without overlooking the errors, such as the lack of detecting works that belong to the public domain,⁷⁵⁹ it is undoubtedly a representative example of high quality filtering technology of our time and consists of a “set of copyright policies and content management tools.”⁷⁶⁰ It has been estimated that its Database includes 50 million works which amount to a period of 600 years’ audio-visual material.⁷⁶¹ Another example can be found in PhotoDNA software developed by Microsoft. It is a digital fingerprint based software or else known as hashes that detect images that relate to terroristic content.⁷⁶² Under the initiative of the EU Commission, a number of hosting ISSPs have already deployed this software in order to cope with terrorism in the digital ecosystem.⁷⁶³

Accordingly, one might conclude that the clash between a duty of care and general monitoring obligations does not exist in practice. This is mainly because the interpretation of Article 15 of the ECD that prohibits any general monitoring obligations is not to be understood as precluding all preventive measures. Such interpretation would be in conflict with *EU acquis*. Further, Article 15 of the ECD seems to be outdated. This is because it was drafted in the 1990s when filtering technology was at its infancy. Nowadays, it is undeniable that filtering technology is more sophisticated and can, with a low margin of error, distinguish unlawful information from legitimate information.

Having discussed the reasons that warrant the imposition of a duty of care on hosting ISSPs drawing evidence from the *EU acquis*, namely from legislation and the line of CJEU case law, this brings us to the next question, namely how such a duty of care should be shaped. This discussion is of seminal importance since however necessary a measure might be, it is the clear articulation of the limits within which this measure can be exercised that would enable the measure to achieve its goals. Otherwise, the imposition

“The best available technology standard” (2011) 111 Columbia Law Review 1209; L. Shinn, “YouTube’s content ID as a case study of private copyright enforcement systems” (2015) AIPLA Quarterly Journal 359.

⁷⁵⁸ S. Jacques, K. Garstka, M. Hviid and J. Street, John, “Automated anti-piracy systems as copyright enforcement mechanism: a need to consider cultural diversity” (2018) 40 European Intellectual Property Review 218.

⁷⁵⁹ Ibid.

⁷⁶⁰ C. Sims and E. Figueira, “YouTube, Google find safe harbour in New York Court” (2010) Communications Lawyer 3.

⁷⁶¹ Footnote 84 in S. Jacques, K. Garstka, M. Hviid and J. Street, John, “Automated anti-piracy systems as copyright enforcement mechanism: a need to consider cultural diversity” (2018) 40 European Intellectual Property Review 218.

⁷⁶² G. Frosio and M. Husovec, “Accountability and Responsibility of Online Intermediaries” in G. Frosio (ed.), The Oxford Handbook of Online Intermediary Liability (Oxford University Press, forthcoming) 10.

⁷⁶³ EU together we protect is available at <https://europa.eu/euprotects/our-safety/awareness-prevention-how-eu-combating-radicalisation-across-europe_en> last accessed 27 December 2019.

of that measure might be biased towards the interests of one of the parties involved and thus fail to reach its full potential. The following section aims to answer which hosting ISSPs shall implement a duty of care towards the circulation of infringing content and fake goods and which the scope of that duty of care shall be.

C. How should a proposed duty of care for hosting ISSPs be shaped?

In this light, this section discusses whether a duty of care shall be treated as a matter of outcome or as a matter of principle as well as how the scope of a duty of care shall be defined based on legal principles, existing trends in case law and academic scholarship.

i. A duty of care as a matter of outcome or as a matter of principle

In the current policy and scholarly landscape, a duty of care is subject to different interpretations. It is either construed as a matter of principle or as a matter of outcome. As a matter of principle, it means that all hosting ISSPs must be assigned with proactive duties towards the circulation of unlawful material within their networks. In contrast, a matter of outcome means that hosting ISSPs are attributed a number of proactive duties according to their business model. For instance, this encompasses their ability to control the usage of the content or the likelihood to attract a number of unlawful contents within their networks.

On one hand, the ascription of a duty of care as a matter of principle might raise concerns as to its implications on the business welfare of certain websites. For instance, for a non-profit hosting ISSP such as Wikipedia,⁷⁶⁴ it would be an excessive burden to adopt a filtering mechanism in order to monitor its platform for copyright infringements. It might be difficult for Wikipedia to develop its in-house technology as YouTube did or excessively costly to license an existing one. Secondly, should the hosting ISSPs not be in compliance with the set of responsibilities, then they will be subject, as elaborated in chapter 3, to primary liability rules.

Further, an additional concern on imposing a duty of care on hosting ISSPs as matter of principle is that a number of hosting ISSPs attract a decimal rate of infringements. In this sense, it would not be fair for these hosting ISSPs to be ascribed a duty of care since their business model does not enable any circulation of infringing material within their

⁷⁶⁴ G. Sartori, "Providers Liability: From the e-commerce directive to the future: In depth analysis for the IMCO Committee" (2017) IMCO Committee 29.

platforms. An illustration of this is Github, an open source platform where software developers use its service so as to share their own codes with other developers.⁷⁶⁵

In the light of the above, it is argued that a duty of care should be imposed as a matter of outcome. This means that a duty of care should not be imposed on each hosting ISSP, rather, it should be imposed on those hosting ISSPs whose business models might also attract unlawful content or to those which have control over the dissemination of material within their networks. This approach, however, is not new. There have been stances in law where different entities were assigned different duties depending on their impact on others' rights.⁷⁶⁶ For instance, Recital 68 of the DSMD excludes from the scope of OCSSPs the non-profit hosting ISSPs such as Wikipedia. This means that while OCSSPs such as Facebook would be assigned to a number of obligations with regard to the dissemination of infringing content online, non-profit hosting ISSPs would be free from complying to those obligations. Accordingly, this will enable those non-profit hosting ISSPs to continue their operation without disruption and thus not deprive internet users of information that is available online.

So, in this respect, with regard to copyright violations, those hosting ISSPs that appear to be the borderline of online infringements or have a certain degree of control towards the usage of content that is disseminated within their networks should have a duty to prevent the emergence of online infringements.

From a normative perspective, this thesis argues that the imposition of a duty of care to hosting ISSPs depending on their business model seems fairer. First of all, without their services, the allegedly infringing material would not have been stored nor transmitted via their networks and thus not reach end-users.⁷⁶⁷ Secondly, in selecting which information is made publicly available, hosting ISSPs exercise editorial discretion.⁷⁶⁸ This means that, like the editors in newspapers, hosting ISSPs are in the pursuit of content that would be

⁷⁶⁵ J. Reda, "Censorship machines are coming: It's time for the free software community to discover its political clout" (Reda's website, 6 April 2018) is available at <<https://juliareda.eu/2018/04/free-software-censorship-machines/>> last accessed 27 December 2019.

⁷⁶⁶ C. Angelopoulos, "EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability capsizes into incoherence" (Kluwer copyright blog, 6 October 2016) is available at <<http://copyrightblog.kluweriplaw.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/>> last accessed 27 December 2019.

⁷⁶⁷ A. Marsoof, *Internet intermediaries and trade mark rights* (Routledge 2019) 106.

⁷⁶⁸ C. Yoo, *The dynamic internet: How technology, users and businesses are transforming the network* (2014) Chapter 9 where Yoo notes that "manage the daily barrage of wanted and unwanted content"; E. Goldman, "Search Engine Bias and the Demise of Search Engine Utopianism" (2006) 8 *Yale Journal of Law and Technology* 189.

more appealing to their subscribers and thus increase the traffic to their sites.⁷⁶⁹ For instance, this was the case of Google which managed to beat its competitors such as AltaVista. What Google did was to deploy an algorithm that offered more effective search listing results to its users than its rivals. In this way, Google became the leader in the search engines market.⁷⁷⁰

What is more, the ascription of a duty of care according to the business model of the hosting ISSP has been supported by a handful of scholars. These scholars argue that since those hosting ISSPs who have more control over the dissemination of the infringing content, or their business model attracts the illicit activity should have a duty of care. For instance, it has been implied in Riordan's taxonomy of hosting ISSPs⁷⁷¹ that it is fairer to attribute a greater responsibility to those hosting ISSPs that are "closest to the end-users". Along similar lines, Marsoof argues that "an intermediary that is proximate to an infringing activity, in that it possesses control over the means of infringement, has a greater responsibility to terminate, if not mitigate, the infringement."⁷⁷² Such a stance has been maintained by Sartor who in his report for the IMCO Committee outlines that "business models and available means should also be considered in determining duties of care."⁷⁷³

What is more, successful examples of duty care can be traced to various sectors. A telling example can be found in trade marks. At policy level, for instance, following the introduction of the "follow the money" approach, a handful of online auction platforms signed a Memorandum of Understanding on the sale of counterfeit goods via the internet.⁷⁷⁴ In this Memorandum, large corporations such as luxury, fashion brands and sporting goods signed agreements with popular hosting ISSPs such as Amazon and Alibaba

⁷⁶⁹ C. Yoo, *The dynamic internet: How technology, users and businesses are transforming the network* (2014) Chapter 9.

⁷⁷⁰ Ibid.

⁷⁷¹ J. Riordan, *The liability of internet intermediaries* (Oxford University Press 2016) 40.

⁷⁷² A. Marsoof, *Internet intermediaries and trade mark rights* (Routledge 2019) 106; see also M.J. Sorensen, "Draft Model Rules on Online Intermediary Platforms" in B. Devolder (ed.), *The Platform Economy: Unravelling the Legal Status of Online Intermediaries* (Intersentia 2019) 181 where Sorensen argues that "there is a big difference between the very active platforms and the more passive platforms. The latter might have less control over the main contract and the users of the platform."

⁷⁷³ G. Sartori, "Providers' Liability: From the e-commerce directive to the future: In depth analysis for the IMCO Committee" (2017) IMCO Committee 29.

⁷⁷⁴ Memorandum of Understanding on the online sale of counterfeit goods (21 June 2016) is available at <file:///C:/Users/krokida/Documents/Signed%20MoU.pdf> > last accessed 27 December 2019.

in order to initiate actions which could terminate the display and circulation of counterfeit goods on their online marketplaces.

Apart from such policy initiatives that encourage cooperation among hosting ISSPs to combat the circulation of counterfeit goods, there are also voluntary private initiatives in order to prevent the dissemination of fake goods within the networks. This can be seen in the case of Amazon which is one of the most popular online auction platforms. After the platform faced an unprecedented number of lawsuits from brand owners due to the counterfeit goods that are circulated within its platform,⁷⁷⁵ Amazon decided to change its policy against fake goods online. This policy is the Brand Registry that enables trade mark owners to register their brand in a Registry.⁷⁷⁶ Once the brand is registered, Amazon may identify instances where the brands are being unlawfully used. For instance, it includes listings with products that use the trade marks in their title that are not correlated with the brands, images that include the logo but belong to products that are not relevant to the brands, and suppliers that display brands' products from countries where the brands do not have promises for manufacturing or distributors.⁷⁷⁷ However, while it may be argued that this policy is primarily aimed at the benefit of the right holders, it has a tantamount positive advantage to the online consumers. This is because, the circulation of counterfeit goods under the guise of lawful brands will be eliminated to a great extent.

Importantly, to allow a massive scale of online infringements might attract bad reputation for the online platform itself and drive off existing as well as potential clients. Further, another crucial point to consider is the loss of trust from other brands within the market. A representative example of such a line of thinking is the Birkenstock decision to withdraw its products from Amazon.⁷⁷⁸ In light of the wide availability of fake copies of Birkenstock

⁷⁷⁵ A. Samuels, "Amazon May Have a Counterfeit Problem: The company is facing multiple lawsuits from brands who say it does not do enough to prevent fakes from being listed on its website" (The Atlantic, 20 April 2018) is available at <<https://www.theatlantic.com/technology/archive/2018/04/amazon-may-have-a-counterfeit-problem/558482/>> last accessed 27 December 2019.

⁷⁷⁶ <https://brandservices.amazon.co.uk/benefits>.

⁷⁷⁷ <https://www.cpcstrategy.com/blog/2018/07/amazon-brand-registry/> states that "Product listings that aren't for your brand and incorrectly use your trademarked terms in their titles.; images that contain your logo, but are for products that don't carry your brand name; sellers shipping products from countries in which you do not manufacture or distribute your brand; product listings being created with your brand name when you have already listed your full product catalogue on Amazon."

⁷⁷⁸ Letter from David Kahan, CEO Birkenstock Americas to Birkenstock Retail Partners (Washington post, 20 July 2017) is available at <https://www.washingtonpost.com/news/business/wp-content/uploads/sites/8/2017/07/Amazon-retailer-letter-7.20.17.pdf?tid=a_inl&noredirect=on> last accessed 27 December 2019.

shoes, the CEO of Birkenstock accused Amazon of being an “accomplice” to the infringements and characterized its functioning as “pathetic”.⁷⁷⁹

With regard to copyright infringements, a representative example can be found in the private voluntary initiative undertaken by YouTube with the use of content identification technology, the Content ID system.⁷⁸⁰ This is because such technology can prevent the emergence of copyright infringement in the first place. Without neglecting its flaws,⁷⁸¹ it is considered a highly sophisticated technology that was developed by YouTube and so far, has been extensively used in order to mitigate the circulation of unauthorized works within its video-exchange platform.⁷⁸² A study conducted on the impact of cultural diversity of automated anti-piracy systems as copyright enforcement mechanisms demonstrates the unique technological infrastructure of the Content ID system along with the efforts to keep it up to date, competitive and efficient.⁷⁸³ In particular, the authors of the study applauded the work of YouTube employees to develop the Content ID system and fix its flaws.⁷⁸⁴

In the light of the above, a duty of care based on the business model of hosting ISSPs seems to be fairer in contrast with the imposition of duty of care as a matter of principle. This is because the ascription of a duty of care to all hosting ISSPs indiscriminately might undermine hosting ISSPs’ business welfare while right holders’ rights are not safeguarded.

⁷⁷⁹ S. Smith, “Birkenstock accuses Amazon of failure to tackle fake replicas”(The Telegraph, 22 December 2017) is available at <<https://www.telegraph.co.uk/business/2017/12/22/birkenstock-accuses-amazon-failure-tackle-fake-replicas/>> last accessed 27 December 2019.

⁷⁸⁰ T. Margoni and M. Perry, “Online intermediary liability and privatised enforcement: the Content ID case” (2016) The Tenth International Conference on Digital Society and eGovernments 36.

⁷⁸¹ P. Tassi, “The Injustice Of The YouTube Content ID Crackdown Reveals Google’s Dark Side” (Forbes, 19 December 2013) is available at <<https://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/#5336a67866c8>> last accessed 27 December 2019; A. Bridy and D. Keller, “U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry” (31 March 2016) 20; T. Ingham, “YouTube’s content ID fails to spot 20%-40% of music recordings” (Music Business Worldwide, 13 July 2016) is available at <<https://www.musicbusinessworldwide.com/youtubes-content-id-fails-spot-20-40/>> last accessed 27 December 2019.

⁷⁸² L. Edwards, “With Great Power Comes Great Responsibility? The Rise of Platform Liability” in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 275 where Edwards notes that “..with the rise of machine learning, automated blocking has begun to look more feasible..”

⁷⁸³ S. Jacques, K. Garstka, M. Hviid and J. Street, “The Impact on Cultural Diversity of Automated Anti-Piracy Systems as Copyright Enforcement Mechanisms: An Empirical Study of YouTube’s Content ID Digital Fingerprinting Technology” (2017) 40 *European Intellectual Property Review* 218-229.

⁷⁸⁴ *Ibid* where the authors note that “it is undeniable that YouTube continues to devote tremendous efforts and resources to improve its Content ID system, altering the algorithm’s operation in relation to specific circumstances. Its customisation of various policies is impressive and offers tailored control of content for its partners across borders. Dedicated engineers work daily to help right-holders control their works online by enabling them to enforce their intellectual property rights on the platform directly, without the need to go to court.”

Conversely, it seems fairer to require from hosting ISSPs whose services might attract online infringements and from hosting ISSPs that exert control over the dissemination of material within their platforms to adopt proactive measures. In this way, not only would right holders' rights be safeguarded, but also hosting ISSPs would be more engaged in the battle of online piracy, which has been aggravated due to the services they offer to the internet users.

ii. The scope of a duty of care

Another aspect of a duty of care to be addressed is the scope. It is important to carve out the scope of a measure since the appropriate articulation of the scope of a measure would enable the measure itself to fulfil its aim without encroaching upon the rights of third parties. To my understanding, the scope of a duty of care for hosting ISSPs addresses the obligation of hosting ISSPs to prevent any illicit activity within their networks. Such prevention is to be achieved either through human review of unlawful content or via the use of advanced technological tools that could identify the infringing content.

a. Trends in case law

At the outset, the concept of prevention of unauthorized content stems from Recital 48 of the ECD that states that hosting ISSPs shall "...prevent certain types of illegal activities."⁷⁸⁵ However, one might wonder how the concept of prevention of illicit activities shall be construed. In this respect, there are three main trends in case law at the European level with regard to the prevention of reemergence of further online infringements. The first trend in case law addresses the need for hosting ISSPs to prevent any further infringements without carving out its boundaries.⁷⁸⁶ A representative example can be found in the landmark judgement of *L'Oreal v ebay*.⁷⁸⁷ In this case, L' Oreal brought legal proceedings against eBay alleging trade mark infringement. After a careful consideration of the facts, the CJEU concluded that eBay shall terminate the trade mark infringements within its platform but must also prevent the further infringements of that kind. This implies that eBay must adopt a proactive role towards the online infringements aiming at terminating and preventing the reappearance of online infringements. Yet, CJEU did not define the scope of preventive measures and thus failed to give a solid answer as

⁷⁸⁵ Recital 48 of the ECD.

⁷⁸⁶ See A. Guadamuz, "Developments in Intermediary Liability" in A. Savin and J. Trzaskowski (eds.) *Research Handbook on EU Internet Law* (Edward Elgar 2014) 312.

⁷⁸⁷ Case C-324/09, *L'Oreal SA V eBay Int'l AG* [2011] E.C.R. I-6011.

to the scope of a duty of care. By contrast, it opened the Pandora's box since many questions with regard to the interpretation of a duty of care have arisen. In this vein, it is plausible to question whether the preventive measures shall address infringements of the same nature by different internet users or infringements of the same nature but from different brands or the infringements committed by the same user. If the latter option is the case, should a duty of care shall cover any kind of intellectual property infringements, from copyright to trade mark infringements committed by the same users. All those questions might lead but to the conclusion that the attribution of a duty of care to hosting ISSPs seems to be based on a nebulous ground.

The second trend in case law has been found in the recently issued judgement of *Glawischnig-Piesczek v Facebook* of 2019.⁷⁸⁸ This line of case law adopts a stance between the wide and narrow interpretation of a duty of care. Whereas the CJEU refrained from carving out the precise boundaries of a duty of care, it gave a hint of the scope of a duty of care by endorsing the concept of the infringement of the same nature.⁷⁸⁹ That said, it concluded that a hosting ISSP must remove information which has previously been declared unlawful as long as the content of the information is the same and without any individual assessment of its illegal nature.⁷⁹⁰ In other words, this implies that the hosting ISSP must prevent illegal content of the same nature must be of the same nature. So, similar to the case of *L'Oreal v ebay*, this case as well does not offer a solid clarification to the scope of duty of care. Indeed, it provides a semi-wide interpretation of the scope within which the preventive measures of hosting ISSPs shall apply.

This conclusion, however, is not a novelty. Indeed, it could find its roots in the *Kerntheorie*⁷⁹¹ which is a peculiarity of the German case law and which concerns the imposition of duty of care on online intermediaries with regard to infringements of the same nature.⁷⁹² This theory has been reiterated in a bedrock of German rulings that examined the disputes of hosting ISSPs and copyright holders for copyright infringements that accrue within their networks and have been committed by internet users. To name a

⁷⁸⁸ Case C-18/18, *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821.

⁷⁸⁹ See for commentary in D. Keller, "Filtering Facebook: introducing dolphins in the net, a new Stanford CIS White Paper – or- why internet uses and EU policymakers should worry about the Advocate General's opinion in *Glawischnig- Piesczek*" (The Center for Internet and Society, 5 September 2019) is available at < <https://cyberlaw.stanford.edu/blog/2019/09/filtering-facebook-introducing-dolphins-net-new-stanford-cis-white-paper-or-why>> last accessed 27 December 2019.

⁷⁹⁰ Case C-18/18, *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para. 55 .

⁷⁹¹ See chapter 2.

⁷⁹² M. Leistner, "Störerhaftung und mittelbare Schutzrechtsverletzung" (2010) GRUR-Beil 1.

few, *Internetversteigerung I*,⁷⁹³ *Internetversteigerung II*⁷⁹⁴ and *Internetversteigerung III*⁷⁹⁵ as well as the *Rapidshare I*⁷⁹⁶ outlined that the hosting ISSPs shall not only delete the infringing links that directed internet users to unauthorized files. Rather, hosting ISSPs are under the obligation to detect and take down any future links of the same kind or, as the Kerntheorie states, of the same nature.⁷⁹⁷

Yet, to impose a duty of care with a wide scope of application or a semi-wide scope of application would imply that hosting ISSPs have the discretion to carve out the boundaries of a duty of care. They would decide the circumstances under which the infringing content shall be removed and thus adopt a stricter or a lighter approach with regard to the take down of content. As a corollary, this understanding might lead to the fragmentation of intellectual property rights' enforcement or might result to collateral censorship of lawful content that has been uploaded by internet users.

The third trend in case law offers a narrow interpretation of the scope of a duty of care. At European level, a representative example of this line of thinking can be found in *Tommy Hilfiger Licensing v Delta Center*.⁷⁹⁸ While this judgement examines the case of an intermediary in the brick and mortar environment, it can be equally applied within the activities of hosting ISSPs who act as intermediaries. In this light, this judgement advances the existing case law with regard to the prevention of infringements at the European level and offers a narrower interpretation of the scope of a duty of care for intermediaries. The case at hand is about a dispute between Hilfiger and the Delta Center company that sublets spaces to traders in the Prague Market Hall. While Delta Center has warned sellers not to sell counterfeit goods, Tommy Hilfiger brand has identified that some sales areas have sold fake copies of the popular brand's products. In this light, Tommy Hilfiger has filed a lawsuit against Delta Center, alleging violation of its trade mark and requesting Delta Center to adopt preventive measures such as for instance the non-conclusion of rental agreements with sellers that have sold fake goods of the brand.⁷⁹⁹ After a careful consideration of the facts, CJEU concluded that preventive measures shall address "new

⁷⁹³ Bundesgerichtshof, *Internetversteigerung I*, 11 March 2004, I ZR 304/01.

⁷⁹⁴ Bundesgerichtshof, *Internetversteigerung II*, 19 April 2007, I ZR 35/04.

⁷⁹⁵ Bundesgerichtshof, *Internetversteigerung III*, 30 April 2008, I ZR 73/05.

⁷⁹⁶ OLG Düsseldorf, *Rapidshare I*, 27 April 2010, I-20 U 166/09.

⁷⁹⁷ J. B. Nordemann, "Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach" (2011) 37 JIPITEC 41-42.

⁷⁹⁸ Case C-494/15, *Tommy Hilfiger Licensing* [2016] ECLI:EU:C:2016:528.

⁷⁹⁹ H. Berendschot, "Summary and analysis of Case C-494/15" in H. Berendschot and K. Janssens (eds.), *Landmark IP decisions of the European Court of Justice 2014-2018* (ELS Belgium 2019) 139-144.

infringements of the same nature by the same market-trader from taking place.”⁸⁰⁰ This means that a duty of care amount to the prevention of the infringement of the same nature by the specific seller. So, transposing this outcome within the context of hosting ISSPs, it means that hosting ISSPs shall prevent the emergence of infringements that have been committed by a specific user whose activities have already been declared illicit.⁸⁰¹

In my opinion, a narrow scope of a duty of care might have merits. For instance, it would offer clarity to the parties involved. As already discussed in the concluding remarks of Part I, legal certainty would make the parties involved aware of the level of enforcement that is required and enable them to adjust their business model to new legal rules. In addition, a clear articulation of the scope of a measure would decrease the chances of abuse of rights of third parties. For example, a precise context, within which the hosting ISSP could exercise its duty of care, would not leave any margin for abuse of the rights of third parties. What is more, any shift from specific obligations to general monitoring obligations would be avoided since the boundaries of specific obligations would be clearly carved out and distinct from general monitoring. Otherwise, a wide scope of a duty of care for hosting ISSPs might conflict with the prohibition of general monitoring obligations, which constitute one of the cornerstones of the development of e-commerce.

b. How to prevent the dissemination of unlawful content or counterfeit goods online.

Another aspect that relates to the scope of a duty of care is the tool that could prevent the dissemination of illegitimate content online. Pursuant to the existing academic scholarship, hosting ISSPs could prevent the emergence of further infringements either through the use of advanced filtering technology or through human review.

On the one hand, the adoption of filtering technology would have merits for right holders and hosting ISSPs. With regard to intellectual property holders, filtering mechanisms would curb to a great extent the dissemination of illegitimate content online. Undoubtedly, to prevent the reemergence of unlawful content might be a panacea for the right holders. Insofar hosting ISSPs are concerned, they would be encouraged to

⁸⁰⁰ Case C-494/15, *Tommy Hilfiger Licensing* [2016] ECLI:EU:C:2016:528, para. 34.

⁸⁰¹ See also C. Angelopoulos, “C-494/15 – Tommy Hilfiger: No Difference between Online and Real World Marketplaces for IP Enforcement” (Kluwer Copyright blog, 10 August 2016) is available at < <http://copyrightblog.kluweriplaw.com/2016/08/10/c-49415-tommy-hilfiger-no-difference-online-real-world-marketplaces-ip-enforcement/> > last accessed 27 December 2019.

develop in-house technology and thus compete their American rivals. Therefore, the adoption of filtering might boost innovation within the Digital Single Market.

Yet, it could be argued that the adoption of filtering mechanisms cannot guarantee the removal of unlawful content. A number of situations have been reported where filtering technology could not differentiate between legitimate and unlawful material. For instance, a video with students protesting for free Tibet was removed from YouTube for the reason that it violated the International Olympic Committee's copyright,⁸⁰² despite the fact it did not infringe the Committee's copyright. Therefore, it appears that the adoption of filtering mechanisms might give rise to censorship and thus encroach upon the right to freedom of expression of internet users.⁸⁰³

However, it should be borne in mind that those challenges to distinguish lawful and illegitimate content should not act as a deterrent for hosting ISSPs from not using advanced filtering technology. Although hosting ISSPs cannot undertake a meticulous fair use assessment,⁸⁰⁴ other criteria can be taken into consideration in assessing whether a material is fair use or not. Such criteria might be, for instance, whether the work has been published already or the size of the portion of the work that has been used.

Moreover, apart from concerns about the efficiency of filtering technology to distinguish lawful and illegitimate content, it could be argued that the imposition of filtering technology might be excessively burdensome for hosting ISPPs. For example, it is estimated that YouTube's technology cost about 60 million dollars to develop. Thus, the imposition of a duty of care might pose serious threats on hosting ISSPs business welfare. This is because filtering can be expensive to develop while the conclusion of licensing agreements for the use of copyrighted works might increase the transaction costs of hosting ISSPs.

⁸⁰² Example in A. Marsoof, "Notice and take down: a copyright perspective" (2015) 5 Queen Mary Journal of Intellectual Property Law 19; S. Seidenberg, "Copyright in the Age of YouTube" (ABA Journal, February 2009) is available at <http://www.abajournal.com/magazine/article/copyright_in_the_age_of_youtube> last accessed 27 December 2019.

⁸⁰³ Center for Democracy and Technology, "Mixed Messages? The Limits of Automated Social Media Content Analysis" (November 2017) 18 where it is stated that "an accuracy rate of 80% means that one out of every five people is treated "wrong" in such decision-making; depending on the process, this would have obvious consequences for civil liberties and human rights."

⁸⁰⁴ Ernesto, "YouTube's copyright protection is a total mess. Can it be fixed?" (Torrentfreak, 22 December 2018) is available at <<https://torrentfreak.com/youtubes-copyright-protection-system-is-a-total-mess-can-it-be-fixed-181222/>> last accessed 24 April 2019.

To circumvent the issue of high transaction costs, the creation of an archive with filtering technologies could be recommended,⁸⁰⁵ managed by the proposed supervisory authority for hosting ISSPs. How this authority could be shaped, as well as its functions, is further elaborated in chapter 6. This authority would have a list of filtering technologies which could be licensed to hosting ISSPs in order to deploy them and prevent the online infringements within their networks.⁸⁰⁶ In this way, hosting ISSPs would comply with their duty of care and any liability would be excluded.

Finally, another opponent of filtering might argue that, with filtering a process of data without lawful basis takes place. This argument was included in the *Scarlet v Netlog* case⁸⁰⁷ where the CJEU handed down that filtering would pose serious threats on users' personal data. Without explaining how filtering would violate users' data, the Court noted that "requiring installation of the contested filtering system would involve the identification, systematic analysis and processing of information connected with the profiles created on the social network by its users."⁸⁰⁸ Given that information is personal data, any systematic analysis without users' consent might encroach upon users' right to privacy as enshrined in Article 8 of the European Charter of Fundamental Rights. However, this argument was overturned in 2019. This is because as per the GDPR,⁸⁰⁹ which is in force since March 2018, any personal data processing must fulfil a set of principles. Such principles are lawfulness, transparency, accountability and data minimization. Yet, one might argue that the use of filtering would be in conflict with Article 22 of the GDPR that states that "the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."⁸¹⁰ However, this obstacle can be overcome if the internet user gives her consent to the process of her data. This option, as Frosio notes, could be included in the terms of use of hosting ISSPs.⁸¹¹ In

⁸⁰⁵ K. Garstka, "Looking above and beyond the blunt expectation: specified request as the recommended approach to intermediary liability in cyberspace" (2016) 7 European Journal of Law and Technology para. 3.

⁸⁰⁶ Ibid.

⁸⁰⁷ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

⁸⁰⁸ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959, para. 45.

⁸⁰⁹ The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years is available at <<https://eugdpr.org/>> last accessed 27 December 2019.

⁸¹⁰ S. Kulk, *Internet Intermediaries and Copyright Law: EU and US perspective* (Kluwer Law International 2019).

⁸¹¹ Frosio G, "Algorithmic enforcement online" in Paul Torremans (ed.), *Intellectual Property and Human Rights* (4th edition, Kluwer Law International forthcoming 2020) 17.

this regard, given that hosting ISSPs abide by these rules, any unlawful process of personal data would be eliminated.

On the other hand, a duty of care of hosting ISSPs could amount to the human review of the content that is disseminated within the networks. Human review could distinguish between the legitimate and illegitimate nature of content. In this respect, in Germany according to the Network Enforcement Law that combats hate speech online, Facebook hired 800 employees who, in parallel with algorithmic review, review videos that might include hate speech and remove them.⁸¹²

However, this can be tricky for hosting ISSPs, especially the ones with high traffic since a high number of employees are required to be hired. In addition, such employees must be skilled in order to distinguish between legitimate and illegitimate content online. Otherwise, a margin of error might occur and lawful content would be removed.

Nonetheless, human review might not be equal to algorithmic review. For instance, there have been instances where human review has performed less efficiently than algorithmic review. A telling example can be found in the case of Garry Kasparov where a computer software managed to beat the World Chess Champion.⁸¹³ In this case, computer programmers developed a software, which is known as Deep Blue and could predict 200,000,000 moves in chess. However, as already explained, in some instances a human review is warranted,⁸¹⁴ such as copyright infringements. To judge whether a copyright infringement has occurred, an understanding of its context is deemed necessary.⁸¹⁵

In the light of the above, this thesis argues that a duty of care shall address either the use of technological tools or human review without excluding the possibility to combine them. This means that both options might be used separately but also complementary. However, it shall be up to the hosting ISSPs as to which option they would adopt according to their business model. This is because filtering-based technology might prove cost-

⁸¹² ARTICLE 19, "Germany: Responding to 'hate speech: Country report" (2018) is available at <<https://www.article19.org/wp-content/uploads/2018/07/Germany-Responding-to-%E2%80%98hate-speech%E2%80%99-v3-WEB.pdf>> last accessed 27 December 2019.

⁸¹³ M.R Anderson, "Twenty years on from Deep Blue vs Kasparov: how a chess match started the big data revolution" (The Conversation, 11 May 2017) is available at <<https://theconversation.com/twenty-years-on-from-deep-blue-vs-kasparov-how-a-chess-match-started-the-big-data-revolution-76882>> last accessed on 27 December 2019.

⁸¹⁴ D. Citron Keats and B. Wittes, "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity" (2017) University of Maryland Legal Studies 17.

⁸¹⁵ This means where the work can be considered as fair use or not.

efficient for those hosting ISSPs that have resources while for other smaller hosting ISSPs this would be an obstacle for their continuous operation since they would be deprived of the appropriate resources to develop such tools or at least license ones. On the other hand, the review by humans of content that is disseminated could eliminate potential errors that technological tools might perform while at the same time it might prove non-efficient since a high number of employees shall be employed and trained. Last but not least, both options could be used by hosting ISSPs. For instance, the use of technological tools would faster identify the infringing content whereas in cases where the hosting ISSPs could not reach a decision on the illegal nature of the content a human review of the allegedly infringing content shall be provided. In case, it is worth to stress that the adoption of filtering mechanisms must fall into the narrow scope of a duty of care. This is because any extension beyond the scope of a duty of care might pose risks to fundamental rights of internet users and thus lead to censorship. For instance, a wide scope of duty of care might take down lawful content since specific conditions under which content could be removed are not carved out. Therefore, following this recommendation and due to the pivotal role that hosting ISSPs play in the digital ecosystem, as already discussed in Section II of this chapter, hosting ISSPs would be able to fulfil their duty of care and combat online piracy.

To sum up, it was concluded that a duty of care shall be imposed on hosting ISSPs as a matter of outcome. This means that it shall be attributed to those hosting ISSPs that attract online infringements and not indiscriminately to ISSPs that provide hosting services to its users. As Sartori has pointed out, a duty of care shall be assigned after taking into consideration the business model of the hosting ISSP.⁸¹⁶ Further, it was concluded that a narrow scope of a duty of care would have merits over a wide scope of a duty of care. This is because a narrow scope of a duty of care would not only achieve its aim, which is to decrease the online piracy but also would have more possibilities to strike a fair balance between the interests of the parties involved, namely hosting ISSPs, right holders and internet users. Finally, how duty of care would be fulfilled shall be contingent to the hosting ISSPs. This means that they could either deploy filtering-based

⁸¹⁶ G. Sartori, "Providers Liability: From the e-commerce directive to the future: In depth analysis for the IMCO Committee" (2017) IMCO Committee 29 is available at [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA\(2017\)614179_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf) last accessed 27 December 2019.

technological tools or resort to human review of the content and goods that are circulated online.

Yet, whereas a duty of care shall be imposed to hosting ISSPs in accordance with their business model and shall entail a narrow scope with regard to the reemergence of infringing content, it could be argued that it might assume knowledge of the illicit activity from the part of the hosting ISSP or interfere to fundamental rights of internet users such as the right to information. For this reason, a duty of care cannot be introduced without limitations. Those limitations aim at safeguarding the rights of hosting ISSPs, to which a duty of care has been assigned, as well as the rights of third parties, such as internet users, without cancelling the positive effect of a duty of care of hosting ISSPs in the battle against online piracy.

D. Limitations upon a proposed duty of care

This section endorses certain limitations for a duty of care on hosting ISSPs in order to safeguard the interests of hosting ISSPs and internet users/ consumers. With regard to hosting ISSPs, drawing parallels with the US legal system, a Good Samaritan clause is suggested with the aim to safeguard the fundamental right of hosting ISSPs to conduct business. A transparency obligation for hosting ISSPs is also suggested in order to guarantee the fundamental right of users to freedom of expression.

i. Hosting ISSPs' perspective: endorsing a "Good Samaritan clause"

As concluded from the discussion in Section IV. B. i, ii, iii, a duty of care is allowed under the *EU acquis* and it is its precise articulation that would enhance the completion of its goals, namely the combat of online infringements online. However, it could be argued that the introduction of a duty of care might endanger the business model of hosting ISSPs. Indeed, despite the great benefits for right holders, a duty of care might run the risk of threatening the operation of the business welfare of hosting ISSPs. This is because one might argue that the use of filtering mechanisms or human review of content that is disseminated online might amount to knowledge of hosting ISSPs of any allegedly infringing content. In this way, a knowledge of hosting ISSPs about illicit activities could be presumed in case copyright holders or brand owners identify infringing content or counterfeit goods online. As Stalla-Bourdillon pointed out, if the hosting ISSPs remove in good faith infringing content by deploying proactive means, then hosting ISSPs shall not

be held liable if infringing content has been found in their networks.⁸¹⁷ This means that since hosting ISSPs take the initiative and deploy the appropriate mechanisms, they should be given liability immunity due to their direct involvement in the battle against online piracy.

This understanding has been mirrored in a handful of court rulings where the commentators observed that a duty of care might result in knowledge or awareness of the illegal activities taking place in their networks. For instance, in the case of *Gisele Spiegel v YouTube*,⁸¹⁸ YouTube voluntarily adopted a filtering mechanism in order to detect unauthorized works. Yet, it was this act of deploying filtering identification technology that led the German Supreme Court to conclude that YouTube had actual knowledge of the infringing acts due to the availability of filtering mechanisms.⁸¹⁹

Similar reflections have been raised in light of the *L'Oreal v eBay* case.⁸²⁰ This is because, as the Court explicitly pointed out, there are instances where hosting ISSPs could be aware of illicit activity after deploying mechanisms in order to identify any wrongdoing within its platform on a voluntary basis.⁸²¹ This understanding means that in order to impose liability rules on hosting ISSPs, the court could take into consideration any proactive action on behalf of the hosting ISSPs. Such action could amount to knowledge or awareness of the unlawful activity.⁸²² Therefore, as Van Eecke pointed out “a hosting provider would be disincentivized from voluntarily keeping an eye on some parts of its platform.”⁸²³ This implies that hosting ISSPs would not be motivated to deploy the appropriate mechanisms in order to prevent the reappearance of online infringements since any application of filtering-based technology would deprive them of their main defense, which is the lack of knowledge of the illicit activity.

⁸¹⁷ S. Stalla-Bourdillon, “On Delfi v Estonia... Is it time to adopt a good-Samaritan style exemption?” (Inform’s Blog, 24 June 2015) is available at <<https://inform.org/2015/06/24/on-delfi-v-estonia-is-it-time-to-adopt-a-good-samaritan-style-exemption-sophie-stalla-bourdillon/>> last accessed 27 December 2019.

⁸¹⁸ Landesgericht Hamburg, 5 March 2010, ref. no. 324 O 565/08.

⁸¹⁹ Landesgericht Hamburg, 5 March 2010, ref. no. 324 O 565/08.

⁸²⁰ Case C-324/09, *L’Oreal SA V eBay Int’l AG* [2011] E.C.R. I-6011.

⁸²¹ Case C-324/09, *L’Oreal SA V eBay Int’l AG* [2011] E.C.R. I-6011, para. 122.

⁸²² See also R. Harvey, “Host providers may be subject to obligations resulting in content removal on a worldwide basis, says AG Szpunar” (2019) 14 Journal of Intellectual Property Law & Practice 836.

⁸²³ P. Van Eecke, “Online service providers and liability: A plea for a balanced approach” (2011) 48 Common Market Law Review 1483-1484.

However, to deprive hosting ISSPs from adopting the defense of knowledge, as the Advocate General pointed out, seems “surreal”.⁸²⁴ This is because it is beyond the current understanding of hosting ISSPs’ policy framework and the reasons that justified the imposition of the secondary liability regime. Such liability provisions aimed to further develop innovation and the entrance of new digital players in the market. As Edwards acutely points out “future innovation which brought with it prosperity required a feeling of safety against future liability.”⁸²⁵ Otherwise, liability rules would deter new hosting ISSPs from actively engaging within the Digital Single Market or leading the current ones to bankruptcy, as happened in the Napster case.⁸²⁶

Finally, such concerns may be evoked in cases of non-commercial hosting ISSPs. A representative example of such thinking is Wikipedia.⁸²⁷ In this case, Wikipedia hired employees to monitor the content that was uploaded online so as to verify the validity of the information that is edited along with the accuracy of such information. Should the employees notice any unlawful information, they remove it from the online platform. However, such removal implies a control over the content.⁸²⁸ This understanding could be taken into consideration by the courts and could subsequently lead to the imposition of damages on Wikipedia. This outcome could either shut down Wikipedia’s website or non-incentivize Wikipedia to monitor its website for unlawful information.⁸²⁹

In the light of the above criticism, many commentators have argued in favour of a Good Samaritan privilege.⁸³⁰ For instance, in the context of proposing amendments on the EU

⁸²⁴ Case C-324/09, *L’Oréal v eBay International*, Opinion of Advocate General Jääskinen (2011) E.C.R. I-6011, para. 146 where he noted “I would find it surreal that if eBay intervenes and guides the contents of listings in its system with various technical means, it would by that fact be deprived of the protection of Article 14 regarding storage of information uploaded by the users.”

⁸²⁵ L. Edwards, “With Great Power Comes Great Responsibility? The Rise of Platform Liability” in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 260.

⁸²⁶ J. Koranteg, “Napster considers bankruptcy” (2002) 20 *Music and Media* 1. It has been noted that due to expensive ongoing copyright litigation pursued by major Music Industry labels against Napster, Napster had to file for bankruptcy.

⁸²⁷ P. Van Eecke, “Online service providers and liability: A plea for a balanced approach” (2011) 48 *Common Market Law Review* 1483-1484.

⁸²⁸ *Ibid.*

⁸²⁹ *Ibid.*

⁸³⁰ S. Stalla-Bourdillon, “On Delfi v Estonia... Is it time to adopt a good-Samaritan style exemption?” (Inform’s Blog, 24 June 2-15) is available at <<https://peepbeep.wordpress.com/2015/06/19/on-delfi-v-estonia-is-it-time-to-adopt-a-good-samaritan-style-exemption/>> last accessed 27 December 2019; M. Leistner, “Copyright law on the internet in need of reform: hyperlinks, online platforms and aggregators” (2017) 12 *Journal of Intellectual Property Law & Practice* 136–149; A. Kuczerway, “General Monitoring obligations: a new cornerstone of Internet Regulation in the EU?” in KU Leuven Centre for IT and IP Law (ed.), *Rethinking IT and IP Law* (Intersentia 2019) 142 where she outlines the negative implications resulting from the lack of a Good Samaritan clause.

Commission's Proposal for the DSMD, Angelopoulos noted that if hosting ISSP are required to take down material under their own initiatives, a 'Good Samaritan' protection for them shall be granted.⁸³¹ In similar fashion, a number of European policy documents lean in favor of a 'Good Samaritan' clause. To name a few, according to EU Commission Public Consultation on e-commerce, stakeholders and in particular hosting ISSPs argue in favour of the introduction of a Good Samaritan clause.⁸³² This understanding, as the EU Commission's staff working document explains, is based on Recital 40 of the ECD that notes that "the provisions of this Directive relating to liability should not preclude the development and effective operation, by the different interested parties, of technical systems of protection and identification methods and of technical surveillance instruments made possible by digital technology within the limits of Directives 95/46/EC and 97/66/EC."⁸³³ Therefore, this means that the development of technology that filters the online infringements should not be correlated with the imposition of liability rules to hosting ISSPs.

The concept of the Good Samaritan privilege has its roots in the US jurisdiction and more precisely is enshrined in Section 230 C 1 and 2 of the CDA Act.⁸³⁴ It states that a hosting ISSP shall not be liable for taking actions in good faith aiming to terminate the circulation of infringing content online or the reappearance of infringing content online.⁸³⁵ The rationale for imposing such a privilege⁸³⁶ stems from the case of *Stratton- Oakmont v. Prodigy*.⁸³⁷ This case addressed the dispute between Prodigy, a computer network and Stratton and Oakmont for libel comments that were posted on their network. The Supreme court held that Prodigy exercised editorial control over the material the users

⁸³¹ C. Angelopoulos, "On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the DSM" (2017) 11.

⁸³² EU Commission, "Public Consultation on the future of the electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce" (2000) 11.

⁸³³ Recital 40 of the ECD.

⁸³⁴ Communications Decency Act, 47 U.S.C. §230.

⁸³⁵ Electronic Frontier Foundation, "Section 230 of the Communications Decency Act: 47 U.S.C. § 230, a Provision of the Communication Decency Act" is available at <<https://www.eff.org/issues/cda230>> last accessed 27 December 2019; Section 230 C 1 and 2 of the CDA Act states that " "(2) Civil liability. 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; or (B) 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)."

⁸³⁶ A. Kuczerawy, "The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?" (24 April 2018) is available at <<https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/>> last accessed 27 December 2019.

⁸³⁷ US Supreme Court, *Stratton Oakmont Inc and Daniel Porush v. Prodigy Services Company*, 24 May 1995 is available at <<https://h2o.law.harvard.edu/cases/4540>> last accessed 27 December 2019.

had posted since it uses monitoring systems to detect unlawful information and thus remove it. In this sense, it exercises a type of censorship over the information that is transmitted online.⁸³⁸ Interestingly, whereas Prodigy took action on its own initiative and deleted the offensive material, the court found Prodigy liable for the defamatory comments under the reasoning that it did not remove all the defamatory comments, which had been posted on its bulletin board.⁸³⁹

In this regard, at European level, the introduction of a Good Samaritan clause may prove to counter-balance the negative criticism for deploying filtering technologies in order to curb online infringements. From the perspective of hosting ISSPs' business model, hosting ISSPs would deploy filtering mechanisms so as to terminate infringements online but without considering such proactive actions as equal to knowledge or awareness of the infringing material. Without any Good Samaritan clause, such proactive actions could make hosting ISSPs aware of the illicit activity and thus lead to their liability. This is because hosting ISSPs could no longer resort to the defense of knowledge which is a requisite of secondary liability regime. In contrast, a Good Samaritan clause may safeguard hosting ISSPs from being held liable under the reasoning that they knew the existence of the infringing material.

ii. What about internet users' perspective?

Apart from the introduction of a Good Samaritan clause in order to safeguard hosting ISSPs' business model, it is also important to establish some safeguards for users in order to achieve a better balance between the different interests at stake. This is because proactive measures, as elaborated in Section IV B. might pose risks to internet users' fundamental right to freedom of expression.⁸⁴⁰ Such safeguards should be explicitly included in the new regulatory framework and not be left to the discretion of hosting ISSPs.

⁸³⁸ US Supreme Court, *Stratton Oakmont Inc and Daniel Porush v. Prodigy Services Company*, 24 May 1995 is available at <<https://h2o.law.harvard.edu/cases/4540>> last accessed 27 December 2019.

⁸³⁹ A. Kuczerawy "The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?" (24 April 2018) is available at: <<https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/>> last accessed 27 December 2019.

⁸⁴⁰ See also J. Van Hoboken, "Hosting intermediary services and illegal content online: an analysis of the scope of article 14 ECD in light of the developments in the online service landscape" (2018) 27 is available at <<https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en>> last accessed 27 December 2019.

Such safeguards are about a statutory obligation for transparency which should be imposed on hosting ISSPs. This transparency obligation would enable users and consumers to be aware of the management policies on content removal and the actions of hosting ISSPs against the circulation of fake goods within their platforms. An analysis of this transparency obligation is undertaken in the following chapter.

V. Conclusion

This chapter hitherto has critically discussed the establishment of a responsibility framework for hosting ISSPs based on co-regulation. It did so by analysing the normative considerations of this framework. It was argued that a responsibility framework is warranted due to the new role of hosting ISSPs. Although at the beginning of e-commerce hosting ISSPs have been considered passive entities, they are now given an active role. That new role depicts hosting ISSPs as enforcers of intellectual property rights, adjudicators of intellectual property rights and implementers of public policies.

What is more, it was noted that a responsibility framework for hosting ISSPs could rest on a strong theoretical underpinning. Drawing insights from Internet regulation theories, I found that the theories of Reidenberg and Lessig argue that governmental authorities could influence users' online via regulating the hosting ISSPs' activities, either by the attribution of a set of responsibilities to hosting ISSPs or by holding them accountable to a hosting ISSP supervisory authority. Therefore, a regime where hosting ISSPs would be assigned to a set of responsibilities and they would be accountable to a hosting ISSP supervisory authority could be justified.

Having discussed the normative and theoretical considerations of the proposed regulatory framework for hosting ISSPs, this chapter also looked at one of the constituents of this responsibility framework which is the imposition of a duty of care to hosting ISSPs. A duty of care is not a novelty since it has already been exemplified at policy and judicial level. However, as my findings indicate, to which hosting ISSPs shall be assigned and its scope are not been set up. For this reason, it was noted that it seems fairer to assign a duty of care to those hosting ISSPs that are closer to the infringements or at least they can control their dissemination. In addition, it was noted that the scope of the duty of care shall be narrow. Although there are three lines of case law with regard to the scope of duty of care, in my opinion the narrow scope of a duty of care shall be preferred. This is because a narrow scope would contribute to legal certainty so that hosting ISSPs would

be aware of the level of enforcement that is needed and enable them to comply their business model with the new legislative requirements. Otherwise, a wide scope of a duty of care would leave many decisions to the discretion of hosting ISSPs and thus might lead to excessive removal of content that could be lawful as well.

However, the ascription of a duty of care shall have limitations in order to avoid any interference of a duty of care with the business model of hosting ISSPs and the abuse of third parties' rights. So, with regard to the limitations upon a duty of care in order to safeguard the business model of hosting ISSPs, I looked at the Good Samaritan principle in the US legal system. This principle would be beneficial since from the perspective of hosting ISSPs' business model such proactive actions would not be considered as equal to knowledge or awareness of the infringing material. In contrast, if there is not a Good Samaritan clause, such proactive actions that are entailed in the duty of care could amount to knowledge and thus would lead to the liability of hosting ISSPs. With regard to the limitations of a duty of care in order to protect the rights of internet users, I argue that a transparency obligation, a thorough analysis of which follows in chapter 5, would be necessary. By disclosing more information about the operation of hosting ISSPs relating to the removal of content and goods online, the right of internet users to freedom of expression would be safeguarded as well as the confidence of consumers towards online platforms and online sales in general would be increased.

Chapter 5: Endorsing a transparency obligation for hosting ISSPs

I. Introduction

As previously discussed in chapter 4, the proposed imposition of duty of care might offer a higher degree of protection to right holders while at the same time with the appropriate safeguards would enable hosting ISSPs to sustain their business welfare. This duty of care that hosting ISSPs would have towards the dissemination of infringing material within their networks might include filtering-based technological tools. However, as this chapter discusses, the use of filtering technology which is based on automated algorithmic decision-making procedures has been subject to severe criticism.

On the one hand, scholars characterize algorithms as “fundamental enablers in modern society”⁸⁴¹ or “sovereign over important aspects of individual lives.”⁸⁴² By gathering news in one single website through aggregation applications or mitigating the dissemination of illegal material via filtering or spam applications, algorithms become important constituents of modern society. On the other hand, others argue that algorithms are “black boxes”.⁸⁴³ This is because their internal structure is obscure to users.⁸⁴⁴ It is this obscure nature of algorithms that gives rise to mounting concerns over their operation. For instance, it could be asked under what conditions hosting ISSPs remove material from their platforms, how they process the notifications for illegal material, or to what extent their actions might amount to censorship.⁸⁴⁵

⁸⁴¹ European Commission’s Directorate-General for Communications Networks. Content and Technology, “algo: aware; Raising awareness on algorithms” (December 2018).

⁸⁴² D. K. Citron and F. Pasquale, “The Scored Society: Due Process for Automated Predictions” (2014) 89 Washington Law Review 19.

⁸⁴³ F. Pasquale, *Black Box Society: The secret algorithms that control money and information* (2015) 9; S. Stalla-Bourdillon, “Online Monitoring, Filtering, Blocking... What is the Difference? Where to Draw the Line?” (2013) Southampton Research Paper 19.

⁸⁴⁴ P.J. Dittrich, “Online Platforms and how to regulate them: an EU overview” (2018) Policy Paper No. 227 5; J. Zerilli, A. Knott, J. Maclaurin and C. Gavaghan, “Transparency in Algorithmic and Human Decision-Making: Is there a double standard?” (2018) 9 Philosophy and Technology 2 where they noted that “the worry seems to be that because deep learning systems arrive at their decisions unaided, i.e. in a manner that is not specified in advance, it is not possible to interpret the system’s internal processes except only approximately and imperfectly”.

⁸⁴⁵ M. Perel (Filmar) and N. Elkin-Koren, “Accountability in Algorithmic Copyright Enforcement” (2016) 19 Stanford Technology Law Review 473 (2016) 530; EDRI “Leaked document: Does the EU Commission really plan to tackle illegal content online?” (21 September 2017) is available at <<https://edri.org/leaked-document-does-the-eu-commission-actually-aim-to-tackle-illegal-content-online/>> last accessed 28 December 2019.

Against this background, the EU Communication on online platforms of 2016 found that the majority of the respondents to the public consultation on hosting ISSPs “called for greater transparency on platform content policy.”⁸⁴⁶ This means that internet users demand more information on the procedures that hosting ISSPs adopt in order to remove material from their networks. In a similar fashion, the importance of a transparency obligation has been reinforced in the behavioural study on transparency on online platforms of 2018.⁸⁴⁷ In particular, it was concluded that transparency is of great benefit to both online consumers and hosting ISSPs.

Therefore, this chapter argues that the introduction of a transparency obligation at European level is necessary. In the context of a responsibility framework, as discussed in chapter 4, hosting ISSPs shall have a transparency obligation. In this regard, this chapter firstly examines the current European and national framework with regard to a transparency obligation. Following this, it examines the normative considerations of transparency so as to identify which goals a transparency obligation aims to pursue. Having explored the need for a transparency obligation, the narrative moves to the interpretation of the proposed transparency obligation. Undoubtedly, while the introduction of transparency mainly safeguards users’ rights, the interests of hosting ISSPs is also taken into consideration. This is because, however useful a transparency obligation might be, the outcome may be detrimental to hosting ISSPs if the limits of a transparency obligation are not clearly articulated. This is of special concern for this research, since its main aim is to maintain an equilibrium between the different interests at stake. For this reason, the last part of this chapter examines how transparency should be construed so as to accommodate users’ interests without subordinating hosting ISSPs’ rights.

II. Current initiatives for a transparency obligation and trends

This section addresses the initiatives and trends for a transparency obligation for hosting ISSPs undertaken at European level as well as at national level within the EU member states.

⁸⁴⁶ EU Commission, “Online platforms and the DSM opportunities and challenges for Europe” (2016) 7.

⁸⁴⁷ EU Commission, “Behavioural Study on the transparency of online platforms- Executive summary” (2018) 6.

A. EU initiatives for a transparency obligation

To address the opacity of hosting ISSPs' operation with regard to the management of online content, initiatives aiming at establishing a transparency obligation have emerged at European level as well as at a handful of national jurisdictions. However, as illustrated below, it seems that all these initiatives are insufficient.

A transparency obligation for hosting ISSPs is not included neither in the ECD nor in the DSM. Instead at European level, suggestions to set out a transparency obligation for hosting ISSPs are included in non-binding documents. These documents concern the battle against unlawful content that is disseminated online, including instances of unauthorized content within online platforms. For instance, in 2017 the EU Commission published a Communication outlining the importance of a transparency obligation in the Digital Single Market.⁸⁴⁸ This transparency obligation concerns the publication of transparency reports on a voluntary basis. In particular, it notes that transparency reports shall encompass a disclosure of information on content policy and the notices for removals hosting ISSPs receive as well as the timeframe within which they respond. In this way, the Communication invites hosting ISSPs to adopt more transparent policies for their internet users while at the same time it attempts to mitigate any abuse of users' rights resulted from filtering mechanisms. As already discussed in chapter 3, such abuse might include the violation of information rights and freedom of expression of internet users.

By the same token, the EU Commission's Recommendation of 1 March 2018, discussing measures to effectively tackle illegal content online, notes in paragraph 20 that:⁸⁴⁹

“In order to ensure transparency and fairness and to avoid the unintended removal of content which is not illegal content, content providers should, as a matter of principle, be informed of the decision to remove or disable access to the content stored at their request and be given the possibility to contest the decision through a counter-notice..”

This recommendation is about the notification to users for the removal of their videos and the availability of counter-notification procedures in order to appeal the unreasonable

⁸⁴⁸ EU Commission, “Tackling illegal content online: Towards an enhanced responsibility of online platforms” COM (2017) 555 final 16.

⁸⁴⁹ EU Commission, “Recommendation of 1.3.2018 on measures to effectively tackle illegal content online” COM (2018) 1177 final 5.

removal. In doing so, users who may not have observed that their uploaded video has been removed will be able to submit a counter-notification. Hence, users' rights, such as the right to effective trial as enshrined in Article 47 of the EU Charter of Fundamental Rights, would be safeguarded.

In line with this, paragraph 23 of the EU Commission's Recommendation notes that:

"In order to better assess the effectiveness of notice-and-action mechanisms and other activities of hosting service providers in respect of content considered to be illegal content and to ensure accountability, there should be transparency vis-à-vis the general public. Hosting service providers should therefore regularly publish reports about those mechanisms and other activities, which should be sufficiently complete and detailed to allow for an adequate insight."⁸⁵⁰

This recommendation addresses the need for transparency reports to be published by hosting ISSPs. Such reports should include information on hosting ISSPs' content policies as well as information on where they store content that has been removed from their platforms. In this way, hosting ISSPs' practices would be under public scrutiny, thus eliminating risks of misconduct from their part.

Along similar lines, following the EU Commission's Recommendation guidelines, the Council of Europe published a Recommendation on the role and the responsibilities of hosting ISSPs.⁸⁵¹ In particular, it invites hosting ISSPs to adopt clear and transparent information regarding their operation. It notes that "[i]nternet intermediaries should clearly and transparently provide meaningful public information about the operation of automated data processing techniques in the course of their activities."⁸⁵² At the same time, the Recommendation encourages hosting ISSPs to publish transparency reports every year and include all the requests for content removals. Such requests for removing content online may be sent from governmental authorities or individual users.⁸⁵³

⁸⁵⁰ EU Commission, "Recommendation of 1.3.2018 on measures to effectively tackle illegal content online" COM (2018) 1177 final 6.

⁸⁵¹ Committee of Ministers, "Recommendation of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries" CM/Rec (2018) 1 is available at <<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680790e14>> last accessed 27 December 2019.

⁸⁵² Ibid.

⁸⁵³ Ibid.

In light of the above, it is possible to observe that a transparency obligation with regard to the removal of copyright infringing contents exists at European level. However, its soft law approach is not legally binding for hosting ISSPs. Therefore, a margin of manoeuvre is entirely left to the discretion of hosting ISSPs.

However, apart from the recommendations for a transparency obligation at European level, a handful of European national jurisdictions have endorsed legislative pieces towards a transparency obligation. Yet, on closer inspection of European national approaches, it appears that the landscape of initiatives for a transparency obligation differs from country to country. These divergent policies might trigger legal uncertainty among the parties involved, namely hosting ISSPs, internet users and right holders.

B. National initiatives for a transparency obligation

Firstly, it can be observed that across European member states, any initiatives for transparency do not address copyright or trade mark violations in the digital world. In contrast, they either explicitly touch upon transparency of hosting ISSPs with regard to the removal of illegal content, such as hate speech or fake news, or solely focus on imposing a transparency obligation on algorithmic decision-making procedures. This understanding was exemplified in Germany where the Network Enforcement Law came into force in 2018 and addressed issues relating to the removal of offensive comments from hosting ISSPs within 24 hours.⁸⁵⁴ In addition, this imposed a transparency obligation to hosting ISSPs; forcing them to publish transparency reports twice a year and reveal the procedures to remove the infringing content and how the users have appealed the decisions.⁸⁵⁵ In similar fashion, the UK Government has published in April 2019 a White Paper on online harms which includes a number recommendations such as the issue of transparency reports by ISSPs annually. These annual transparency reports include the practices that ISSPs deploy in order to delete offensive or hate speech content online.⁸⁵⁶ Further, other countries have introduced a transparency obligation for algorithmic decision-making processes. A telling example can be found in Estonia where the government recently passed a law about the algorithmic-liability of Artificial Intelligence

⁸⁵⁴ ARTICLE 19 Working Party, "Germany: The Act to Improve Enforcement of the Law in Social Networks" (August 2017) is available at <<https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf>> last accessed 27 December 2019.

⁸⁵⁵ P. Oltermann, "Tough new German law puts tech firms and free speech in spotlight" (The Guardian, 5 January 2018) is available at <<https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight>> last accessed 27 December 2019.

⁸⁵⁶ HM Government, "Online Harms (White Paper)" (April 2019) 7, 57.

schemes.⁸⁵⁷ This new law aims to clarify potential liability from algorithmic decision-making and addresses a wide range of stakeholders, such as private sectors, individuals and public authorities, which could make use of algorithms in the course of their operation.

Secondly, other initiatives across European borders impose a transparency obligation in the digital world without limiting the scope of applying a transparency obligation to hosting ISSPs. This means that a transparency obligation is placed in order to enhance Digital Growth from a broader perspective. For example, the Denmark Government published a strategy that provides several guidelines to Danish corporations that deal with digital services.⁸⁵⁸ In this strategy, the role of transparency as one of the most important requirements for online growth and innovation is outlined. In a similar fashion, in the Netherlands, the recently published Dutch Digitalization Strategy stresses the need for transparency in the digital services.⁸⁵⁹ In particular, it notes that a disclosure of information on supplier's identity for goods online is recommended and stresses the need for transparency in algorithmic decision-making process in the digital world.⁸⁶⁰

Thirdly, among these national jurisdictions, it seems that a number of member states limit their initiatives for a transparency obligation at policy level while others take a step further and include it in their legislation. For instance, the Italian government has issued a policy document regarding the challenges of algorithmic decision-making process for citizens. In particular, this document stresses any risks that stem from algorithms and concludes with suggesting potential safeguards.⁸⁶¹ In addition, in the UK, there is an initiative to establish a Center for Data Ethics and Innovation whose main aim is to assist regulators in order to identify ethical issues that arise from the use of algorithms, cooperate with other research institutes and promote awareness of the use of algorithms

⁸⁵⁷ Estonian Government, "Prime minister: to implement artificial intelligence, countries need a unified approach and ability to adapt" (16 October 2018) is available at <<https://www.valitsus.ee/en/news/prime-minister-implement-artificial-intelligence-countries-need-unified-approach-and-ability>> last accessed 27 December 2019.

⁸⁵⁸ The Danish Government, "Strategy for Denmark's Digital Growth" (2018) is available at <https://eng.em.dk/media/10555/digital-growth-strategy-report_uk_web-1.pdf> last accessed 27 December 2019.

⁸⁵⁹ Government of the Netherlands, "Dutch Digitization Strategy" (2018) is available at <<https://www.government.nl/documents/reports/2018/06/01/dutch-digitalisation-strategy>> last accessed 27 December 2019.

⁸⁶⁰ Ibid.

⁸⁶¹ Al White Paper, "Artificial Intelligence at the service of the citizen" is available at <<https://ai-white-paper.readthedocs.io/en/latest/>> last accessed 28 December 2019.

among citizens and consumers.⁸⁶² In contrast, France has not restricted itself only to policy attempts. Rather, the French Government introduced a legislative piece in 2017 endorsing a transparency obligation for hosting ISSPs. More specifically, the newly issued French Consumer Code urges as per Article L. 111-7 II ISSPs to provide transparent information to consumers with regard to the removal, indexing and ranking of the content within their networks.⁸⁶³ Hence, while some countries are more decisive towards the application of a transparency obligation and incorporate them into their national legislation, others prefer to limit any transparency initiatives at policy level.

Therefore, it is possible to conclude that initiatives on a transparency obligation are limited and fragmented. As these findings indicate, this is due to various reasons. At European level a transparency obligation is included in non-binding documents and thus has limited applicability. Further, European national jurisdictions either address transparency in the context of online platforms or recommend a transparency obligation for algorithmic decision-making procedures without limiting their scope on hosting ISSPs. Finally, some European member states have limited themselves to recommend a transparency obligation at policy level while other European member states have already integrated a transparency obligation into their national legislation. As a corollary of this divergent landscape, parties involved might face legal uncertainty. More specifically, internet users and consumers may be in doubt about their legal rights if the content that they upload is erroneously removed. Right holders may be unsure of the adequate protection of their works and goods online. Lastly, this lack of a uniform approach at European level might either impede new hosting ISSPs to enter the Digital Single Market or create confusion to the existing hosting ISSPs that operate in different European national jurisdictions.

On this basis, I argue that a statutory transparency obligation for hosting ISSPs should be introduced at European level. For this reason, the following section elaborates on the normative considerations of this transparency obligation.

⁸⁶² Department for Digital, Culture, Media and Sport, “Centre for data ethics and innovation consultation”(June 2018) is available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715760/CDEI_consultation_1_.pdf> last accessed 28 December 2019.

⁸⁶³ Propriete Industrielle et economie numerique “Part 1: A law for a digital French Republic – online platforms”(21 February 2017) is available at <<http://www.dreyfus.fr/en/new-technologies/part-1-a-law-for-a-digital-french-republic-online-platforms/>> last accessed 28 December 2019.

III. Normative considerations of a proposed transparency obligation

From a normative perspective, the introduction of a transparency obligation for hosting ISSPs appears to be warranted due to an array of reasons. As discussed below, these reasons mainly address the promotion of democratic values and the respect of online users' and consumers' rights.

Firstly, it has been argued that transparency would promote the rule of law.⁸⁶⁴ This is because under the current practice, the thresholds and the conditions that generate the automatic removal of material from hosting ISSPs are unknown to end-users. A telling example can be found in the erroneous removal of a video where students were protesting in favour of a free Tibet.⁸⁶⁵ Under the generic statement of copyright violation, students were not aware of the reasons that led to the removal of their video and thus were left in doubt about their legal rights. However, setting out a transparency obligation would give internet users ample opportunity for reviewing the conditions that trigger the removal. Given reviewability is an important constituent of the rule of law, such obligation might reinforce democratic governance.⁸⁶⁶

Moreover, the disclosure of information would increase users' awareness towards the practices that hosting ISSPs follow.⁸⁶⁷ This understanding is considered to be a cornerstone for European Law since via transparency, users would have the opportunity to verify the compatibility of the procedures with the existing legal requirements.⁸⁶⁸ In other words, as Buizje notes, it would enable users to "ensure that it is actually doing what it should be doing"⁸⁶⁹ or, as Article 29 Data Protection Working Party noted, "it is about engendering trust in the processes which affect the citizen by enabling them to

⁸⁶⁴ M. Hildebrandt, "The new imbroglia- living with machine algorithms" (2016) *Vrije Universiteit Brussel* 2; M. Perel (Filmar) and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 *Stanford Technology Law Review* 483.

⁸⁶⁵ This example has been found in A. Marsoof, "Notice and take down: a copyright perspective" (2015) 5 *Queen Mary Journal of Intellectual Property Law* 19; S. Seidenberg, "Copyright in the Age of YouTube" (ABA Journal, February 2009) is available at <http://www.abajournal.com/magazine/article/copyright_in_the_age_of_youtube> last accessed 24 April 2019.

⁸⁶⁶ J. Zerilli, A. Knott, J. Maclaurin and C. Gavaghan, "Transparency in Algorithmic and Human Decision-Making: Is there a double standard?" (2018) 9 *Philosophy and Technology* 3.

⁸⁶⁷ T. Zarsky, "The trouble with algorithmic decisions: an analytical road map to examine efficiency and fairness in automated and opaque decision making" (2016) 41 *Science, Technology and Human Values* 129.

⁸⁶⁸ M. Perel (Filmar) and N. Elkin-Koren, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 *Stanford Technology Law Review* 483.

⁸⁶⁹ A. Buizje, *The Principle of transparency in EU Law* (Unpublished PhD thesis 2013) 56-57.

understand, and if necessary, challenge those processes.”⁸⁷⁰ Therefore, cases that might amount to censorship of free speech and thus contradict the current legal system would be prevented.⁸⁷¹ A similar approach has already been adopted in the case of right holders on a voluntary basis. In this light, a number of hosting ISSPs have already voluntarily approached groups of right holders and given them the opportunity to gain an understanding of their practices. For instance, it has been reported that Google signed an agreement with the French audio-visual sector that enables right holders access to the filtering-based technology that hosting ISSPs adopt in order to curb the online infringements.⁸⁷² Therefore, it is possible to argue that since similar steps to make rights holders aware of the procedures of hosting ISSPs are available to right holders, users shall also take advantage of them.

Therefore, having the opportunity to review the conditions and be aware of the practices hosting ISSPs adopt, users would thus know the reasons upon which the decisions for removal have been made. In this way, it may be posited that transparency would enhance due process.⁸⁷³ Due process, as Pasquale notes, is “critical to a legitimate legal system”,⁸⁷⁴ since it permits users to challenge a decision after obtaining information of the facts of the removal.⁸⁷⁵ Otherwise, it seems impossible to challenge a decision without knowing the reasons that led to this decision. This lack of information would be in conflict with the right to a fair trial right or the right to effective remedy, as enshrined in the European Charter of Fundamental Rights and the European Convention of Human Rights

⁸⁷⁰ Article 29 Data Protection Working Party, “Guidelines on transparency under Regulation 2016/679” (2016) 5.

⁸⁷¹ F. Pasquale “Secret Algorithms Threaten the Rule of Law” (MIT Technology Review, 1 June 2017) is available at <https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/> last accessed 28 December 2019.

⁸⁷² F. Romero- Moreno, “Notice and stay down and social media: amending Article 13 of the Proposed Directive on Copyright2 (2018) 33 International Review of Law, Computers and Technology 187.

⁸⁷³ M. Perel (Filmar) and N. Elkin-Koren, “Accountability in Algorithmic Copyright Enforcement” (2016) 19 Stanford Technology Law Review 478.

⁸⁷⁴ F. Pasquale “Secret Algorithms Threaten the Rule of Law” (MIT Technology Review, 1 June 2017) <https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/> last accessed 28 December 2019.

⁸⁷⁵ J. Zerilli, A. Knott, J. Maclaurin and C. Gavaghan, “Transparency in Algorithmic and Human Decision-Making: Is there a double standard?” (2018) 9 Philosophy and Technology 3.

accordingly.⁸⁷⁶ Both rights, as the Council of Europe outlines, are “fundamental to the respect and protection of individual rights.”⁸⁷⁷

However, it could be argued that the principles of due process are only relevant to the environment of public authorities and cannot be applicable to the activities of private entities such as the hosting ISSPs. In this sense, internet users cannot question the decisions of private platforms and appeal against them. Yet, this view lies on unstable ground. It seems that, although hosting ISSPs are not governmental institutions, their activities appear to be tightly correlated with fundamental rights such as intellectual property rights, the right to freedom of expression, or the right to privacy. For instance, hosting ISSPs nowadays enforce intellectual property rights by removing illegal material from their platforms or detecting counterfeit goods within their networks.⁸⁷⁸ Hence, they shape our “informational environment” by deciding which information reaches the end-users and which information does not.⁸⁷⁹ Finally, social networks such as Facebook process a large amount of users’ personal data every day. In light of the power of hosting ISSPs,⁸⁸⁰ it seems that the need to safeguard fundamental rights of users is crucial. Otherwise, without due process, a new era of unaccountable hosting ISSPs may emerge. This is what Citron and Pasquale have described as “a new feudal order of unaccountable reputational intermediaries.”⁸⁸¹

⁸⁷⁶ G. Noto La Diega, “Against the Dehumanization of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information” (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 23.

⁸⁷⁷ Committee of Ministers, “Guide to good practice in respect of domestic “ (adopted on 18 September 2013) < https://www.echr.coe.int/Documents/Pub_coe_domestics_remedies_ENG.pdf> last accessed 7 January 2019.

⁸⁷⁸ T. Synodinou, “Intermediaries’ liability for online copyright infringement in the EU: evolutions and confusions” (2015) 31 *Computer Law and Security Review* 58-59 .

⁸⁷⁹ M. Taddeo and L. Floridi, “The Debate on the Moral Responsibilities of Online Service Providers” (2016) 22 *Science and Engineering Ethics* 1575-1603.

⁸⁸⁰ A number of scholars have pointed out the power of online intermediaries: S. Stalla-Bourdillon, “Internet intermediaries as responsible actors? Why is it time to rethink the E-Commerce Directive as well” in M. Taddeo and L. Floridi (eds.), *The responsibilities of online service providers* (Springer 2017) 275; D. Broeders and L. Taylor, “ Does Great Power come with Great Responsibility? The need to talk about corporate political responsibility” in M. Taddeo and L. Floridi (eds.), *The responsibilities of online service providers* (Springer 2017) 315; D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 81-99; J. Wang, *Regulating Hosting ISPs’ responsibilities for copyright infringement: The freedom to operate in the US, EU and China* (Springer 2018); M. Thompson, “Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries” (2016) 18 *Vanderbilt Journal of Entertainment & Technology Law* 783 -784.

⁸⁸¹ D. K. Citron and F. Pasquale “The Scored Society: Due Process for Automated Predictions” (2014) 89 *Washington Law Review* 19.

Further, it has been argued that transparency would enhance the legitimacy of hosting ISSPs' activities.⁸⁸² This view is important due to the questionable enforcement and quasi-adjudication duties that hosting ISSPs have been assigned to undertake. In particular, there is a pressing concern that revolves around whether hosting ISSPs compromise their enforcement tasks with their own private business interests and their partners' interests.⁸⁸³ However, being aware of the grounds upon which hosting ISSPs reach a decision, users would show more willingness to accept the specific decision.

In line with this, and given that there is legitimacy, trust comes to the forefront as well. If users were aware of the importance of the role of hosting ISSPs, they would trust, to a greater extent, the services hosting ISSPs offer. This is because users would make sure that hosting ISSPs that are entitled to remove online material from their platforms exercise their activities in a fair way.⁸⁸⁴ In this sense, transparency could act as a guide to users on what to expect from the online services and have a deeper understanding of the practices they use. As Brill notes "transparency should also include helping consumers navigate the complex ecosystem of data, devices, and big data analytics operating behind the scenes, so that consumers understand the practices that can affect them, and exercise choices about the practices."⁸⁸⁵ Therefore, users may have more confidence and faith in online services. They may also be less sceptical about undertaking transactions with hosting ISSPs, and less reluctant to do so.

A representative example of such a line of thinking can be found in an EU Commission's Study on the transparency of hosting ISSPs, which claims that providing information for a specific product in a hosting ISSP can enhance the trust of online consumers.⁸⁸⁶ In particular, this study demonstrates that the lack of information about the identity of the seller could prevent the users from choosing this specific product. In contrast, it has been

⁸⁸² M. Perel (Filmar) and N. Elkin-Koren, "Accountability in algorithmic copyright enforcement" (2016) 19 *Stanford Technology Law Review* 494.

⁸⁸³ M. Tessier, J. Herzog and L. Madzou, "Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness" in L. Belli and N. Zingales (eds.), *Platform regulations- How to regulate them and how they regulate us* (2018) 181.

⁸⁸⁴ R. Binss, M. Van Kleek, M. Veale, U. Lyngs and J. Zhao and N. Shabolt "It's reducing a human being to a percentage: perceptions of justice in algorithmic decisions" (2018) *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.

⁸⁸⁵ J. Brill, "Keynote Address Before Coalition for Networked Information: Transparency, Trust, and Consumer Protection in a Complex World" (15 December 2015) 5 is available at <https://www.ftc.gov/system/files/documents/public_statements/895843/151216cnikeynote.pdf> last accessed 28 December 2019.

⁸⁸⁶ EU Commission, "Behavioural Study on the transparency of online platforms- Executive summary" (2018) 6.

observed that when there is information on the third party the percentage of users that select these goods could reach up to 50%. Furthermore, the study highlights the importance of reviews. While there is low likelihood of purchasing the precise goods when reviews are not available, the likelihood of buying it in cases where there are reviews could increase sales by up to 200%. This means that the provision of information for the third party or the existence of reviews for the products attracts online consumers and preserves online business welfare. As the study effectively summarizes, transparency in the online word aims to accommodate not only consumers' interests but also hosting ISSPs' business interests since a great number of consumers will show a higher amount of trust towards their online activities.⁸⁸⁷

However, transparency would not only enhance the legitimacy of the hosting ISSPs' decisions and thus promote users' trust. Indeed, it would also have benefits for hosting ISSPs' business models. In particular, transparency would contribute to the quality of the services they offer as it would encourage hosting ISSPs to adopt good methods and thus perform better. Drawing parallels with the concept of transparency in public institutions, Addink and Ten Berge point out that a transparency obligation is tightly correlated with "socially accepted standards and values and with the principles of democracy and the rule of law."⁸⁸⁸ This means that higher standards of achievement will be set out, thus reinforcing important democratic values. Likewise, within the framework of online copyright and trade mark infringements, transparency would induce hosting ISSPs to adopt better practices. For instance, given that "algorithms can be incredibly complicated and can create surprising new forms of risk, bias and harm",⁸⁸⁹ hosting ISSPs would first examine the efficiency and the accuracy of those algorithms before putting them into practice. In this way, as Elkin- Koren points out, under the fear of disgrace or public criticism about their methods, "decision- makers who function in a transparent environment are discouraged from engaging in problematic conduct."⁸⁹⁰ This implies that

⁸⁸⁷ EU Commission, "Study on Behavioral study on the transparency of online platforms: Final report" (2018) 48 where it has been found that "online transparency is clearly in the interests of consumers. Equally, it might be argued that it is in the interests of platforms and traders who could expect to see a growth in online activity as a result of increased consumer confidence and trust."

⁸⁸⁸ G.H. Addink and J.B.J.M. ten Berge, "Study on Innovation of Legal Means for Eliminating Corruption in the Public Service in the Netherlands" (2007) Netherlands Comparative Law Association 12.

⁸⁸⁹ Data and Society, "Algorithmic Accountability: A Primer" (18 April 2018) 6; S. Venkant, "When an algorithm isn't" (Medium, 2 October 2015) is available at <<https://medium.com/@geomblog/when-an-algorithm-isn-t-2b9fe01b9bb5>> last accessed 28 December 2019.

⁸⁹⁰ M.Perel (Filmar) and N. Elkin-Koren, "Accountability in algorithmic copyright enforcement" (2016) 19 Stanford Technology Law Review 495.

hosting ISSPs would be afraid to deviate from the rules since information regarding their actions would be made available to users. Therefore, higher rates of good performance would be achieved, and marginal errors would be tempered to a great extent.

Further, it is possible to argue that a transparency obligation would mitigate any information asymmetries that exist between hosting ISSPs and internet users. Information asymmetry takes place “when one party to a transaction has pertinent information that the other party lacks.”⁸⁹¹ While this understanding seems difficult to apply in the copyright context, it finds fertile ground in the trade mark framework. For instance, in the offline world, the trader and the consumer have knowledge of the features of a product.⁸⁹² They can both verify the origin and the quality of a product, characteristics that are fundamental to consumers in order to make a decision and purchase a specific product among others.⁸⁹³ This is in contrast with the online environment where only the trader and the hosting ISSP have knowledge over the characteristics of the goods.⁸⁹⁴ This is because, as Sorensen points out “the need to secure transparency through information is based on the assumption that the contracting parties have different levels of knowledge relevant to their choice to enter into a contract.”⁸⁹⁵ Hence, this implies that it is up to hosting ISSPs to control the dissemination of goods. Otherwise, online consumers are vulnerable to confusion and deception when purchasing products online.⁸⁹⁶

Finally, transparency would enhance the right to information. This is because in the online world, a number of hosting ISSPs might indiscriminately remove material without justifying the reasons for its removal. This understanding can be exemplified by a handful of ISSPs such as Google⁸⁹⁷ where it has been found that this search engine removes links from their search listing results that do not favour their business partners or as a response to individual requests.⁸⁹⁸ In particular, in its terms and conditions, Google notifies users

⁸⁹¹ Ch. Shen, J. Chiou, B. Kuo, "Remedies for information asymmetry in online transaction: An investigation into the impact of web page signals on auction outcome" (2011) 21 *Internet Research* 156.

⁸⁹² N. Economides, "The Economics of Trademarks" (1988) 78 *Trademark Reporter* 526.

⁸⁹³ N. Economides, "The Economics of Trademarks" (1988) 78 *Trademark Reporter* 526.

⁸⁹⁴ A. Marsoof, *Internet intermediaries and trade mark rights* (Routledge 2019) 12; Ch. Shen, J. Chiou, B. Kuo, "Remedies for information asymmetry in online transaction: An investigation into the impact of web page signals on auction outcome" (2011) 21 *Internet Research* 156.

⁸⁹⁵ M.J. Sorensen, "Draft Model Rules on Online Intermediary Platforms" in B. Devolder (ed.), *The Platform Economy: Unravelling the Legal Status of Online Intermediaries* (Intersentia 2019) 182.

⁸⁹⁶ See also Ed. Rubin, "The internet, consumer protection and practical knowledge" in J. Winn, *Consumer Protection in the Age of the 'Information Economy'* (2006) 37.

⁸⁹⁷ E. Laidlaw, "Private Power, Public interest: an examination of search engine accountability" (2008) 17 *International Journal of Law and Information Technology* 133.

⁸⁹⁸ *Ibid.*

that they will “remove pages from their results if they believe the page violates their Webmaster Guidelines, if they believe that they are required to do so by law, or at the request of the webmaster who is responsible for the page.”⁸⁹⁹ Likewise, Baidu in its terms of service notes that “Baidu Users agree that Baidu is entitled to.... remove and delete any content in this service based on Baidu’s own discretion for any reason, including but not limited to disuse for a long period of time or if Baidu considers a Baidu User to have violated the terms and conditions of this Agreement.”⁹⁰⁰ In a similar fashion, Twitter includes in its terms of service the statement “We reserve the right to remove Content that violates the User Agreement, including for example, copyright or trade mark violations...”.⁹⁰¹ It is this element of the policy that has been criticized as resulting to the indiscrete removal of web results and content online. This is because this broadly defined statement could imply that hosting ISSPs have a margin of manoeuvre and could thus remove links or material after receiving individual requests without clarifying their reasoning. In this way, hosting ISSPs could either grace its business partners or be subject more easily to external political influence that could give those rewards.

Bearing in mind the above, it is possible to argue that the role of transparency is very important in the online world as it is a great asset for internet users, online consumers and subsequently the business model of hosting ISSPs. In particular, with regard to internet users and online consumers, this is because transparency would enhance the rule of law and due process. For instance, it would give users information with regard to the removal of their content. In doing so, users would be able to observe whether the hosting ISSP has complied with the rules and either accept or challenge the decision. In contrast, the lack of information about the conditions that trigger the removal of material would undermine the rule of law and the principle of due process since users would be deprived of the right to effective remedy and the right to a fair trial as set out in the EU Charter of Fundamental Rights and European Convention of Human Rights. Further, the ascription of a transparency obligation would justify the legitimacy of the decisions undertaken by the hosting ISSPs’ activities and thus generate trust to online consumers. This is because with transparency users would be aware of the thresholds that generate the removal of

⁸⁹⁹ Webmaster Guidelines <<https://support.google.com/webmasters/answer/35769?hl=en>> last accessed 14 January 2019.

⁹⁰⁰ Baidu User agreement is available at <<http://motu.baidu.com/protocal.html>> last accessed 15 May 2019.

⁹⁰¹ Twitter Terms of services is available at <<https://twitter.com/en/tos>> last accessed 15 May 2019.

their material. Otherwise, users would be suspicious of the principal reasons their material was taken down and whether this decision had a legitimate basis.

In addition, transparency would have a positive impact on transactions between hosting ISSPs and online consumers. This is because it would eliminate the information asymmetries in online purchases since consumers in the online world would have more information about the quality and the origin of goods. Therefore, consumers would not be deceived and their trust and confidence in the online services would increase.

Yet, apart from safeguarding internet users/ online consumers' rights, a transparency obligation would induce hosting ISSPs to adopt better practices in the operation of their business and therefore the principle of good governance would be enhanced. This is because under the fear of being publicly criticized about their business policies, hosting ISSPs would be incentivized to undertake a prior examination of their practices in order to eliminate any errors or malfunctions.

In light of the above, it could be posited that a transparency would have benefits not only for users but also for hosting ISSPs' interests. Yet, as mentioned at the beginning of this chapter, however necessary a transparency obligation might be, it is crucial to articulate the limits within which such a transparency obligation would be exercised. Otherwise, the potential advantages a transparency obligation might have could lead to adverse results for hosting ISSPs. It is to these limits the following section of this chapter now turns.

IV. How should a proposed transparency obligation be shaped?

In order to frame the limits within which a transparency obligation would take place, it is important to take into consideration in which context a transparency obligation would be applicable and how it would be construed. This is because, as explained at the beginning of this chapter, it has been argued that "different contexts require different levels of transparency."⁹⁰² This means, for instance, that a full disclosure of an algorithm would have a detrimental effect on the business model of hosting ISSPs since third parties would be able to take advantage of it and find pathways to circumvent or, as referred to by Yakowitz and others, to "game the algorithm."⁹⁰³ Indeed, a transparency obligation shall

⁹⁰² R. Caplan, J. Donovan, L. Hanson and J. Matthews, "Algorithmic Accountability: A primer: Tech Algorithm Briefing: How algorithms perpetuate racial bias and inequality" (2018) 7.

⁹⁰³ J. Yakowitz Bambauer and T. Zarsky, "The Algorithm Game" (2018) 94 Notre Dame Law Review 11

take into consideration the interests of internet users/online consumers as well as the hosting ISSPs. In particular, with regard to online consumers, Devenney argues that “care must be taken to recognise the limits on the extent to which the provision of information can cure the many varied and complex disadvantages under which different consumers may be operating.”⁹⁰⁴ This implies that in the case of online consumers, the provision of information relating to the functioning of the online marketplace must take into consideration the position of online consumers, such as the information asymmetries that exist,⁹⁰⁵ while at the same time the disclosure of information shall not harm the business model of the online marketplace.

Against this background, the narrative continues by examining the different contexts in which a transparency obligation should be applicable and how it should be articulated so as to maintain a balance between the different interests at stake. In particular, on the basis of the normative considerations that have been discussed in the previous section, I assess how a transparency obligation should be construed in relation to the algorithms that hosting ISSPs use, to their terms and conditions and to the issue of transparency reports.

A. *Transparency in algorithmic decision-making process*

As mentioned at the beginning of this chapter, to curb the increasing number of online infringements, hosting ISSPs mainly use algorithms. These algorithms decide the removal of the material based on an automated decision-making process. While this process excludes any human intervention, which can be “cost-saving” for hosting ISSPs,⁹⁰⁶ average users may perceive it as a ‘black box’.⁹⁰⁷ This is because algorithms are inscrutable, as Introna notes, and users cannot oversee them and thus gain an understanding of their function.⁹⁰⁸

⁹⁰⁴ J. Devenney, “The legacy of the Cameron-Clegg coalition programme of reform of the law on the supply of goods, digital content and services to consumers”(2018) 6 *Journal of Business Law* 488

⁹⁰⁵ See chapter 5 III.

⁹⁰⁶ D. Citron, “Technological Due Process” (2008) 85 *Washington University Law Review* 1252.

⁹⁰⁷ D. Citron and F. Pasquale, “The scored society: due process for automated predictions” (2014) 85 *Washington Law Review* 5 where the authors note that “the lack of transparency of credit scoring systems leaves consumers confounded by how and why their scores change.”; G. Frosio, “Algorithmic enforcement online” in P. Torremans (ed.), *Intellectual Property and Human Rights* (4th edition, Kluwer Law International forthcoming 2020) 30 where Frosio notes that “algorithmic enforcement finds its primary Achilles’ hill in algorithms’ transparency”.

⁹⁰⁸ L. Introna, “ Algorithms, Governance and Governmentality: on governing academic writing” (2016) 41 *Science, Technology and Human Values*; D. Heaven, “Not like us: Artificial Minds we can’t understand” (2013) *New Scientist* 32-35; Heaven argues that there are cases where algorithms are not understood to their

It is this inscrutable and opaque nature of algorithms that has raised calls for transparency.⁹⁰⁹ Such calls dictate that hosting ISSPs should disclose their algorithms to users so that users would be aware of, and could challenge, the reasons that triggered the removal of their content online.⁹¹⁰

The main proponent of full transparency of the algorithm is Lessig.⁹¹¹ In his landmark book *Code and Other laws of Cyberspace*, he argues that in order to understand how internet infrastructure works, an “open” code is needed.⁹¹² This is because, as he explains, internet infrastructure is regulated by lawmakers who, through internet infrastructure, aim to control the behaviour and the activities of internet users. By disclosing the code, users would be aware of the practices that their governments follow in order to regulate their behaviour.

Other proponents of full disclosure of algorithms are Introna and Nissenbaum. They outline the need for full disclosure of algorithms that the search engines use in order to index material or facilitate the search of information.⁹¹³ This is because, as they argue, algorithms may, either intentionally or unintentionally, downgrade or upgrade specific websites. By excluding certain information while at the same time prioritizing other material, algorithms undermine the importance of the internet as a public good and erode the main principles upon which has been built.⁹¹⁴ Such principles mainly concern the boost of free flow of information and free access to an open internet.⁹¹⁵

However, the full disclosure of the algorithm to end-users seems problematic. This is mainly due to three specific reasons. The first reason touches upon the consideration of

manufacturers as well; in addition in R. Caplan, J. Donovan, L. Hanson and J. Matthews, “Algorithmic Accountability: A primer” (2018) 7 where they argue that “the more complex and sophisticated an algorithm is, the harder it is to explain, even by a knowledgeable algorithmic engineer.”

⁹⁰⁹ T. Zarsky, “The trouble with algorithmic decisions: an analytical road map to examine efficiency and fairness in automated and opaque decision making” (2016) 41 *Science, Technology and Human Values* 121; Marchill, C. Neuberger and F. Schindler, “Transparency on the Net: Functions and Deficiencies of Internet Search Engines” (2003) 5 *The Journal of Policy, Regulation and Strategy for Telecommunications* 52; E. van Couvering, “Is relevance relevant? Market, Science and War: Discourses of search engine quality” (2007) 12 *Journal of Computer-Mediated Communication* 866.

⁹¹⁰ D. Citron, “Technological Due Process” (2008) 85 *Washington University Law Review* 1308.

⁹¹¹ L. Lessig, *Code and other laws of cyberspace* (1999) 139.

⁹¹² *Ibid.*

⁹¹³ L. Introna and H. Nissenbaum, “Shaping the web: Why the Politics of search engines matters” (2000) *The Information Society* 181.

⁹¹⁴ *Ibid.*, 178.

⁹¹⁵ OECD, “OECD Principles for Internet Policy Making” (2014) 5-6 is available at <<https://www.oecd.org/internet/ieconomy/oecd-principles-for-internet-policy-making.pdf>> last accessed 15 May 2019.

an algorithm as a business trade secret,⁹¹⁶ a notion which lies at the core of the business model of a company.⁹¹⁷ As Pasquale notes “trade secrecy is a business tool”.⁹¹⁸ Many hosting ISSPs have developed their own algorithms and integrated them into their business operation.⁹¹⁹ These algorithms hugely increased the popularity and the revenues of several hosting ISSPs⁹²⁰ by either addressing the way information is presented to end-users or focusing on detecting illegal content that is circulated within a platform without author’s permission. For instance, Facebook has developed its own algorithm in order to manage its News Feed section, which concerns the posts Facebook’s users can view, taking into consideration different parameters such as gender, education, and location of the users.⁹²¹

Given the importance of algorithms as business tools, many hosting ISSPs abstain from disclosing the algorithm because they are afraid that their competitors will take advantage of them.⁹²² As Diakopoulos points out, such a full disclosure “may undermine their competitive advantage.”⁹²³ This is because the competitors of a company might copy its algorithm and thus provide the same services to internet users.⁹²⁴ This understanding has been exemplified in a handful of court rulings. In those cases, the courts rejected the claims of right holders and refrained from ordering the full disclosure of an algorithm under the reasoning that an algorithm is protected under Trade Secrecy Laws. For instance, in the dispute between Viacom, a film and TV industry corporation, and YouTube,⁹²⁵ Viacom brought legal proceedings against YouTube, requesting the Court to

⁹¹⁶ R. Wexler, “Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System” (2018) 70 Stanford Law Review 1383; D. Citron and F. Pasquale, “The scored society: due process for automated predictions” (2014) 89 Washington Law Review 17.

⁹¹⁷ F. Pasquale, “Restoring transparency to automated authority” (2011) Seton Hall Research Paper 237.

⁹¹⁸ Ibid.

⁹¹⁹ D. Citron, “Technological Due Process” (2008) 85 Washington University Law Review 1290; Citron notes that “Because vendors typically build these systems, the source code is proprietary and closed.”

⁹²⁰ C. Cheung, P. Chiu and M. Lee, “Online social networks: Why do students use facebook?” (2011) 27 Computers in Human Behaviour 1337.

⁹²¹ J. Martin, “The New Facebook Algorithm: Secrets Behind How It Works and What You Can Do To Succeed” (Carney, 15 February 2018) is available at <https://carney.co/daily-carnage-feature/new-facebook-algorithm-secrets-behind-works-can-succeed/> last accessed 28 December 2019.

⁹²² D. Citron and F. Pasquale, “The scored society: due process for automated predictions” (2014) 89 Washington Law Review 5.

⁹²³ N. Diakopoulos, “Algorithmic accountability reporting: on the investigation of black boxes” (2013) Town Center for Digital Journalism 12.

⁹²⁴ F. Pasquale, *Black Box Society: The secret algorithms that control money and information* (2015) 142.

⁹²⁵ *Viacom Intern. Inc. v. Youtube Inc.* 676 F.3d 19 United States Court of Appeals, Second Circuit 2012 is available at https://cyber.harvard.edu/people/tfisher/cx/2012_Viacom.pdf last accessed 28 December 2019; M. Perel (Filmar) and N. Elkin-Koren, “Black box tinkering: beyond disclosure in algorithmic enforcement” (2017) 69 Fla. L. Rev.193.

order YouTube to disclose its algorithm that identifies copyright infringing material within its platform. After a careful examination of the facts, the District Court declared that a company's algorithm is protected under Trade Secret Law and outlined its commercial importance for a company along with the tremendous labour and economic effort that is needed in order to develop such an algorithm.⁹²⁶ Subsequently, as a corollary to this approach, the Court declined the request of Viacom and did not order the disclosure of the algorithm. Otherwise, as the Court has noted, the disclosure of an algorithm might mean the end to the owner's competitive edge.⁹²⁷ This means that either the owner could lose the dominant position they may have in the market or that their competition would be detrimentally affected. For instance, YouTube's competitors, such as Dailymotion, could have benefitted from the revelation of the algorithm and attempted to create a similar one, potentially becoming more competitive and thus attract more customers to their services.

Further, so important are trade secrets for a business that any disclosure without the corporation's consensus could give the right to the business to ask for damages.⁹²⁸ This is because a trade secret is the intellectual property of a business and must be protected against infringers.⁹²⁹ Such an understanding was reinforced in the long-running legal battle of the Linux case.⁹³⁰ In this case, SCO, a software company, brought legal proceedings against IBM, alleging that IBM used SCO's algorithm without its authorisation. More specifically, after SCO and IBM concluded an agreement to use certain technological knowledge, IBM decided to change its business strategic plan and invest more on Linux promotion. Despite the dismissal of SCO's allegation for misuse of trade secrets, this case demonstrates the importance of an algorithm as a trade secret since a company can bring legal proceedings against another company alleging the misuse of its trade secret. Therefore, drawing conclusions from this case, one might extrapolate that trade secrets are fundamental parts of a business model and any disclosure could have a detrimental effect for the company with regard to its competitiveness.

⁹²⁶ *Viacom Intern. Inc. v. Youtube Inc.*, United States District Court, S.D. New York, Jul 1, 2008 253 F.R.D. 256 (S.D.N.Y. 2008). <<https://casetext.com/case/viacom-intern-inc-v-youtube-inc> > last accessed 28 December 2019.

⁹²⁷ *Ibid.*

⁹²⁸ F. Pasquale "Restoring transparency to automated authority" (2011) Seton Hall Research Paper 238.

⁹²⁹ *Ibid.*

⁹³⁰ A. LaFontaine, "Adventures in software licensing: SCO v. IBM and the future of the open source model" (2006) 4 *Journal on Telecommunications and High Technology Law* 449.

The second reason that justifies the rejection of any request towards the revelation of an algorithm can be found in the risks of circumvention by potential infringers-users. This risk has been outlined by Facebook's representative who argued that Facebook refrains from any revelation of its algorithm so that the users do not know about its "workarounds".⁹³¹ This is mainly because, with the disclosure of the full algorithm of the company, many users would know the operation an online intermediary operates and thus might identify potential loopholes. Such loopholes can be circumvented with the use of certain services such as Smart DNS or VPN services. These services have been extensively used by a number of internet users already in order to download illegal content from file-sharing websites. For instance, it has been reported that many companies, such as Smart DNS services and VPN services, help users to unblock geo-blocking technical measures so that they can continue committing copyright infringements.⁹³² While geo-blocking is not illegal per se,⁹³³ the use of such services might pose serious threats to hosting ISSPs' welfare. Therefore, it seems that a transparency obligation would erode the efficiency of an algorithm since users would be aware of its peculiarities and flaws and thus be able to circumvent them. This is why, Strathern, citing Goodhart, pointed out "when a measure becomes a target, it ceases to be a good measure."⁹³⁴

The third reason supporting maintaining the secrecy of algorithms touches upon the lack of usefulness of disclosure of an algorithm to users. Take the example of a 65 years old individual. Although she uses social networks and auction platforms, she is considered the average unskilled internet user. Whether the algorithm is revealed to her or not, it will not clarify her concerns why her content has been removed or why she bought a counterfeit product. Unless someone is experienced in understanding and interpreting complicated algorithms, it seems that the average user will not benefit from the revelation of the algorithm. This is because it is not possible to interpret an algorithm in

⁹³¹ K. Huszti-Orban, "Countering Terrorism and Violent Extremism Online: what role for social media platforms?" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are regulated and how they regulate us* (2018) 204; J. Urban, J. Karaganis and B. Schofield, "Notice and Takedown in everyday practice" (2017) Berkeley Law Policy Paper 4.

⁹³² Ernesto, "PayPal starts banning VPN and SmartDNS services" (Torrentfreak, 5 February 2016) is available at <<https://torrentfreak.com/paypal-starts-banning-vpn-and-smartdns-services-160205/>> last accessed 28 December 2019.

⁹³³ M. Trimble, "Geoblocking and Evasion of Geoblocking – Technical Standards and the Law" in R. Lobato and J. Meese, *Geoblocking and Global Video Culture* (2016) 55 where Trimble argues that geoblocking is used as a tool of regulation and enforcement of intellectual property rights.

⁹³⁴ M. Strathern, 'Improving ratings': audit in the British University system" (1997) 5 *European Review* 308.

simple words or at least in a way that is understood to the average user.⁹³⁵ For instance, the Windows Vista algorithm includes 50 million lines with numerical and mathematical symbols.⁹³⁶ Subsequently, the full disclosure of this algorithm code to most users would not help them understand the main reasons that justify the removal of their content.

Undoubtedly, the criticism against the full disclosure of an algorithm has its own merits. However, although full disclosure of their algorithms would be detrimental for hosting ISSPs' business welfare, it could be argued that some level of transparency is acceptable. The primary aim of this type of transparency would be to accommodate the needs of users without neglecting hosting ISSPs' interests.

This thesis posits that a transparency obligation in the algorithmic decision-making process should be understood either as a right of an individual to request explanation of the content removal,⁹³⁷ or as "qualified transparency"⁹³⁸ which means that the full disclosure of an algorithm can only be made to a governmental authority.

With regard to the first option, to set out a right to explanation for online intellectual property infringements seems a novelty. For this reason, in order to gain a better understanding of this right, an analogy can be drawn from the General Data Protection Regulation.⁹³⁹ Looking closely at Articles 13, 14 and 15 of the GDPR, it is possible to observe that data controllers must reveal their rationale behind their decision-making processes. More specifically, as per Articles 13 and 14 of the GDPR, data controllers must disclose the existence of and the logic behind the algorithmic decision-making process while Article 15 notes that the data controller must provide to the data subject information about "...the significance and the envisaged consequences of such processing for the data subject."⁹⁴⁰

⁹³⁵ G. Noto La Diega, "Against the Dehumanization of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information" (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 23.

⁹³⁶ L. Introna, "Algorithms, Governance and Governmentality: on governing academic writing" (2016) 41 *Science, Technology and Human Values* 7.

⁹³⁷ J. Kroll argues that the ability of internet users to understand the reasons behind the removal of content safeguards procedural regularity. This means that "each participant will know that the same procedure was applied to her and that the procedure was not designed in a way that disadvantages her specifically." in J. Kroll and others, "Accountable algorithms" (2017) 165 *University of Pennsylvania Law Review* 22.

⁹³⁸ F. Pasquale, *Black Box Society: The secret algorithms that control money and information* (2015) 9; F. Pasquale, "Beyond Innovation and Competition: The Need for Qualified Transparency in Internet" (2014) 104 *Northwestern University Law Review* 105.

⁹³⁹ Hereinafter GDPR.

⁹⁴⁰ Article 15 (h) GDPR.

Although it has been argued that the above-mentioned Articles do not include any right to explanation,⁹⁴¹ the prevailing view seems in favour of a right to explanation. This is because scholars who support the right to explanation adopt a broader interpretation of these Articles. For instance, Maglieri and Comande argue that the new GDPR offers a right to explanation which is based on a wide interpretation of Articles 13, 14 and 15 along with Recital 71.⁹⁴² To my understanding, in order to have a right to explanation, there must be an ex-post information to data subjects about their personal data. This means that a data subject can request after the process of personal data more information about the process. By contrast, the provision of ex-ante information does not constitute a right to explanation. In this regard, while Maglieri and Comande found that Articles 13, 14 and 15 offered ex-ante information to data subjects, they argue that if these articles are examined through the lens of Recital 71, they can be interpreted as provision of ex-post information and thus a right to explanation emerges. Recital 71 endorses a right to explanation and notes that “...such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment....”

Yet, as pointed out at judicial level, from an European law perspective a recital is non-binding and its value is “normative supplementary” and not interpretative.⁹⁴³ This understanding has been clarified in the *Nilsson* case.⁹⁴⁴ In this case, in para. 54 the CJEU outlined that “on this point, it must be stated that the preamble to a Community act has no binding legal force and cannot be relied on as a ground for derogating from the actual provisions of the act in question.”⁹⁴⁵ At the same time, the Court concluded that the interpretation of a Recital shall not be in conflict with the existing provisions in the Directive.⁹⁴⁶

⁹⁴¹ L. Edwards and M. Veale, “Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for” (2016) 16 *Duke Law and Technology Review* 18.

⁹⁴² G. Maglieri and G. Comande, “Why a right to legibility of automated decision-making exists in the General Data Protection Regulation” (2017) 7 *International Data Privacy Law* 254-255.

⁹⁴³ *Ibid.*

⁹⁴⁴ This example has been given by Maglieri and Comande in order to reinforce the view that the preamble to Community act is normative supplementary; see C-162/97 *Nilsson*, (1998) ECR I- 7477.

⁹⁴⁵ C-162/97 *Nilsson*, (1998) ECR I- 7477, para. 54.

⁹⁴⁶ G. Maglieri and G. Comande, “Why a right to legibility of automated decision-making exists in the General Data Protection Regulation” (2017) 7 *International Data Privacy Law* 255.

It is this clarification that is made by the Court that urged Maglieri and Comande to posit that since the interpretation of Recital 71 does not contradict the existing legal provisions, it could provide an “explanatory value” to the existing legal provisions of the GDPR and thus a wide interpretation of Articles 13, 14, 15 and 22 of GDPR is warranted.

Such a stance has been maintained by Noto La Diega, who argues that a right to explanation is endorsed in Articles 13, 14, 15 and 22 of the GDPR after taking into consideration Recital 71.⁹⁴⁷ This is because, as he argues, a “purposive approach and a correct valorisation of the role of the recitals”⁹⁴⁸ shall be taken into consideration. This means that the right to explanation in the recital shall signal the main purpose of the GDPR which is to safeguard data subjects’ personal data in the course of the processing. Along similar lines, the Council of Europe outlined that “ ... the data subject should be entitled to know about the personal data concerning him or her and the logic which served as a basis for the profiling...”⁹⁴⁹ Article 29 Working Party in its report on Guidelines on Automated individual decision-making and Profiling and its report on Guidelines on consent outlines the need to provide information to the data subject about the process of personal data.⁹⁵⁰

On the basis of the above, it could be argued that a right to explanation could be endorsed with regard to online intellectual property infringements. However, in this case, instead of processing personal data, hosting ISSPs filter the content that internet users upload within the networks through automated process. For instance, with regard to the case of algorithms that social networks or video-exchange music platforms use and as discussed earlier, whereas it is prohibitory to reveal the full algorithm to users, the negative effects could be mitigated if users were aware of the parameters under which algorithms operate. In particular, excluding the commercial keywords and any fundamental technical details of algorithms, users must be in a position to question hosting ISSPs for more

⁹⁴⁷ G. Noto La Diega “Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information” (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 23.

⁹⁴⁸ *Ibid.*

⁹⁴⁹ Council of Europe, “The protection of individuals with regard to automatic processing of personal data in the context of profiling” Recommendation CM/Rec (2010)13 and explanatory memorandum 50-51.

⁹⁵⁰ Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679” (2018) 25 notes that “nevertheless good practice to provide the above information. In any event the controller must provide sufficient information to the data subject to make the processing fair and meet all the other information requirements of Articles 13 and 14.”; Article 29 Working Party, “Guidelines on consent under Regulation 2016/679” (2018) 5.

information about the ways filtering algorithms operate.⁹⁵¹ For instance, after their content has been removed, users must be in a position to interrogate online platforms about their decision-making process. In this way, it would not only the users who would be eligible to challenge the hosting ISSPs' decisions, but also hosting ISSPs' actions would be in accordance with the right to fair remedy and right to fair trial as enshrined in the European Convention of Human Rights and European Charter of Fundamental Rights.⁹⁵² This understanding was also reinforced by the Council of Europe's Recommendations in 2008 and 2015. More specifically, the Recommendation on promoting the respect of freedom of expression in 2008 noted that, in case hosting ISSPs deploy filtering-based technologies, internet users should be offered the option "...to challenge the blocking or filtering of content and to seek clarifications and remedies."⁹⁵³ In a similar fashion, the Recommendation on media and information society in 2015 notes that hosting ISSPs must "ensure that internet users have access to effective remedies when their rights and freedoms have been restricted or when they believe that their rights have been violated."⁹⁵⁴

However, it could be argued that among the users whose content has been unreasonably removed, there are also infringer-users who uploaded or shared unauthorized content online. Thus, it may be considered why these infringer-users should be made aware of the parameters fed within an algorithm. Drawing parallels with democratic values, clear and codified procedures are in conformity with the principles of due diligence and the rule of law. Every individual shall be aware of the legal rules and the potential penalties which exist in case an individual break the law. Likewise, in the case of taking down material, every user that interacts with this kind of online platform should be made aware of the practices it follows. Yet, it is up to the internet user to decide whether she will upload or share illegal material online.

⁹⁵¹ F. Romero-Moreno, "Notice and stay down and social media: amending Article 13 of the Proposed Directive on Copyright" (2018) 33 *International Review of Law, Computers and Technology* 196.

⁹⁵² G. La Diega, "Against Dehumanisation of Decision-Making: Algorithmic Decisions at the crossroads of Intellectual Property, Data Protection and Freedom of Information" (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 23.

⁹⁵³ Committee of Ministers, "Recommendation to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters" CM/ Rec (2008) is available at <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4> last accessed 28 December 2019.

⁹⁵⁴ Committee of Ministers, "Recommendations in the field of media and information society Media and Internet Division" (2015) is available at <<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44>> last accessed 28 December 2019.

Apart from individuals who have the right to explanation, another interpretation of a transparency obligation with regard to algorithms is “qualified transparency”, as introduced by Pasquale.⁹⁵⁵ “Qualified transparency” is understood as the partial disclosure of an algorithm in order to balance the interests of the parties involved, namely hosting ISSPs, internet users and right holders. In this case, after taking into consideration trade secrecy laws and the reasons that encourage hosting ISSPs to refrain from disclosing their algorithms, Pasquale explains that the revelation of an algorithm should be made only towards a governmental body that would be in charge of examining the accuracy of algorithms.⁹⁵⁶

Interestingly, although Pasquale introduced the concept of qualified transparency with regard to search engines’ search results, it could be argued that qualified transparency can also be extended to other kinds of hosting ISSPs such as social networks and video-exchange platforms. In this case, the algorithm could be disclosed to an authority to which hosting ISSPs would be accountable. This authority would assess the algorithm and identify any flaws embedded therein.⁹⁵⁷ In this way, marginal errors in cases of material removals would be eliminated and users and consumers’ rights would be safeguarded to a great extent. Otherwise, as Frosio points out “unsupervised AI pervasiveness has the capacity to lower dramatically human rights standards online.”⁹⁵⁸ This means that the lack of supervision of algorithmic enforcement might encroach upon fundamental rights of users such as the right to freedom of expression and information and thus lead to censorship. Further elaboration on the nature of this authority is discussed in chapter 6 where the principles and main functions of the proposed hosting ISSP supervisory authority are set out.

However, apart from the right to explanation that internet users should have towards the removal of their material and the possibility of a partial disclosure of the algorithms that hosting ISSPs use in order to remove material from their networks to a proposed hosting ISSP supervisory authority, it could be argued that another type of a transparency

⁹⁵⁵ F. Pasquale, “Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries” (2014) 104 *Northwestern University Law Review* 173.

⁹⁵⁶ *Ibid.*

⁹⁵⁷ T. Harford, “Algorithms judge us so know their rules” (*Financial Times*, 22 November 2019) is available at <<https://www.ft.com/content/e155f91a-0b86-11ea-b2d6-9bf4d1957a67>> last accessed 26 December 2019.

⁹⁵⁸ G. Frosio, “Algorithmic enforcement online” in P. Torremans (ed.), *Intellectual Property and Human Rights* (4th edition, Kluwer Law International forthcoming 2020) 33.

obligation could be adopted at operational level of hosting ISSPs, namely the terms of service of hosting ISSPs.

B. Operational transparency

The terms of service of hosting ISSPs usually make users aware of the practices that they adopt towards their subscribers. These terms of services give online users the opportunity to submit a counter-notification for the removal of the content that users have uploaded. For instance, YouTube gives the opportunity to its users to submit a counter-notification when their content has been removed.⁹⁵⁹

However, this does not mean that every hosting ISSP gives this opportunity to its subscribers or, if it is offered, it might cover different kinds of material. For example, in a survey conducted by a non-profit online censorship organization found that Instagram and Facebook offer a counter-notification option only in cases where the profile of the user has been removed.⁹⁶⁰ On the other hand, Twitter offers the possibility for counter-notification to any form of removal,⁹⁶¹ while Google, following the right to be forgotten case,⁹⁶² implemented a particular content removal request at the bottom of its search listings results.⁹⁶³

By introducing a right to counter-notify the erroneous removal of content, internet users would be offered the appropriate legal remedy to claim their legal rights. The right to have the appropriate remedy is explicitly included in Article 47 of the EU Charter of Fundamental Rights.

However, the right of internet users for a counter-notification might lack essence if it is not accompanied by a notification sent to internet users when their content has been removed. The importance of notifying the affected parties of a dispute is not a novelty since it has already been endorsed at judicial level. For instance, with regard to blocking injunctions, in the *Cartier II* case,⁹⁶⁴ it has been outlined that when a blocking injunction

⁹⁵⁹ <https://support.google.com/youtube/answer/2807684?hl=en-GB>

⁹⁶⁰ Online censorship, "Unfriending censorship: insights from four months of crowdsourced data on social media censorship" (2016) 17 is available at <<https://www.onlinecensorship.org/en/news-and-analysis/44> > last accessed 28 December 2019.

⁹⁶¹ Ibid.

⁹⁶² Case 131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González* [2014] ECR I-000; see also O. Lynskey "Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez" (2015) 78 *Modern Law Review* 522-534.

⁹⁶³ Google, EU Privacy Removal, Personal Information Removal Request Form.

⁹⁶⁴ *Cartier v BskyB* (2014) EWHC 3354 (Ch).

is ordered, the blocking website shall not just note that this specific site is blocked. Rather, it shall give information on the parties that requested the blocking injunction and provide further information on affected internet users who wish to challenge the order.⁹⁶⁵ In a similar fashion, in the *FAPL v BT* case, which was about a live blocking order,⁹⁶⁶ it was deemed that a notification shall be sent to hosting providers each week when their IP address is blocked as well as to subscribers of the providers in case they wish to challenge the blocking order.

This understanding implies that a transparency obligation at operational level of hosting ISSPs shall not restrict appeal mechanisms in cases of counter-notifications. Rather it shall also cover users' notifications upon the take down of their content by hosting ISSPs. This view stems from Article 6 (1) of the European Convention of Human Rights and Article 47 of the EU Charter of Fundamental Rights. Both Articles address the right to a fair trial and a right to the appropriate remedy or more informally the equality of arms. The equality of arms has been described by Rubenstein as ““whether parties are equally equipped to engage to adversarial adjudicatory procedures.”⁹⁶⁷ This implies that each party in a dispute shall be granted the same rights and not be placed in a disadvantageous position against the other party. In the case of hosting ISSPs, this means that users shall be informed that their material has been removed and thus can seek a recourse of their rights. In doing so, users will be aware that their material has been removed and could thus challenge the decision.⁹⁶⁸ Therefore, an effective review system, as Kaleda refers to it, will come to the forefront and safeguard internet users' rights.⁹⁶⁹ Otherwise, procedural users' rights will be jeopardised and, since the material would remain hidden, users' rights to impart information and prevent other users from accessing it would be impeded.

This understanding excludes the belief that a transparency obligation with regard to the terms of services of hosting ISSPs amounts to a detailed exposition of terms and conditions of the operation of hosting ISSPs. This would be impossible and without any practical sense. For example, it has been reported that most users do not read the terms and conditions when they subscribe to an online service. For example, a study conducted

⁹⁶⁵ *Cartier v BskyB* (2014) EWHC 3354 (Ch) 264.

⁹⁶⁶ *FAPL v BT* (2017) EWHC 27.

⁹⁶⁷ W. Rubenstein, “The concept of equality of in civil procedure” (2002) 23 *Cardozo Law Review* 1868.

⁹⁶⁸ D. Citron, “Technological Due Process” (2008) 85 *Washington University Law Review* 1253-1254 where Citron notes that “Inadequate notice will discourage some people from seeking hearing.”

⁹⁶⁹ S. Kaleda, “The role of the principle of effective judicial protection in relation to website blocking injunctions” (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 7.

by Ben-Shahar and Schneider found that the length of terms and conditions discourage internet users from reading them while the linguistic complexity of terms and conditions is not understandable by internet users at all.⁹⁷⁰ Therefore, it seems that including all the decision-making processes and full details about the terms under which hosting ISSPs operate might not be beneficial to users.

From a policy perspective, the adoption of appeal mechanisms and users' notifications have been supported by a wide number of sectors. For instance, the EU Commission has introduced several recommendations with regard to transparency in online platforms in its recently issued Recommendation on battling illegal online content. In particular, the European policymakers outlined that there is a need to adopt an appeal mechanism and notify users as a matter of transparent procedures hosting ISSPs must adopt.⁹⁷¹ Similarly, the Recommendation of the Council of Europe on the promotion of respect for freedom of expression and information with regard to internet filters has pointed out that in cases where filtering-based technologies are deployed, "effective and readily accessible means of recourse and remedy" shall be provided to internet users.⁹⁷² Likewise, another Recommendation of the Council of Europe in the field of media and information society notes the need to "ensure that internet users have access to effective remedies when their rights and freedoms have been restricted or when they believe that their rights have been violated."⁹⁷³ In addition, at UK level, the Select Committee on Communications of the House of Lords is in favour of adopting transparent procedures with regard to counter-

⁹⁷⁰ O. Ben-Shahar O and C. E. Schneider, "The Failure of Mandated Disclosure" (2011) 159 University of Pennsylvania Law Review 647 where the authors found that "...when mandates are too detailed, both disclosers and disclosees have trouble. Forms become so long and elaborate that disclosers have problems assembling and organizing the information, and disclosees do not read them and cannot understand, assimilate, and analyze the avalanche of information."; see also F. Marotta-Wurgler, "Will Increased Disclosure Help? Evaluating the Recommendations of the ALI's 'Principles of the Law of Software Contracts'" (2014) 78 University of Chicago Law Review 172.

⁹⁷¹ *FAPL v BT* (2017) EWHC 480 Ch. (27).

⁹⁷² Committee of Ministers, "Recommendation to member states on measures to promote the respect for freedom of expression and information with regard to internet filters" CM/ Rec (2008) is available at <https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805d3bc4> last accessed 28 December 2019.

⁹⁷³ Committee of Ministers, "Recommendations in the field of media and information society Media and Internet Division" (2015) is available at <<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44>> last accessed 28 December 2019.

notification procedures for internet users whose material has been erroneously taken down.⁹⁷⁴

Such a stance has been maintained by Frank La Rue, the UN Rapporteur on the promotion and protection of the right to freedom of opinion and expression in his report of April 2018. La Rue criticized the lack of transparent procedures in relation to the removal of content online. More specifically, he stressed that transparency and notifications to users are directly correlated.⁹⁷⁵ This is because, as he explains, operational transparency “alleviates the pressure on notifications in individual cases, while weaker overall transparency increases the likelihood that users will be unable to understand individual removals in the absence of notifications tailored to specific cases.”⁹⁷⁶ Otherwise, users would be unaware of the removal of their content in the first place and they would not be able to challenge it. Along similar lines, in light of the practices that Facebook uses in order to remove terroristic content from its platform, the UN Rapporteur addressed a letter to Facebook’s CEO stressing the need to apply the Guiding Principles on Business and Human Rights that encourage the approach of “respect, protect, remedy”.⁹⁷⁷ In this sense, Facebook shall notify its users after their content has been removed and offer them the appropriate procedural safeguards to contest the removal.⁹⁷⁸

Lastly, this view has been echoed by prominent voices in academic scholarship who outline the need for sending notifications to users after their content is removed. In particular, De Gregorio recommends a human rights approach towards the removal of content online.⁹⁷⁹ Such an approach, he argues, should include notification to users, along with the opportunity for them to appeal the decision. This approach should be introduced

⁹⁷⁴ British and Irish Legal Education and Technology Association, “Written evidence submitted for the House of Lords, Select Committee on Communications, “The internet: To Regulate or Not to Regulate? Summary of Response” (2018) 1.

⁹⁷⁵ EU Commission, “Recommendation of 1.3.2018 on measures to effectively tackle illegal content online Brussels” COM (2018) 1177 final.

⁹⁷⁶ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (6 April 2018) 13.

⁹⁷⁷ Guiding Principles on Business and Human Rights on Implementing the United Nations “Protect, Respect and Remedy Framework” is available at <https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf> last accessed 28 December 2019.

⁹⁷⁸ Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2018) 7.

⁹⁷⁹ G. De Gregorio, “Expressions on Platforms: Freedom of Expression and ISP liability in the European Digital Single Market” (2018) CoRe 214.

on a mandatory basis. In similar fashion, Riordan⁹⁸⁰ and Kaleda,⁹⁸¹ in the context of a blocking injunction, explain that it has been observed that many users are not aware that specific websites are blocked. For this reason, they argue that a notice to individual users or at least a general notice would enhance their awareness towards the reasons that trigger the blocking of the site as well as the review process.

On the basis of the above, a transparency obligation at operational level of hosting ISSPs would address an effective review mechanism. Such mechanism shall include users' notification as well as the appropriate appeal mechanisms to contest the decision of hosting ISSPs with regard to the removal of their content. In this way, internet users' rights would be safeguarded, and potential abuses would be mitigated.

C. *Transparency reports*

Finally, another context where transparency should be applicable can be found in transparency reports. Transparency reports are already issued on a voluntary basis from a handful of hosting ISSPs while European policy makers have also stressed the mandatory need for issuing transparency reports.

Google was the first to introduce transparency reports in September 2010.⁹⁸² Following Google's reports, a handful of hosting ISSPs followed suit in response to the requests they receive in order to remove content from their platforms.⁹⁸³ Likewise, at policy level, a number of European documents have also reinforced the need for issuing transparency reports. For instance, the Communication on tackling illegal content online notes that hosting ISSPs "should publish transparency reports with sufficiently detailed information on the number and type of notices received and actions taken, as well as the time taken for processing, and the source of the notification."⁹⁸⁴ What is more, at legislative level, Germany is the first European member state that has issued a special Law for Social Media

⁹⁸⁰ J. Riordan, *The liability of internet intermediaries* (Oxford University Press 2016) 457-458.

⁹⁸¹ S. Kaleda, "The role of the principle of effective judicial protection in relation to website blocking injunctions" (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 7.

⁹⁸² Global Information Society Watch, "The internet and corruption: Transparency and accountability online" (2012) 26.

⁹⁸³ A. Holland and others, "NOC online intermediaries case studies series: intermediary liability in the United States" (18 February 2015) Berkman Center for Internet and Society 60; J. Urban, J. Karaganis and B. Schofield, "Notice and Takedown in everyday practice" (2017) *Berkley Law* 9.

⁹⁸⁴ EU Commission, "Communication on tackling illegal content online towards an enhanced responsibility of online intermediaries" COM (2017) 555 final 16.

with regard to the removal of unlawful content from their networks.⁹⁸⁵ According to this Law, hosting ISSPs have an obligation to issue transparency reports every six months, entailing number of removal requests and the final removals of illegal content. Lack to comply with the transparency obligation might trigger fines of between 5-10 million euros for hosting ISSPs.

The main idea behind the issue of such transparency reports, as McKinnon reveals, “involves censorship and surveillance carried out not by government agents or Internet police but by the private sector.”⁹⁸⁶ This means that with transparency reports, companies want to communicate to the public the criteria that trigger the removal of online content and defend themselves against potential criticism. Such criticism relies on thorny issues of censoring content online and overseeing internet users’ activities. While the matter of surveillance is out of the scope of this research, the issue of censoring content is one of the central matters of this research. For instance, a number of civil society organizations, such as Open Rights Group, argue that hosting ISSPs tend to overzealously block material in order to exonerate themselves from liability under the safe harbour provisions of the ECD.⁹⁸⁷

To tackle this criticism, hosting ISSPs include in their transparency reports more information about the removal of the content. For instance, they specify the reasons that generate the removal of the material and, in particular, whether it was for issues related to copyright, hate speech, nudism or violation of community standards. In addition, they include information about who made this request, for instance, whether it is a private or governmental request. In this way, internet users’ trust towards the services hosting ISSPs offer is reinforced.⁹⁸⁸

However, the issue of transparency reports might not only promote users’ trust towards the online services. Indeed, transparency reports would enable a proposed hosting ISSP supervisory authority, which is discussed in chapter 6, to oversee the right functioning of hosting ISSPs’ operation. As already seen in chapter 3, hosting ISSP’s role nowadays is not

⁹⁸⁵ Bundesministerium der Justiz and fuer Verbraucherschutz, *Netzwerkungsdurchgesetz* is available at <<https://www.bmjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html>> last accessed 28 November 2019.

⁹⁸⁶ R. McKinnon, *Consent of the Networked: The Worldwide struggle for Internet Freedom* (2012) 210.

⁹⁸⁷ Open Rights Group, *Web Blocking* is available at <<https://www.openrightsgroup.org/issues/web-blocking>> last accessed 28 December 2019.

⁹⁸⁸ A. Holland and others, “NOC online intermediaries case studies series: intermediary liability in the United States” (18 February 2015) Berkman Center for Internet and Society 63.

restricted to the role of an intermediary. Rather, hosting ISSPs enforce intellectual property rights and shape our information environment. The majority of consumers rely on their e-commerce services in order to purchase goods. Given that the activities of hosting ISSPs directly affect right holders and internet users, the issue of transparency reports would enable their compliance with the existing legal provisions and the rule of law.

Yet, it could be argued that a mandatory issuing of transparency reports would not receive a warm welcome from the majority of hosting ISSPs. Indeed, hosting ISSPs claim that the mandatory publication of transparency reports will place an additional burden on hosting ISSPs since such reports may increase their transaction costs.⁹⁸⁹ This means that hosting ISSPs might need to engage a higher number of human labour resources in order to formulate such reports as well as additional employees to manage the system. In this way, hosting ISSPs with higher revenues would be able to issue such reports, whereas new entrants on the market might face difficulties to issue such reports annually.

In the light of this discrepancy, this thesis argues for the issue of transparency reports for companies with a certain annual turnover. To attribute responsibilities to hosting ISSPs according to their size is not a novelty at European level.⁹⁹⁰ Supporting this argument, Article 17 of the DSMD addresses OCSSPs that host large amounts of content.⁹⁹¹ Although it lacks clarity, this Article implies that filtering mechanisms should be deployed from those hosting ISSPs which enable the dissemination of a large amount of content such as the GAFA group.⁹⁹² Along similar lines, the compromised text from the EU Parliament excludes from the adoption of a filtering mechanism those hosting ISSPs that have less than €10M annual turnover and employ fewer than 50 employees.⁹⁹³

⁹⁸⁹ J. Urban, J. Karaganis and B. Schofield, "Notice and Takedown in everyday practice" (2017) Berkley Law 50.

⁹⁹⁰ C. Angelopoulos, "EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability Capsizes into Incoherence" (Kluwer copyright blog, 6 October 2016) is available at <<http://copyrightblog.kluweriplaw.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/>> last accessed 28 December 2019.

⁹⁹¹ Council Directive 2019/790/EC 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 (Text with EEA relevance) PE/51/2019/REV/1, OJ L 130, 17.5.2019 (hereinafter DSMD).

⁹⁹² C. Angelopoulos, "EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability Capsizes into Incoherence" (Kluwer copyright blog, 6 October 2016) is available at <<http://copyrightblog.kluweriplaw.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/>> last accessed 28 December 2019; GAFA: Google, Amazon, Facebook, Apple.

⁹⁹³ J. Reda, "Article 13 is back on – and it got worse, not better" (Reda's website, 5 February 2019) is available at <<https://juliareda.eu/2019/02/article-13-worse/>> last accessed 30 December 2019.

However, other critical voices against the issue of transparency reports argue that they might meet with criticism from civil society organizations and associations for the enforcement of rights online. This is because the reports would reveal the internal mechanisms hosting ISSPs adopt in order to take down material from the platforms. It is these internal mechanisms that might generate criticism towards hosting ISSPs' practices. Such criticism could address the thresholds of unlawfulness that should be embedded into a work or different view as to how ISSPs should handle notices for copyright infringements. This understanding may lead to an influx of notices from right holders to hosting ISSPs. Given that right holders would know now the thresholds of illegality that triggers the removal of the content, they could send notifications for removal to hosting ISSPs. Yet, this understanding might have a dual effect. On the one hand, if hosting ISSPs removed the allegedly infringing material upon receiving notification, right holders would be satisfied. On the other hand, if hosting ISSPs did not respond or ignored the notices from right holders, there would be a high risk of lawsuits against hosting ISSPs.⁹⁹⁴ This is mainly because right holders would be aware of the instances where hosting ISSPs did not comply with the procedures.

Yet, this pitfall could be eliminated by applying a different level of transparency to this kind of report. This means that a detailed explanation of the internal procedures would amount to citing copyright removals depending on countries who requested them and what were the thresholds of unlawfulness. This type of concern has emerged in light of all the transparency reports issued by hosting ISSPs nowadays on a voluntary basis. On closer examination, it can be observed that the great majority of reports do not indicate the country from which the request has been sent.⁹⁹⁵ For example, Twitter refrains from specifying the country of origin of the request,⁹⁹⁶ as do Facebook,⁹⁹⁷ and YouTube.⁹⁹⁸ This information is valuable since it enables rights holders to assess whether hosting ISSPs' removals abide by the copyright rules. Given copyright standards vary from country to country, sometimes the requirements for a work to constitute a parody in the UK differ from the requirements for that work to be considered as a parody in the Greek legal

⁹⁹⁴ J. Urban, J. Karaganis and B. Schofield, "Notice and Takedown in everyday practice" (2017) Berkley Law 50

⁹⁹⁵ Global Information Society Watch, "The Internet and corruption: Transparency and accountability online" (2012) 26.

⁹⁹⁶ <https://transparency.twitter.com/en/copyright-notice.html>

⁹⁹⁷ <https://transparency.facebook.com/>

⁹⁹⁸ <https://transparencyreport.google.com/copyright/overview?hl=en>

system.⁹⁹⁹ This means that a right holder could more easily assess whether the removal of the specific content in this jurisdiction complied with the national legislation.

Overall, it could be extrapolated that different contexts require different levels of transparency. This is because, as discussed earlier, one single type of transparency would not accommodate the different interests at stake, namely the interests of hosting ISSPs, right holders and internet users. For instance, if full transparency was applicable to algorithms, hosting ISSPs' business welfare would be endangered while at the same time it would not be beneficial to average unskilled users. In contrast, it is only highly skilled users, potential hackers or competitors of a hosting ISSP that could benefit from the disclosure of the full algorithm. Therefore, this thesis argues for two measures to be introduced. Firstly, the introduction of a right to explanation would mean that users can request more information about the removal of their content, and secondly, an authority should be established to audit the algorithms that hosting ISSPs use. Another context where a transparency obligation should be applicable is the terms of service of hosting ISSPs. In this case, this thesis argues that hosting ISSPs should be compelled to notify users after their content has been removed and offer the appropriate counter-notification procedures so that users can appeal hosting ISSPs' decisions. In this way, fundamental rights such as the right to a fair trial and the right to appropriate remedy would be respected. Finally, a transparency obligation would amount to the issue of transparency reports. Such transparency reports would not include internal technical procedures of hosting ISSPs, thus preventing users from being able to circumvent them. Rather, they would include a list of removals related to copyright or trade mark classified per country and the specific reasons that lead to the removal of the content. Subsequently, users would be aware of the requests that had originated from each country and the reasons that triggered the removal or non-removal of their content.

V. Conclusion

This chapter has engaged in a critical discussion to endorse a statutory transparency obligation for hosting ISSPs. This is because, as discussed in Section III of this chapter, from a normative perspective, a transparency obligation would promote the rule of law. For instance, it would give users information about the content management policies that hosting ISSPs follow. Therefore, users would be able to observe whether the hosting ISSP

⁹⁹⁹<https://www.copyrightuser.org/understand/exceptions/parody-pastiche/>

abide by the rules and either justify or challenge the decision. The non-disclosure of information about the conditions that lead to the removal of content would undermine the rule of law and the principle of due process. This is because internet users would be deprived of the right to effective remedy and the right to a fair trial as enshrined in the EU Charter of Fundamental Rights and European Convention of Human Rights respectively.

Further, the imposition of a transparency obligation would warrant the legitimacy of hosting ISSPs' activities and thus enhance confidence for e-commerce services to online consumers. This is because transparency users would be aware of the thresholds that generated the removal of their material. Without disclosing the thresholds that generated the removal of the content, users would have doubts about the conditions that led to their material being removed and this would call into question the legitimate basis of this removal.

Apart from enhancing important democratic values, a transparency obligation would have a positive impact on transactions between hosting ISSPs and consumers. This is because it would curb the existing information asymmetries. This understanding finds applicability mainly in the trade mark context where transactions between consumers and online auction platforms take place. In particular, with a transparency obligation, consumers in the online world would have more information about the goods that are displayed online and therefore, their trust in the online services would be enhanced.

However, the introduction of a transparency obligation would not only safeguard users' rights but also induce hosting ISSPs to adopt better practices. Under the fear of being disgraced or publicly criticized about their methods, hosting ISSPs would be induced to undertake a prior assessment of their practices before they put them into practice and observe their outcomes. In this way, it is possible to argue that transparency would mitigate any errors or malfunctions and thus improve the principles of good governance.

It should be noted that, given that "different contexts require different levels of transparency",¹⁰⁰⁰ such a transparency obligation should be shaped accordingly. For instance, if the algorithms that hosting ISSPs use were fully disclosed, the competitors of

¹⁰⁰⁰ R. Caplan, J. Donovan, L. Hanson and J. Matthews, "Algorithmic Accountability: A primer" (2018) 7 is available at <https://datasociety.net/output/algorithmic-accountability-a-primer/> last accessed 28 December 2019.

hosting ISSPs along with potential hackers might either copy or more easily circumvent them. As a corollary, if the competitors of a hosting ISSP copy its algorithm, then the hosting ISSP might lose its competitive edge. Further, if potential hackers manage to more easily circumvent the algorithm, its business model and thus its credibility would be in serious doubt.

Therefore, this thesis argues for the introduction of a right to explanation so that users can request more information about the decision-making process of hosting ISSPs. At the same time, the algorithms would only be disclosed in front of the previously proposed hosting ISSP supervisory authority that would control its proper operation.

Another context to which a transparency obligation should apply are the terms of services of hosting ISSPs. For instance, by notifying the users when their content has been removed as well as provide them with counter-notification mechanisms would enhance users' fundamental rights such as the right to fair trial and the right to appropriate remedy.

Finally, a transparency obligation should include the issue of transparency reports. Such transparency reports would refrain from including internal technical procedures that hosting ISSPs use in order to remove material from their networks. Rather, these transparency reports would include a list of removals for copyright and trade mark violations per country and the reasons that warrant such a removal. In this way, users would be aware of which requests come from a specific country, the reasons that justified their removal and thus their trust in the hosting ISSP would be enhanced. These transparency reports would also enable the proposed hosting ISSP supervisory authority to check the operation of hosting ISSPs and assess the compliance of their practice with the existing rule.

In this light, the following chapter engages with the proposed hosting ISSP supervisory authority and in particular, it discusses the normative considerations for the proposed hosting ISSP supervisory authority as well as the principles and functions of the proposed hosting ISSP supervisory authority.

Chapter 6: Towards a hosting ISSP supervisory authority

I. Introduction

As elaborated in chapters 4 and 5, within the proposed responsibility framework based on co-regulation hosting ISSPs shall be assigned with a set of responsibilities. Such proposed responsibilities shall focus on curbing the growth of online infringements while at the same time they shall respect the fundamental rights of internet users. For instance, it was suggested in chapter 4 that hosting ISSPs should have a duty of care towards the unlawful content or counterfeit goods that are disseminated within their networks while at the same time, as discussed in chapter 5, they should have a transparency obligation towards their users with regard to the removal of the content they host and the goods that they circulate within their networks.

As discussed in chapter 4, the proposed responsibility framework shall be based on a co-regulation scheme. Drawing upon the Internet regulatory theories of Reidenberg and Lessig, a co-regulatory regime implies a state interference to regulate internet users' actions via hosting ISSPs. It is this state interference that could be illustrated in the establishment of a hosting ISSP supervisory authority to which hosting ISSPs shall be accountable.¹⁰⁰¹

The idea of a supervisory authority has already been exemplified at policy and scholarship level. For instance, it could be traced in Article 17 (9) of the DSMD that envisages the creation of a mechanism whose main purpose is to deal with users' complaints: "Member States shall also ensure that out-of-court redress mechanisms are available for the

¹⁰⁰¹ R. J. Barcel and K. Koelman, "Intermediary liability in the E-Commerce Directive: so far so good, but it's not enough" (2000) 16 Computer Law and Security Report 237; M. Bunting, "Keeping Consumers Safe Online Legislating for platform accountability for online content" (2018) Communications Chambers 33; K. Garstka, "Looking above and beyond the blunt expectation: specified request as the recommended approach to intermediary liability in cyberspace" (2016) 7 European Journal of Law and Technology 15; M. Tessier, J. Herzog and L. Madzou, "Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and how they regulate us* (2018) 182 -183; S. Jacques and K. Garstka, "Automated anti-piracy systems: A call for further evidence-based policies" (Kluwer copyright blog, 4 April 2019) is available at <<http://copyrightblog.kluweriplaw.com/2019/04/04/automated-anti-piracy-systems-a-call-for-further-evidence-based-policies/>> last accessed 27 December 2019; E. Laidlaw, "Private Power, Public Interest: An Examination of Search Engine Accountability" (2009) 17 International Journal of Law and Information Technology 141.

settlement of disputes”.¹⁰⁰² The creation of such a body has also been discussed in the course of the whole legislative process of drafting this Directive. The EU Council’s compromised text noted in Article 13 (7) that “Member States shall endeavor to put in place independent bodies to assess complaints related to the application of the measures”¹⁰⁰³ while in similar terms the EU Parliament’s compromised text Article 13 (2b) noted that “Member States shall ensure that users have access to an independent body for the resolution of disputes...”¹⁰⁰⁴

Apart from the DSMD that requires the establishment of an independent body that handles emerging disputes online, initiatives or suggestions for creating independent bodies that deal with disputes either between hosting ISSPs and online users, or between hosting ISSPs and right holders, have been witnessed at national level in member states¹⁰⁰⁵ or recommended through empirical studies by academic scholarship respectively.¹⁰⁰⁶

¹⁰⁰² Council Directive (EC) 2019/790/EC 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 (Text with EEA relevance) PE/51/2019/REV/1, OJ L 130 (hereinafter DSMD).

¹⁰⁰³ EU Council, Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market - Agreed negotiating mandate, Interinstitutional File: 2016/0280 (COD).

¹⁰⁰⁴ EU Parliament, P8_TA-Prov (2018) 0337, Copyright in the Digital Single Market, Amendments adopted by the European Parliament on 12 September 2018 on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market (COM (2016) 0593- C8-0383/2016- 2016/0280 (COD)).

¹⁰⁰⁵ In France, there is a proposal for new legislation based on co-regulation, Mission report, “Creating a French framework to make social media platforms more accountable: acting in France with a European vision” (May 2019); In the UK, HM Government, “Online Harms (White Paper)” (April 2019) 57; In Germany, Bundesministerium der Justiz und fuer Verbraucherschutz, Netzwerkdurchsetzungsgesetz is available at <<https://www.bmjjv.de/SharedDocs/FAQ/EN/NetzDG/NetzDG.html>> last accessed 28 December 2019; EU Parliament, “Legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online” (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)); Council Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (2018) OJ L 303.

¹⁰⁰⁶ M. Tessier, J. Herzog and L. Madzou, “Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness” in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility*, United Nations Internet Governance Forum Geneva (December 2017) 182; “UK Gov Aim to Make ISP Piracy Website Blocks Cheaper and Easier “ (ISP review, 15 June 2018) is available at <<https://www.ispreview.co.uk/index.php/2018/06/uk-gov-to-make-isp-piracy-website-blocks-cheaper-and-easier.html>> last accessed 28 December 2019; L. Edwards suggests the appointment of “An Ombudsman able to get remedies for users” in Edwards L, “With Great Power Comes Great Responsibility? The Rise of Platform Liability” in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 289; K. Garstka, “Guiding the Blind Bloodhounds: How to Mitigate the Risks art. 17 of Directive 2019/790 poses to the Freedom of Expression” in P. Torremans (ed.), *Intellectual Property and Human Rights* (Kluwer Law and Business 2020); M. Vermeulen, “Online content: to regulate or not to regulate- is that the question?” (2019) Association for progressive communications 10-11; S. Kulk, *Internet Intermediaries and Copyright Law: EU and US perspective* (Kluwer Law International 2019) 305.

Against this background, this chapter, explores the underlying needs for establishing a supervisory authority for hosting ISSPs with regard to copyright and trade mark infringements that accrue within their networks. In particular, it discusses the normative considerations of introducing such an authority, the scope of the proposed authority as well as the principles and functions under which it would operate.

II. Normative considerations for the proposed hosting ISSP supervisory authority

Although a co-regulatory approach is not common in the field of Intellectual Property Law, there is a plethora of reasons that would justify the establishment of a hosting ISSP supervisory authority.

Firstly, the creation of a hosting ISSP authority for copyright and trade mark infringements would enhance legal certainty among right holders, hosting ISSPs and internet users. This is because, as discussed in chapter 2, the current legal legislative framework under the ECD seems outdated. This is mainly due to the lack of harmonisation of secondary liability rules at European level along with the different interpretations of Article 14 of the ECD. What is more, as my findings indicate, the current legal framework under the DSMD is controversial since it entails an array of problematic aspects that aggravate the existing legal uncertainty which has already been triggered by the ECD. As a corollary of this framework, right holders are unsure about the protection of their rights and hosting ISSPs are not sure of the specific conditions under which they could evade liability. For this reason, to hold hosting ISSPs to account to a hosting ISSP supervisory authority for fulfilling specific obligations would provide a more robust legal framework for right holders and hosting ISSPs respectively. Indeed, Hugenholtz has pointed out that in cases where fundamental rights come to forefront, only clear and codified legal provisions may not only safeguard rights holders' interests but also promote internet users' rights to freedom of expression and personal data.¹⁰⁰⁷ Yet, this does not mean that users or right holders should not seek redress in front of the courts. The establishment of a hosting ISSP supervisory authority should be applied without prejudice to the fundamental right of

¹⁰⁰⁷ P. B. Hugenholtz, "Codes of Conduct and Copyright enforcement in cyberspace" in I. Stamatoudi (ed.), *Copyright enforcement and the internet* (Kluwer Law International 2010) 320.

internet users and right holders to resort to the courts' legal arena when their rights have been violated.¹⁰⁰⁸

The establishment of a hosting ISSP supervisory authority would not only enhance legal certainty to rights holders but also to hosting ISSPs. As mentioned above, due to the outdated legal framework under the ECD along with the controversial regime under the DSMD that was elaborated on in chapters 2 and 3 respectively, the existence of such an authority would promote legal certainty to hosting ISSPs. This understanding would safeguard their right to conduct business as per Article 16 of the EU Charter of Fundamental Rights since hosting ISSPs would be sure of how to adjust their business models in order to comply with the rules. Further, another corollary to the creation of a hosting ISSP supervisory authority is the adoption of more clear rules about the procedures they follow. Finally, to avoid being highly sanctioned for non-compliance with the rules, hosting ISSPs would be forced to deploy even more sophisticated technology so as to mitigate infringements online. Therefore, a hosting ISSP supervisory authority would not only safeguard content owners' and brand owners' rights, but also encourage hosting ISSPs to adopt more efficient practices in order to prevent sanctions.

Secondly, another reason that indicates the need to create a hosting ISSP supervisory authority revolves around the facilitation of internet users' and right holders' access to justice.¹⁰⁰⁹ Access to justice is understood as the access of citizens to judicial redress mechanisms in order to protect their rights. This is because, as explained in chapter 2 and 3, the current legislative framework under the ECD and the DSMD seems to fail to meet the expectations of the parties involved. As Laidlaw points out, there is a risk that the lack of effective judicial redress might lead to internet users turning to hosting ISSPs for complaints.¹⁰¹⁰ Indeed, this understanding was exemplified in Article 17 (9) of the DSMD that dictates that "...Member States shall also ensure that out-of-court redress

¹⁰⁰⁸ As set out in Articles 47-50 of the EU Charter of Fundamental Rights <<https://fra.europa.eu/en/charterpedia/title/vi-justice>> last accessed 28 December 2019.

¹⁰⁰⁹ E. Laidlaw, "Are We Asking Too Much from Defamation Law? Reputation Systems, ADR, Industry Regulation and Other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age: Proposal for Reform" (2017) 6; P. Chapdelaine, "Copyright User Rights and Remedies: An access justice perspective" (2018) Laws 7-10; I. Barral-Vinals, "Enforcing e-consumer protection beyond alternative dispute resolution (ADR): ODR" in J. Devenney and M. Kenny (eds.), *European consumer protection : theory and practice* (Oxford University Press 2012) 88.
Cambridge : Cambridge University Press, 2012.

¹⁰¹⁰ E. Laidlaw, "Are We Asking Too Much from Defamation Law? Reputation Systems, ADR, Industry Regulation and Other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age: Proposal for Reform" (2017) 75.

mechanisms are available for the settlement of disputes. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies.” Yet, as explained in chapter 3, the establishment of dispute resolution mechanisms by hosting ISSPs might prompt reflections on their credibility and thus would not guarantee redress for users whose rights have been infringed. A number of instances that criticize the inadequacy of dispute resolution mechanisms operated by hosting ISSPs can be found in empirical studies and academic scholarship contributions. For instance, a study conducted by Jacques and Garstka on the impact of YouTube on cultural diversity,¹⁰¹¹ found that “the current online creative ecosystem already relies on private agreements reached between right holders and hosting ISSPs at the expense of the wider public.”¹⁰¹² In order to support this finding, they cite the example of the PRS-YouTube deal. PRS for Music is an association that protects songwriters, singers and musicians. The deal between PRS and YouTube states that in case of derogatory use, PRS will send a notification to YouTube and cooperate with the hosting ISSP in order to take down this specific work.¹⁰¹³ Therefore, it might be possible to observe that the dispute resolution mechanisms operated by hosting ISSPs might favor their business interests and exclude users’ right to access justice.

Yet, given there is “no right without a remedy”,¹⁰¹⁴ internet users must be offered an efficient redress mechanism. This role would be played by a hosting ISSP supervisory authority which would serve as a place where users’ complaints would be disposed. Otherwise, internet users’ access to justice might be restricted.

Thirdly, the creation of a hosting ISSP supervisory authority would enhance legitimacy and accountability. This is because the power and legitimacy of a supervisory authority stems from authorized government bodies. This means that the authority is accountable for its

¹⁰¹¹ S. Jacques, K. Garstka and others, “An Empirical Study of the Use of Automated Anti-Piracy Systems and their Consequences for Cultural Diversity” (2018) 15 Scripted 277.

¹⁰¹² Ibid, 308.

¹⁰¹³ Music Business Worldwide, “PRS deal with YouTube: what does it mean for songwriters?” (6 September 2009) is available at <<https://www.musicbusinessworldwide.com/prs-deal-with-youtube-what-does-it-mean-for-songwriters>> last accessed 28 December 2019; Electronic Frontier Foundation considers this as a “fair use massacre” is in S. Mcsherry, “The Fair Use Massacre Continues: Now Warner’s Going After the Babies” (EFF, 12 March 2009) is available at <<https://www.eff.org/deeplinks/2009/03/fair-use-massacre-continues-now-warner-s-going-aft>> last accessed 27 November 2019.

¹⁰¹⁴ Footnote (61.) “It is a settled and invariable principle in the laws of England, that every right when withheld must have a remedy, and every injury it’s [sic] proper redress.” See E. Katsh and O. Rabinovich-Einy, *In Digital Justice: Technology and the Internet of Disputes* (Oxford University Press 2017) 15.

actions or omissions to government actors. In this sense, citizens' rights, such as the freedom of expression or the right to privacy, would be safeguarded. Indeed, with the context of discussing the advantages of co-regulatory approaches, Mardsen has pointed out that co-regulatory approaches address issues of promoting accountability, enhancing legitimacy and respecting human rights in the online world.¹⁰¹⁵

What is more, the creation of a hosting ISSP supervisory authority would ensure the right functioning of the duty of care and the transparency obligation that hosting ISSPs must undertake.¹⁰¹⁶ This is because, within the responsibility framework suggested in this thesis, hosting ISSPs would terminate and prevent upon notification the appearance of online infringements within their platforms.¹⁰¹⁷ However, as seen earlier in chapter 5, a handful of hosting ISSPs prefer to resort to algorithmic enforcement due to the massive scale of content that is transmitted via their networks. How such algorithms operate remains a "black box". For this reason, a number of scholars have suggested that an independent authority could audit the algorithms and identify any flaws which could lead to false removals of content from online platforms.¹⁰¹⁸ As a corollary of this approach, any restriction to users' free speech rights would be eliminated. Further, a hosting ISSP supervisory would make sure that hosting ISSPs exercise controls with regard to the goods that are displayed within their platforms and thus prevent counterfeit goods from reaching end-consumers. In this way, consumers' rights would be safeguarded.

Moreover, another reason that justifies the creation of a hosting ISSP supervisory authority revolves around the promotion of the rule of law. This is because adjudication duties must only be imposed on entities that are authorized by government institutions and act under the principles of independence, proportionality, accountability. This governmental institution could be the hosting ISSP supervisory authority that would reach decisions on issues relating to online copyright and trade mark infringements. Otherwise,

¹⁰¹⁵ C. Mardsen, *Internet co-regulation* (Cambridge University Press 2011) 128.

¹⁰¹⁶ Chapter 6 Section V 1.

¹⁰¹⁷ This understanding has been also exemplified in the report of Committee on Economic and Monetary Affairs on the overview and structure of financial supervision and regulation in the U.S Report of the Committee on Economic and Monetary Affairs on the overview and structure of financial supervision and regulation in the U.S (2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/492470/IPOL_STU%282015%29492470_EN.pdf> last accessed 15 December 2019; In particular, the report points out that the disclosure of practices and mechanisms which the companies adopt will eliminate any risks for non-compliance or any other illegality.

¹⁰¹⁸ F. Pasquale, *Black Box Society: The secret algorithms that control money and information* (Harvard University Press, 2015) 3; F. Romero-Moreno, "Notice and stay down' and social media: amending Article 13 of the Proposed Directive on Copyright" (2018) 33 *International Review of Law, Computers and Technology* 1.

any decision issued by a non-government body might undermine the rule of law. However, it could be argued that the proposed duty of care on hosting ISSPs would amount to adjudicative duties. This is because it is up to the hosting ISSPs to penalize the allegedly infringers either by removing content or even blocking the access of internet users to specific websites.¹⁰¹⁹ Yet, a duty of care is not an adjudication instrument. Conversely, duty of care is an instrument that aims to terminate or at least curb intellectual property violations within hosting ISSPs' networks. It must be seen as a fundamental tool against piracy online. In any case, it would seem ironical to impose adjudicate duties to hosting ISSPs provided that it is mainly their services that accentuated the rates of copyright and trade mark violations online.¹⁰²⁰

Further, another reason that justifies the establishment of a hosting ISSP supervisory authority is the protection of the diversity of the content. Indeed, it has been outlined that the removal of content by hosting ISSPs might endanger the diversity of the content.¹⁰²¹ Considering parodies as a study case, it has been found that content identification technological tools might remove videos that entail parodies of songs since it might face difficulties in identifying them as fair use. In addition, an empirical study conducted by Erikson and Kretschmer raises concern about the skills and knowledge of human moderators that are employed by hosting ISSPs to distinguish between fair use content and infringing content.¹⁰²² Online world facilitates the circulation of content so that end-users from every corner of the world would have access to it. Given that the aim of copyright is to encourage creativity and the dissemination of works,¹⁰²³ a supervisory hosting ISSP authority would guarantee to a greater extent the availability of works online.

Finally, another reason that warrants the creation of a hosting ISSP supervisory authority is the prospect of a higher level of protection for consumers' rights. This is because online consumers seem to be unprotected in cases where they are deceived by retailers selling counterfeit goods online. More specifically, due to the information asymmetry that exists

¹⁰¹⁹ M. Perel and N. Elkin-Koren, "Accountability in algorithmic copyright enforcement" (2016) 19 *Stanford Technology Law Review* 513.

¹⁰²⁰ L. Edwards, "With Great Power Comes Great Responsibility? The Rise of Platform Liability" in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 288.

¹⁰²¹ The diversity of the content includes parodies, political speeches, educational videos, historical documentaries; S. Jacques, K. Garstka and others, "An Empirical Study of the Use of Automated Anti-Piracy Systems and their Consequences for Cultural Diversity" (2018) 15 *Scripted* 308.

¹⁰²² K. Erikson and M. Kretschmer, "Empirical approaches to intermediary liability" (2019) 6 *Create Working Paper* 17.

¹⁰²³ S. Karapapa and L. McDonagh, *Intellectual Property Law* (Oxford University Press 2019) 13-14; T. Cotter, "Some observations on the Law and Economics of Intermediaries" (2005) 1 *Michigan State Law Review* 9.

in online commercial transactions, it seems almost impossible for online consumers to bring legal proceedings against individual traders.¹⁰²⁴ Moreover, due to the limitation of liability clause, online consumers are not contractually entitled to turn to hosting ISSPs for compensation of any losses as a result of purchasing counterfeit goods from online marketplaces. A telling example can be found in eBay's terms and conditions where Section 6 on the Limitation of Liability states that "... We are not liable for any loss of money, goodwill or reputation, or any special, punitive, indirect or consequential damages arising, directly or indirectly, out of your use of or your inability to use our eBay Now Services or the items you purchased through our eBay Now Service. Some jurisdictions do not allow the disclaimer of warranties or exclusion of damages, so the above disclaimers and exclusions may not apply to you."¹⁰²⁵

However, whilst the creation of a hosting ISSP supervisory authority would offer several advantages to all parties at stake, it might suffer from drawbacks. In particular, it has been argued that holding hosting ISSPs accountable to a supervisory authority might increase their transaction costs. In particular, it is likely that hosting ISSPs will have to keep documentation in order to prove compliance with the supervisory authorities. For instance, within the data protection context, the report of the Information Commissioner's Office notes that the new accountability rules will give rise to compliance costs. In particular, it notes that the GDPR "places too much emphasis on compliance paperwork, rather than results."¹⁰²⁶ This is because, as per Article 28 of the General Data Protection Regulation (GDPR),¹⁰²⁷ business corporations are required to keep the necessary documentation so as to prove their compliance with the existing provisions. However, to keep documents, on the one hand does not mean that the organization employs the appropriate technical measures so as to comply with the rules while on the other hand, such documentation might add an extra burden on the hosting ISSPs.¹⁰²⁸

¹⁰²⁴ Although the European Commission's Communication on New Deal for Consumers has announced new measures for protecting online consumers, its suggestions are non-binding.

¹⁰²⁵ eBay terms of service are available at <<https://pages.ebay.com/ebaynow/terms.html>> last accessed 28 December 2019.

¹⁰²⁶ ICO, Documentation <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/>> last accessed 28 December 2018.

¹⁰²⁷ Council Regulation (EC) 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 (2016) O.J. L 119.

¹⁰²⁸ Information Commissioner's Office, Documentation <<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/>> last accessed 28 December 2018.

Although this argument has its own merit, it has to be borne in mind that such a negative effect could be prevented with the adoption of the ‘one stop shop’ principle similar to the data protection framework. In particular, as per the GDPR’s Articles 55-56 the concept of one stop shop has been introduced.¹⁰²⁹ The ‘one stop shop’ principle enables data processors to account for their actions to the data protection authority where the main establishment is regardless of their activities in other member states, thus tempering their compliance costs at a certain extent. In this light, within the intellectual property law context, only the leading supervisory authority would request that the hosting ISSP demonstrates compliance with the requirements as set by existing law. In any case, it is important to outline that keeping documentation in order to prove to the hosting ISSP supervisory authority that a hosting ISSP undertook the set of responsibilities it was assigned with seems a necessary evil in order to comply with the appropriate measures.

Further, the creation of a hosting ISSP supervisory authority that deals exclusively with secondary intellectual property infringements would prove more efficient in terms of tackling copyright and trade mark infringements. The value of this consideration can be understood if one imagines an authority that deals with all types of intellectual property infringements. This means that the authority would address primary as well as secondary intellectual property infringements. However, to add into the scope of a hosting ISSP supervisory authority, primary infringements might prove either inefficient or devoid of legal basis. For instance, it is difficult to identify alleged infringer users since most of the times they hide behind fake IP address or use Virtual Private Networks,¹⁰³⁰ thus making the disclosure of their identities almost impossible.¹⁰³¹ On the other hand, a number of legislative pieces that targeted primary infringer users have failed due to negative criticism. For instance, in 2009, under the mandate of Nicolas Sarkozy, the French Government initiated the Hadopi Law,¹⁰³² according to which users’ identity would be disclosed to right holders if they did not comply with three notices.¹⁰³³ This law received

¹⁰²⁹ Article 29 Data Protection Working Party, “Guidelines for identifying a controller or processor’s lead supervisory authority” adopted on 13 December 2016.

¹⁰³⁰ L. Edwards, “With Great Power Comes Great Responsibility? The Rise of Platform Liability” in L. Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019) 282.

¹⁰³¹ Cited footnote 50 in G.B. Dinwoodie, “A comparative analysis of the secondary liability of online service providers” in G. B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Springer 2016);

¹⁰³² S. Dato, “France drops controversial ‘Hadopi law’ after spending millions: The ‘three strikes’ anti-piracy measure, introduced under Nicolas Sarkozy, would have cut off users’ access to the internet” (The Guardian, 9 July 2013) is available at <<https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy>> last accessed 17 April 2019.

¹⁰³³ P. De Filippi and D. Bourcier, “Three-Strikes’ Response to Copyright Infringement: The Case of Hadopi” in F. Musiani, D. Cogburn, L. DeNardis and N.S. Levinson (eds), *The Turn to Infrastructure in Internet Governance*

severe criticism from civil society organizations that denounced the blatant violation of right to privacy and outlined the lack of legal basis of disclosure of personal details of internet users without a court order.

What is more, with regard to the scope of the proposed hosting ISSPs' supervisory authority, it might be called into question that this authority only addresses copyright and trade mark infringements that accrue in the digital ecosystem. For instance, it could be questioned as to why this hosting ISSP supervisory authority would not deal with other online infringements such as defamation, terroristic content or fake news. As discussed in chapter 1, the scope of this research focuses on copyright and trade mark violations. This is due to the fact that these two types of intellectual property infringements are the most common in the digital ecosystem and their violations have preoccupied at most a handful of courts at European and national level respectively.¹⁰³⁴ Although the option to add into the scope of a hosting ISSP supervisory authority other types of online infringements cannot be precluded, a further examination of this is required. However, given that defamatory comments or fake news or hate speech issues fall outside the scope of this research, this further examination could be the subject for a future research project.

Bearing in mind the above, one might conclude that the creation of a hosting ISSP supervisory authority would safeguard to a greater extent the different interests of the parties involved. In contrast to the current outdated framework under Article 14 of the ECD and the problematic aspects of Article 17 of the DSMD, the creation of a hosting ISSP supervisory authority might offer a more robust legal framework for hosting ISSPs, right holders and internet users; enhancing legal certainty and due process principles.

Having demonstrated the need for introducing a hosting ISSP supervisory authority for copyright and trade mark infringements as well as the scope of such a hosting ISSP supervisory authority, the next question concerns what the principles and functions of this hosting ISSP supervisory authority should be. In order to determine this, the operation of four authorities that have been established in four jurisdictions is explored, namely

(Palgrave-Macmillan 2016); J. Phillips, "Three Strikes.....and then?" (2009) 4 *Journal of Intellectual Property Law and Practice* 521; A. Strowel, "The Graduated response in France: Is it The good reply to online copyright infringements?" in I. Stamatoudi (ed.), *Copyright Enforcement and the Internet* (2010) 147; V. Benabou, "The Chase: The French Insight into the "Three strikes" System" in I. Stamatoudi (ed.), *Copyright Enforcement and the Internet* (2010) 163.

¹⁰³⁴ *L'Oreal v eBay Int'l AG* (2009) EWHC 1094 AT; *eBay Inc v. LVMH* Case 11-10505 (Cour de Cassation of France, 3 May 2012); OLG Düsseldorf, *Rapidshare I*, 27 April 2010, I-20 U 166/09.

Greek,¹⁰³⁵ Italian,¹⁰³⁶ Spanish¹⁰³⁷ and the UK¹⁰³⁸ one. For this reason, their examination can inform this research. However, as is demonstrated in the following section, such authorities are not ideal but would offer a good start upon which a hosting ISSP supervisory authority could build. It should also be noted that the decision to elaborate on the administrative agencies in Greece and Italy is because the one in the UK has not been set up yet while the administrative authority in Spain is recently established and, to my knowledge, it has not issued any decisions yet.

III. Examples of supervisory authorities for copyright and trade mark infringements: not ideal but a good start

A. *Administrative agency in Greece*

Within the context of Intellectual Property Law, a Committee on Internet Violations of Intellectual Property has been established. Pursuant to Article 66 E of the Greek Intellectual Property Law 4481/2017, this Committee operates under the auspices of the Hellenic Copyright Organization and its main duties are to adjudicate private disputes between hosting ISSPs and right holders for the circulation of unlawful material within their networks. Therefore, right holders can file an application to the Committee asking the removal of content that is online without their permission, instead of initiating civil proceeding in courts and requesting blocking injunctions or damages.¹⁰³⁹

The scope of Article 66E (1) of the Greek Intellectual Property Law covers those ISSPs that provide internet access or hosting services, operators of websites, and users that upload

¹⁰³⁵ An analysis of the Greek agency follows.

¹⁰³⁶ An analysis of the Italian agency follows.

¹⁰³⁷ Out of Laws News, "Spain legislates for out-of-court copyright enforcement" ((Out of Law Blog, 29 November 2018) is available at <<https://www.out-law.com/en/articles/2018/november/spain-out-of-court-copyright-enforcement/>> last accessed 28 December 2019.

¹⁰³⁸ ISP Review, "UK Gov Aim to Make ISP Piracy Website Blocks Cheaper and Easier" (ISP review, 15 June 2018) is available at <<https://www.ispreview.co.uk/index.php/2018/06/uk-gov-to-make-isp-piracy-website-blocks-cheaper-and-easier.html>> last accessed 28 December 2019; Interestingly, in the context of online harms, the UK Government has published an initiative that suggests the establishment of a supervisory authority for hosting ISSPs, see more information on HM Government, "Online Harms (White Paper)" (April 2019) 1.

¹⁰³⁹ General information on the Greek Committee on intellectual property violations is available at <<https://www.opi.gr/en/committee/general-information>> last accessed 28 December 2019.

unauthorized material online. However, it does not cover those activities of internet users that download or stream or file-share unauthorized material.¹⁰⁴⁰

In order to seek redress in front of the Committee, the copyright holder must have already notified the hosting ISSP with regard to the infringing content that exists within its platform and the hosting ISSP either has not processed the notification or has dismissed the notification. In this case, the copyright holder can resort to the Committee by filing an application against the specific hosting ISSP. The Committee issues its decision within ten days. If the application is not rejected by the Committee, then the hosting ISSP is obliged to remove the infringing content. In the case of ISSPs that offer internet access, the Committee orders them to terminate the internet access of users to websites unlawful material such as those websites where users can upload or download illegal films. In case of non-compliance with the Committee's decision, a fine between 500- 1000 euros might be imposed.¹⁰⁴¹

In this way, this procedure of the Greek Committee appears to offer advantages to right holders. Firstly, it provides them with a fast redress for their rights that have been violated online. For instance, within ten days right holders will have a negative or positive answer to their application with regard to the infringements of their rights. Secondly, this procedure offers an efficient way for right holders to seek legal protection in case their rights have been infringed. As demonstrated in chapter 2, due to the outdated legal framework of the ECD and its befuddled national implementation, right holders were unsure about the protection of their rights. However, the clear framework that represents this procedure can offer legal certainty to right holders. Thirdly, a representative example of how right holders might appeal this procedure can be mirrored in the 5 decisions that the Committee has issued since its establishment in November 2018. These decisions concern the blocking of websites with unlawful material, which reinforce the view put forward in this thesis that right holders would seek redress for their rights' violations to this new procedure.

¹⁰⁴⁰ Th. Chiou, "Greece: new notice and take down administrative mechanism for online copyright cases now in force"(IPkat, 5 March 2018) <<http://ipkitten.blogspot.com/2018/03/greece-new-notice-and-take-down.html>> last accessed 28 December 2019.

¹⁰⁴¹ Ch. Tsigkou, "Notice and Takedown Procedure under Greek Intellectual Property Law 4481/2017" (2018) JIPITE C 206; Infographique about the complaints procedure for copyright infringements online is available at < https://opi.gr/images/various/infographic_en.jpg> last accessed 28 December 2019.

However, this Committee does not have only advantages. Indeed, several concerns about its scope and its legal basis have been expressed. Firstly, activities such as downloading or peer to peer file-sharing are not included into the scope of this Committee. As explained in chapter 2, there have been many cases that preoccupied national courts with regard to file-sharing. The Pirate Bay saga that has preoccupied courts at national as well as European level is an illustrative example.¹⁰⁴²

Secondly, some scholars have commented on the legitimacy of this Committee. This is because, as Chiou¹⁰⁴³ and Tsigkou¹⁰⁴⁴ state, the creation of this agency does not fulfil the criteria of Greek Administrative Law. In particular, the Committee is not accountable to a higher administrative authority. Such lack of a hierarchical authority may undermine the legitimacy of the decisions issued by this administrative agency as courts could annul the decisions of the Committee since the Committee's structure does not fulfil the requirements of a public administrative body. This understanding seems crucial for the establishment of the recommended supervisory authority. A supervisory independent authority must be accountable to a public administrative institution such as the Ministry of Culture that would oversee its decisions and its activities. Otherwise, the decisions issued by the authority would lack legitimacy and would be very easily challenged by the courts.¹⁰⁴⁵

Nevertheless, it should be borne in mind that this Committee is still at its infancy and there is room for improvements in the near future. In any case, the operation of the Committee has shown positive steps so far.

B. Administrative agency in Italy

Another example of a national administrative authority that deals with copyright violations can be found in the Italian jurisdiction. This authority has been introduced via a Regulation¹⁰⁴⁶ that was issued by the Italian Authority for Communication Industries.

¹⁰⁴² Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456.

¹⁰⁴³ Th. Chiou, "Greece: new notice and take down administrative mechanism for online copyright cases now in force" (IPkat, 5 March 2018) <<http://ipkitten.blogspot.com/2018/03/greece-new-notice-and-take-down.html>> last accessed 21 December 2019.

¹⁰⁴⁴ Ch. Tsigkou, "Notice and Takedown Procedure under Greek Intellectual Property Law 4481/2017" (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 204.

¹⁰⁴⁵ *Ibid.* 205.

¹⁰⁴⁶ Regolamento in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure elettronica e procedure attuative ai sensi del decreto legislativo 9 April 2003, N. 70 is available at <<https://www.agcom.it/documents/10179/0/Documento/b0410f3a-0586-449a-aa99-09ac8824c945>> last accessed 28 December 2019; in English is available at <<http://www.portolano.it/wp->

Article 2 of this Regulation covers activities of those users that upload unauthorized material on the online platforms. Excluded from the scope of the Regulation are individual users as well as peer to peer networks that enable users to exchange illegal files of films or music.¹⁰⁴⁷

Unlike the Greek Committee on intellectual property violations whose legal nature is not clear yet,¹⁰⁴⁸ the Italian Authority for Communication Industries is integrated in the public administrative structure since it is accountable to the Italian Parliament. The Parliament appoints a member of the Authority whose main purpose is to issue decisions relating to removal of unlawful content within the online platforms. In addition, it handles the requests depending on their degree of urgency. More specifically, the Authority examines a request for removal either in 35 working days or in 12 working days. The latter is described as the “fastissimo” process which takes place under certain circumstances such as massive copyright infringements. Further, according to the Regulation, non-compliance fines will be imposed on the internet access providers within three days upon issuing the order. Such fines may vary from 10.000 to 258.000 euros and may be appealed in front of the Italian Administrative Court within 60 days.¹⁰⁴⁹

Similar to the Greek Committee on intellectual property violations, the main purpose of the Italian authority’s procedure is to offer to right holders a “fast” and “user friendly” recourse of right holders whose rights have been infringed.¹⁰⁵⁰ In this light, this authority seems to have success since there have been already a few decisions with regard to the termination of websites’ operation with unlawful material. For example, in the case of www.cineblog-01.net,¹⁰⁵¹ right holders filed two complaints to AGCOM alleging copyright infringements of eleven movies that were made available to a website without their permission. After examining the request, the Italian Authority treated the unlawful

content/uploads/2013/12/English-translation-of-the-IT-Regulation-on-the-copyright.pdf> last accessed 28 December 2019.

¹⁰⁴⁷ Similar to the Greek Committee for intellectual property violations online.

¹⁰⁴⁸ Ch. Tsigkou, “Notice and Takedown Procedure under Greek Intellectual Property Law 4481/2017” (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 204-205.

¹⁰⁴⁹ Andy, “Italian ISPs Say New Copyright Amendment Infringes Human Rights” (Torrentfreak, 27 July 2017) <<https://torrentfreak.com/italian-isps-say-new-copyright-amendment-infringes-human-rights-170728/>> last accessed 21 December 2019.

¹⁰⁵⁰ IPT, “Notice and take down, at last!” (DLA Piper Blog, 31 March 2014) is available at <<https://blogs.dlapiper.com/iptitaly/?p=54587>> last accessed 28 December 2019.

¹⁰⁵¹ Delibera n. 41/14/CSP, Provvedimento ai sensi degli articoli 8, commi 2 e 4, e 9, comma 1, lett. d), del Regolamento in materia di tutela del diritto d’autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del decreto legislativo 9 aprile 2003, n. 70, di cui alla delibera n. 680/13/CONS (Proc. n. 02/DDA/FP).

availability of eleven films as massive infringements and ordered the “fastissimo” process, thus blocking the entire website.¹⁰⁵²

However, despite the advantages this authority might offer to right holders, it has been argued that more clarification in the terms introduced in the Regulation is required. For instance, Article 1 of the Regulation introduces the new concept of ‘the webpage manager’, which is “the information society service provider, other than those referred to in Articles 14, 15 and 16 of the Decree, who, within a website, manages a space where are present digital works or parts thereof or hyperlinks (link or torrent) to the same, also uploaded by third parties.”¹⁰⁵³ This concept is a new term that is not included in the provisions of the ECD and the absence of any clarification or how its concept departs from the existing terminology of ECD and DSMD might create confusion to right holders. What is more, further clarification is required with regard to the threshold that generates the fast or the slow procedure for examining a complaint with regard to the termination of the operation of a website with infringing material.¹⁰⁵⁴

Overall, it was noted at the outset of this section that both administrative agencies aim to offer a fast and efficient recourse to right holders. While a few flaws have been identified, this does not mean that they cannot be seen as a good start upon which the recommended hosting ISSP supervisory authority should be built.

In this regard, the following section articulates the principles the proposed hosting ISSP supervisory authority should entail. Such principles, however, are not a novelty. Existing supervisory authorities at European level in other legal contexts, such as in the Data Protection, Competition Law or Finance Law, operate under the same principles. For this reason, it would be beneficial for this study to draw parallels with those authorities from other fields of law. Yet, it could be argued that a clear distinction should be made here in terms of the scope of a hosting ISSP supervisory authority and the existing Data Protection

¹⁰⁵² A. Belan, “BREAKING NEWS: AGCOM issues the first fastissimo administrative blocking injunction” (IPKat, 24 April 2014) <<http://ipkitten.blogspot.com/2014/04/breaking-news-agcom-issues-first.html>> last accessed 21 December 2019.

¹⁰⁵³ Regolamento in materia di tutela del diritto d’autore sulle reti di comunicazione elettronica e procedure elettronica e procedure attuative ai sensi del decreto legislative 9 April3 2003, N. 70 is available at< <https://www.agcom.it/documents/10179/0/Documento/b0410f3a-0586-449a-aa99-09ac8824c945>> last accessed 28 December 2019.

¹⁰⁵⁴ It has been argued that in the case of www.cineblog-01.net, the blocking of the whole website could prompt serious concerns over censorship as well as the proportionality of the measure in force; Andy, “Italian ISPs Say New Copyright Amendment Infringes Human Rights” (Torrentfreak, 27 July 2017) <<https://torrentfreak.com/italian-isps-say-new-copyright-amendment-infringes-human-rights-170728/>> last accessed 21 December 2019.

or National Competition authorities. This is because it could be viewed that Data Protection authorities or competition law authorities do not have a similar scope of activities with the proposed hosting ISSP supervisory authority. Indeed, a company might bring against the competition authority for anti-competitive behavior and another company may face the scrutiny of the Information Commissioner's Office for engaging into profiling, data breaches. In contrast, a hosting ISSP supervisory authority would deal with copyright and trade mark infringements committed by the users of hosting ISSPs and not hosting ISSPs themselves. The purpose of the following section is to merely outline the principles under which the proposed hosting ISSP supervisory authority should operate and not to analyze the spectrum of its activities.

IV. Principles of the proposed hosting ISSP supervisory authority

The following section suggests a number of principles that could address the operation of the hosting ISSP supervisory authority and the decisions it issues.

A. Independence

The concept of independence would be an important principle for a hosting ISSP supervisory authority. This is because, as explored in chapter 3, the existing mechanisms for dispute resolution that hosting ISSPs adopt might be under the pressure of the major copyright industry representatives. In this sense, they might favor their own interests and subordinate the interest of users, consumers and smaller right holders.

This ascription of an independent status to an authority has already been widely applicable in a handful of authorities at European level. Consider, for instance, the recommendations of the EU Commission to national member states when they were establishing competition law and data protection law authorities. For instance, in 2014 in the context of the European Semester, the EU Commission made a recommendation to Spain to establish a competition law authority that is "effective, autonomous and independent."¹⁰⁵⁵ In a similar fashion, within the Data Protection framework, Article 52 of the GDPR dictates that each national supervisory authority shall perform its duties and make decisions independently.¹⁰⁵⁶

¹⁰⁵⁵ G. Monti, "Independence, interdependence and legitimacy: the EU Commission, National Competition Authorities, and the European Competition Network" (2014) Working Papers 3.

¹⁰⁵⁶ Article 52 (1) (2) GDPR states that "Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

Scholars have identified two kinds of independence, the formal and the actual independence.¹⁰⁵⁷ On the one hand, formal independence concerns the legal provisions that guarantee the independent function of the supervisory authority.¹⁰⁵⁸ This means that in order to safeguard the independence of an authority, statutory legal provisions must prescribe its independent status.¹⁰⁵⁹ This is illustrated in the case of cartels in competition law context. Cartel is a practice among companies which is illegal and thus prohibited by European Competition Law.¹⁰⁶⁰ Lack of legal provisions that safeguard the independence of the authority that oversees and imposes sanctions would lead to fragmented situations such as countries where cartel is highly sanctioned and countries where cartel practice is tolerated.¹⁰⁶¹ Having been documented in statutory provisions, the independent status of competition law authorities has enabled the authorities to act and issue decisions taking into consideration the existing legal framework.

On the other hand, actual independence amounts to the way the supervisory authority accomplishes its duties and mainly stems from the interaction between the authority and the external stakeholders or governmental bodies.¹⁰⁶² As the OECD report on the Governance of regulators points out, actual independence is achieved through “an appropriate working relationship with government and other stakeholders.”¹⁰⁶³ This is because the way under which the decisions are issued is also contingent upon the members who issue such decisions. This includes, among others, the degree of independence those members have from political actors or relevant stakeholders when a decision is made.

Further, personal independence of the staff employed in the authority also falls within the scope of actual independence. In *Commission v Hungary*,¹⁰⁶⁴ the Hungarian

The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.”

¹⁰⁵⁷ S. Alves, J. Capiu and A. Sinclair, “Principles for the Independence of Competition Authorities” (2015) 11 Competition Law Journal 15-16.

¹⁰⁵⁸ Ibid.

¹⁰⁵⁹ C. Hanretty and C. Koop, “Shall the law set them free? The formal and actual independence of regulatory agencies” (2012) 7 Regulation and Governance 3.

¹⁰⁶⁰ European Commission, Competition, Cartels <http://ec.europa.eu/competition/cartels/overview/index_en.html> last accessed 28 December 2019.

¹⁰⁶¹ A. M. Mateus, “Why should National Competition Authorities be Independent and how should they be Accountable?” (2007) 3 European Competition Journal 21.

¹⁰⁶² S. Alves, J. Capiu and A. Sinclair, “Principles for the Independence of Competition Authorities” (2015) Competition Law Journal 16.

¹⁰⁶³ OECD, “The Governance of Regulators” (2014) OECD Best Practice Principles for Regulatory Policy.

¹⁰⁶⁴ C-288/12- *Commission v Hungary*.

Commissioner was dismissed before the completion of his six-year mandate due to actions undertaken by the Hungarian Government, aiming at the replacement of all Data Protection's members.¹⁰⁶⁵ In response, the EU Commission initiated legal proceedings against the Hungarian Government on the basis of Article 16 of the Treaty on the Functioning of the European Union and Article 8 of the EU Charter of Fundamental Rights which safeguard the independence of data protection supervisors. After careful consideration of the facts, the Court ruled that the replacement of Data Protection Commissioner prior to completion of his service encroached upon existing EU law provisions because independence include the "obligation for the Member State concerned to allow that authority to serve its full term of office."¹⁰⁶⁶

In the light of the above, it is possible to argue that to ascribe an independent status to the proposed hosting ISSP supervisory for copyright and trade mark infringements could have merits for the parties whose interests are involved. Such merits could amount to the completion of policy objectives of copyright and trade mark law. Given that the outdated framework under the ECD and the problematic regime under the DSMD, as discussed in chapters 2 and 3 respectively, give rise to legal uncertainty to right holders and users, an independent hosting ISSP supervisory authority might offer a better protection of their interests. For instance, with regard to copyright law, the independence of the authority may create legal certainty to content owners. This in turn would give incentives to right holders to further create works. Likewise, in the context of trade marks, brand owners would feel that their rights were protected, and enforcement was not left to hosting ISSPs which are mainly private corporations with business interests. Thus, cases like the one with Louis Vuitton in 1970 when Louis Vuitton decided to withdraw its products from the market due to the high volume of counterfeit bags,¹⁰⁶⁷ would be avoided.

This understanding of completion of policy objectives has been outlined in other sectors where supervisory authorities exist. For instance, with regard to competition law policies, it has been evidenced in an OECD survey that one third of the respondents outlined that

¹⁰⁶⁵ EU Commission, "Court of Justice upholds independence of data protection authorities in case against Hungary" (8 April 2014) < http://europa.eu/rapid/press-release_MEMO-14-267_el.htm > last accessed 28 December 2019.

¹⁰⁶⁶ C-288/12- *Commission v Hungary*, para. 50.

¹⁰⁶⁷ A. Radon, "Counterfeit Luxury Goods Online: An Investigation of Consumer Perceptions" (2012) 4 *International Journal of Marketing Studies* 74.

“greater independence” can enhance the competition law objectives.¹⁰⁶⁸ With the establishment of an authority outside the public sector, or quasi-incorporated into the public sector, external influence towards the member of the authority may be limited. In this light, core competition aims such as the increase of competitive process and higher economic efficiency will likely be achieved.¹⁰⁶⁹ A similar understanding could be equally applied within the context of copyright and trade mark violations online. Independence of the hosting ISSP supervisory authority could complete the copyright law goals such as the dissemination of creative works while for trade mark rights it would boost innovation within the business market since a high degree of protection would be offered to brands.

B. Accountability

Another principle the proposed hosting ISSP supervisory authority would possess is accountability.¹⁰⁷⁰ As discussed in Section III. A of this chapter, the lack of accountability of the Greek administrative agency for copyright infringements online has given rise to criticism that might undermine the legitimacy of its decisions.

From a general point of view, accountability is to be understood as “the obligation of a person to another person according to which the former must give account of, explain and justify her actions or decision in an appropriate way.”¹⁰⁷¹ Endorsing this definition into the current narrative, the entity, who in this case is the hosting ISSP supervisory authority, must be accountable to a hierarchical higher institutional body. This means that a supervisory authority would have a vertical accountability.

Vertical accountability may include either the sharing of information to the superior institution with regard to previous actions or sharing of information in the course of the supervision duties.¹⁰⁷² In both cases, this means that the decisions and the actions

¹⁰⁶⁸ OECD Global Forum on Competition, “The objectives of competition law and policy” (2003) is available at < <http://www.oecd.org/daf/competition/2486329.pdf> > last accessed 28 December 2019.

¹⁰⁶⁹ Ibid.

¹⁰⁷⁰ The concept of accountability emerges from the latin word *accomptare* that means *to account* and *computare* which means calculate, see R. Weber, “The legitimacy and accountability of the Internet’s governing institutions” in I. Brown (ed.), *Research Handbook on Governance of the Internet* (2013) 100; It has been widely used in Ancient Greece where Athenians were holding the public servants accountable for their actions, see D. D. von Dornum, “The Straight and the Crooked: Legal Accountability in Ancient Greece” (1997) 97 *Columbia Law Review* 1483.

¹⁰⁷¹ R. Weber “The legitimacy and accountability of the Internet’s governing institutions” in I. Brown (ed.), *Research Handbook on Governance of the Internet* (2013) 100.

¹⁰⁷² OECD, “Working party on regulatory management and reform designing independent and accountable regulatory authorities for high quality regulation, Proceedings of an Expert Meeting in London, United Kingdom” (2005) 54.

undertaken by the authority would be under the scrutiny of the superior institution whose aim is to supervise the authority that deals with copyright and trade mark infringements online.

The application of the principle of accountability on the supervisory authority would have merits for the different parties at stake. In particular, accountability might enhance the legitimacy of their decisions and actions. This means that those decisions issued by the proposed hosting ISSP supervisory authority would be legally binding and thus they could be challenged only in courts. Otherwise, the legal validity of the decisions issued by the ISP supervisory authority would be questionable. This was the case in Greece, with the Committee on Intellectual Property violations, as discussed in Section III. A of this chapter. Given that the Greek Committee does account for its actions neither to a higher administrative body nor to the Ministry of Culture,¹⁰⁷³ the decisions issued by the Committee do not have the same legal effect on individuals. Conversely, ascribing accountability to a hosting ISSP supervisory authority means that individuals cannot ignore its decisions while its annulment can only be ordered after the issue of a court ruling. As a corollary, this understanding might promote the credibility and the efficiency of the hosting ISSP supervisory body.¹⁰⁷⁴

Other examples of accountable supervisory bodies can be found in different legal contexts. A very recent example of this understanding is *Schrems* ruling,¹⁰⁷⁵ which can be drawn from the data protection framework in light of the Snowden revelations. In this case, Michael Schrems, a doctoral researcher on privacy and a Facebook user, lodged a complaint with the Irish National Data Protection Authority requesting the termination of the transfer of his data from Facebook Ireland to Facebook Inc. in the US. At European level, the EU Commission under the Safe Harbor agreement considers the transfer of data from Europe to US as safe and valid.¹⁰⁷⁶ In this light, the Authority declined his request,

¹⁰⁷³ Ch. Tsigkou, "Notice and Takedown Procedure under Greek Intellectual Property Law 4481/2017" (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 204.

¹⁰⁷⁴ R. Weber, "The legitimacy and accountability of the Internet's governing institutions" in I. Brown (ed.), *Research Handbook on Governance of the Internet* (2013) 100.

¹⁰⁷⁵ Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

¹⁰⁷⁶ S. Monteleone and L. Puccio, "From safe harbour to privacy shield: advances and shortcomings of the new EU-US data transfer rules" (2017) 4 is available at <[http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA\(2017\)595892_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/595892/EPRS_IDA(2017)595892_EN.pdf)> last accessed 28 December 2019.

reasoning that the Safe Harbor agreement was valid, and he was bound by it.¹⁰⁷⁷ Following this outcome, Schrems decided to challenge the decision of the Irish Data Protection Authority and brought legal proceedings against the Authority in front of the Irish High Court.

At European level, a pertinent example of an accountability mechanism is the EDPB.¹⁰⁷⁸ EDPB is the European Data Protection Board¹⁰⁷⁹ that replaced the Article 29 Working Party and undertook its activities. It is an independent European body whose purpose is to ensure the consistent application of data protection provisions across Europe. Such a body is answerable for its actions and decisions to European agencies.¹⁰⁸⁰ In practice, this means that EU Commission can control, on the basis of Article 17 (1) of the Treaty on European Union,¹⁰⁸¹ the legitimacy of its decisions and member states and the relevant stakeholders can challenge in front of the courts its decisions pursuant to Article 263(1)¹⁰⁸² of the Treaty of the Functioning of the European Union.¹⁰⁸³

Therefore, to hold the proposed ISSP supervisory authority accountable to a hierarchical superior government body could promote the legitimacy of its decisions and thus offer an extra layer of protection for all the parties involved in the dispute.

¹⁰⁷⁷ M. Škrinjar Vidović, “Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities” (2015) *Croatian Yearbook of European Law and Policy* 262.

¹⁰⁷⁸ At national level, the national data protection authority in every member state is accountable to a higher institution. In Greece, for instance, is the Greek Parliament, see in Hellenic Parliament archive <<https://www.hellenicparliament.gr/UserFiles/c0d5184d-7550-4265-8e0b-078e1bc7375a/7873691.pdf>> last accessed 28 December 2019.

¹⁰⁷⁹ For more information on EDPB, see: <https://edpb.europa.eu/>.

¹⁰⁸⁰ O. Lynskey, “The Europeanisation of data protection law” (2016) 19 *Cambridge Yearbook of European Legal Studies* 252.

¹⁰⁸¹ Article 17 (1) of the TEU “The Commission shall promote the general interest of the Union and take appropriate initiatives to that end. It shall ensure the application of the Treaties, and of measures adopted by the institutions pursuant to them. It shall oversee the application of Union law under the control of the Court of Justice of the European Union. It shall execute the budget and manage programmes. It shall exercise coordinating, executive and management functions, as laid down in the Treaties. With the exception of the common foreign and security policy, and other cases provided for in the Treaties, it shall ensure the Union's external representation. It shall initiate the Union's annual and multiannual programming with a view to achieving interinstitutional agreements.”

¹⁰⁸² Article 263 (1) of the TFEU “The Court of Justice of the European Union shall review the legality of legislative acts, of acts of the Council, of the Commission and of the European Central Bank, other than recommendations and opinions, and of acts of the European Parliament and of the European Council intended to produce legal effects vis-à-vis third parties. It shall also review the legality of acts of bodies, offices or agencies of the Union intended to produce legal effects vis-à-vis third parties.”

¹⁰⁸³ *Ibid.*

C. *Proportionality*

Another principle that a hosting ISSP supervisory authority would have is proportionality with regard to the decisions that this authority issues. In other words, a hosting ISSP supervisory authority would examine the cases under the lens of proportionality. This may concern either the adoption of proportionate measures in order to oversee the actions of hosting ISSPs or proportionate sanctions when hosting ISSPs do not comply with the orders of the authority.

From a general point of view, the principle of proportionality traces its roots back to the Prussian courts of 19th century and after the Second World War was diffused globally as a constituent of constitutional review in a handful of national jurisdictions.¹⁰⁸⁴ At European level, the principle of proportionality is perceived as the “cornerstone of EU law”.¹⁰⁸⁵ This is because it is considered a substantial legal principle upon which the European legal system rests. As Stone, Sweet and Matthews point out “After the consolidation of the ECJ's "constitutional" doctrines of supremacy and direct effect, the emergence of proportionality balancing as a master technique of judicial governance is the most important institutional innovation in the history of European legal integration.”¹⁰⁸⁶ This means that the principle of proportionality constitutes a fundamental principle of the EU Law and thus could be equally placed next to the fundamental principles of EU Law that recognize the supremacy and the direct effect of EU legislation to the national legislation of EU member states.

The principle of proportionality was officially included for the first time in Article 52 of the EU Charter of Fundamental rights, which dictates that “any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others.” This implies that proportionality is the most appropriate mechanism to warrant the limitation of fundamental rights and thus could serve as a legitimate basis to weigh up the different interests at stake.

¹⁰⁸⁴ W. Sauter, “Proportionality in EU Law: A Balancing Act?” (2013) TILEC Discussion Paper 1.

¹⁰⁸⁵ J. Schwarze, *European Administrative law* (2006) 677.

¹⁰⁸⁶ A. Stone Sweet & J Matthews, “Proportionality Balancing and Global Constitutionalism” (2009) 47 *Columbia Journal of Transnational Law* 73.

Given the seminal importance of proportionality in maintaining a balance between the different interests at stake, it seems that a handful of supervisory authorities at European level operate under the principle of proportionality.¹⁰⁸⁷ By using the principle of proportionality, the proposed ISSP supervisory authority for copyright and trade mark infringements would ensure that a balance is to be reached between “the means used and the intended aim”.¹⁰⁸⁸

Relevant examples of supervisory authorities that adopt the principle of proportionality can be found in data protection framework. For instance, in order to impose fines on companies where data breaches have taken place, the Information Commissioner’s Office in the UK takes into consideration the gravity of data breach. This was the case of Uber, whose systems were hacked, resulting to a severe data breach of passengers and drivers. Crucially, instead of notifying the competent regulatory authorities for the data breach, Uber decided to pay the hackers a respectable amount of money so that they destroy the data they stole.¹⁰⁸⁹ After this incident was leaked to the media, the ICO examined the case and imposed a very high fine on Uber. This is because, as the investigator of the ICO explained, this data breach that resulted in the theft of the personal data of 47 million passengers and drivers not only demonstrated Uber’s incomplete security measures, but it also highlighted the disrespect of Uber towards its clients and employees whose rights and freedoms were severely violated without them being notified.¹⁰⁹⁰

The principle of proportionality is also applicable in the competition law sector. For example, the Spanish Competition Authority imposes fines after taking into consideration the principle of proportionality.¹⁰⁹¹ However, the Spanish Court noted that between November 2010 and February 2012 a handful of decisions issued by the Spanish Competition Authority have been considered disproportionate and thus have been

¹⁰⁸⁷ EDPS, “Report on assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit” (2017) 12.

¹⁰⁸⁸ K. Lenearts and P. Van Nuffel, *European Union Law* (2011) 141.

¹⁰⁸⁹ BBC News, “Uber pays \$148m over data breach cover-up” (27 September 2018) is available at <<https://www.bbc.co.uk/news/technology-45666280>> last accessed 28 December 2019.

¹⁰⁹⁰ Information Commissioner’s Office, “ICO fines Uber £385,000 over data protection failings” (27 November 2018) is available at <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/>> last accessed 28 December 2019; ICO investigator noted “This was not only a serious failure of data security on Uber’s part, but a complete disregard for the customers and drivers whose personal information was stolen. At the time, no steps were taken to inform anyone affected by the breach, or to offer help and support. That left them vulnerable.”

¹⁰⁹¹ Spanish Supreme Court, Judgment of 24 May 2004, case nº 7600/2000.

annulled.¹⁰⁹² Such disproportionate decisions were about the imposition of high fines irrespective of the gravity of harm.

In the light of the above, the principle of proportionality could be used by the proposed hosting ISSP supervisory authority when the authority examines disputes between copyright holders and brand owners with hosting ISSPs. In this way, through the lens of proportionality the hosting ISSP supervisory authority would take into consideration the business model of hosting ISSPs as well as the impact of the decisions to the fundamental rights of third parties such as the internet users.

D. Consistency

Another principle that the proposed hosting ISSP supervisory authority would have is consistency. Consistency is understood as the compatibility of decisions taken by two separate national supervisory authorities in similar case scenarios.

The ascription of the principle of consistency would have benefits for a hosting ISSP supervisory authority. Such benefits could include the promotion of legal certainty. In light of this understanding, it is possible to observe that a number of national supervisory authorities in different legal contexts attempt to follow a consistent approach with regard to the decisions they issue. For example, according to the report of Article 29 Working Party of the Data Protection framework,¹⁰⁹³ Data Protection Authorities must cooperate with other Data Protection Authorities with the aim to apply the enforcement of data protection laws in a consistent manner.¹⁰⁹⁴ As per Article 57 (1) (g) of GDPR, each supervisory authority shall “cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensure the consistency of application and enforcement of this Regulation.” In line with this, consistency in cases of ascription of administrative fines should also be maintained. This means that when a supervisory authority decides to impose fines or sanctions on hosting ISSP, a

¹⁰⁹² Allen & Overy, “The proportionality principle in competition law” <http://www.allenoverly.com/SiteCollectionDocuments/The%20proportionality_principle_in_competition_law.PDF> last accessed 28 December 2019.

¹⁰⁹³ THE ARTICLE 29 WORKING PARTY CEASED TO EXIST AS OF 25 MAY 2018 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492> last accessed 28 December 2019.

¹⁰⁹⁴ Article 29 Working Party, “Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679” (adopted on 3 October 2017) is available at <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237> last accessed 28 December 2019.

consideration of similar scenarios where other national authorities have ascribed penalties must be undertaken. In this regard, pursuant to Article 83 (2) of GDPR, a Data Protection Authority must assess a number of points before reaching a decision about fines. Such points may vary from the degree of responsibility of the data controller to the degree of cooperation with the supervisory authority. However, this understanding presupposes a pre-coordination and information exchange between the relevant authorities.

In a similar fashion, the principle of consistency is applicable to Competition Law Authorities. This means that the Authorities must ensure that their decisions are not in conflict with EU statutory rules as well as court rulings handed down by the CJEU and the European Court of Human Rights.¹⁰⁹⁵ For instance, the European Competition Network requires the close cooperation of the national competition authorities with exchange of information in order to ensure the full enforcement of competition law rules.¹⁰⁹⁶ Such information is only appropriate when it is used complementary to EU legal rules and in cases when the outcome is the same.¹⁰⁹⁷ Additional measures such as investigations and fact-finding measures are also available.¹⁰⁹⁸

The same understanding of the principle of consistency has been adopted by financial supervisory authorities at European level. Unlike the data protection authorities which are established in all 28 EU member states, the financial supervisory authorities are not established at national member states. Rather, they are based in only one-member state and oversee the activities of national financial institutions across all 28 EU member states. However, their decisions must be consistent. For example, the Joint Committee of the three European Supervisory Authorities initiated a set of Guidelines whose purpose is to preserve consistency between the decisions of the financial authorities.¹⁰⁹⁹ In particular, the Guidelines focus on the promotion of information exchange between the authorities,

¹⁰⁹⁵ EU Commission, "EU Competition Law: Rules applicable to antitrust enforcement" 2013 <http://ec.europa.eu/competition/antitrust/legislation/handbook_vol_1_en.pdf> last accessed 28 December 2019.

¹⁰⁹⁶ EU Commission, "Notice on cooperation within the Network of Competition Authorities" (2004/C 101/03) para. 2.2.3.

¹⁰⁹⁷ EU Commission, "EU Competition Law: Rules applicable to antitrust enforcement" (2013) <http://ec.europa.eu/competition/antitrust/legislation/handbook_vol_1_en.pdf> last accessed 28 December 2019.

¹⁰⁹⁸ Ibid.

¹⁰⁹⁹ European Securities and Markets Authority, "Final report on Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions: The AML/CFT Colleges Guidelines ESMA" (2019) 5.

the conduct of impact assessments relating to the progress of the financial authorities and supervision of the decision-making rules the authorities follow.”¹¹⁰⁰

To summarize, drawing parallels with data protection, competition and finance law authorities enables illustration of the principles a hosting ISSP supervisory authority should have. Such principles concern the independence of the authority, the consistent and proportionate decisions it would issue and finally the accountability it should have towards a hierarchically superior administrative body. Following this, the narrative moves to the functions the proposed hosting ISSP supervisory authority should exercise. As discussed in the following section, such functions would include enforcement duties, acting as mediator for disputes via its mechanism designed exclusively for complaints either sent by users, right holders or hosting ISSPs and educative duties.

V. Functions of the proposed hosting ISSP supervisory authority

A. *Enforcement duties*

By ascribing enforcement power to the administrative authorities, the state validates the legitimacy of their operation.¹¹⁰¹ Such enforcement duties may extend to either ensure the right application of rules to adjudicate disputes or impose administrative fines.¹¹⁰²

Amidst its enforcement duties, the hosting ISSP supervisory authority would ensure that hosting ISSPs comply with their responsibilities. Such proposed responsibilities, as discussed in chapters 4 and 5, concern the duty of care of hosting ISSPs to prevent the dissemination of counterfeit goods or unauthorized works within their platforms, as well as a transparency obligation. However, to prevent the circulation of unlawful content within their platforms, hosting ISSPs could resort to filtering technology. Apart from the merits filtering systems can present, it has been found that marginal errors can be performed by content identification technology.¹¹⁰³ In this sense, the hosting ISSP supervisory authority would audit the algorithms before their use or in the course of the

¹¹⁰⁰ Ibid.

¹¹⁰¹ L. Belli and C. Sappa, “The Intermediary Conundrum: Cyber-regulator, cyber-police or both?” (2017) 8 Intellectual Property Information and Technology and Electronic Commerce 185.

¹¹⁰² Ibid.

¹¹⁰³ House of Lords, Select Committee on Communications, “The Internet: To regulate or not to regulate: Summary or response” 3; J. Reda’ website, “Upload filters” is available at <<https://juliareda.eu/eu-copyright-reform/censorship-machines/>> last accessed 28 December 2019; E. Engstrom and N. Feamster, “The limits of filtering: a look at the functionality and shortcomings of content detection tools”(2017) 17 is available at <<https://www.engine.is/the-limits-of-filtering>> last accessed 28 December 2019.

operation so as to ensure the right functioning of filtering technology.¹¹⁰⁴ Therefore, any restriction of users' free speech would be avoided to a great extent.

With regard to the correct functioning of the transparency obligation, the hosting ISSP supervisory authority would ensure that hosting ISSPs publish transparency reports with regard to their content management as well as provide users with the opportunity to submit counter-notifications in case their material has been removed. As discussed in chapter 3 and chapter 4, there have been instances where hosting ISSPs have concluded agreements with industry representatives and thus neglected users' counter notifications.¹¹⁰⁵ In other instances hosting ISSPs have resorted to over-enforcement of intellectual property rights in order to evade liability under Article 14 of the ECD.¹¹⁰⁶ Against this background, it is possible to argue that it could be reasonable to hold hosting ISSPs accountable to a supervisory authority in order to demonstrate that they issue transparency reports and provide the opportunity to their internet users to appeal the removal of their content.

Indeed, this understanding has already been exemplified in a handful of court rulings. In these cases, the courts have noted that individuals who are under monitoring should be offered a legal remedy to safeguard their rights. So, in *Tele2 Sverige AB v Post-och telestyrelsen*, where the CJEU examined the impact of surveillance of communications to the privacy of individuals, it has been stated that national member states shall ensure, via independent authorities such as the Data Protection Authorities, that individuals could exercise their right to effective legal remedy in cases where their personal data was processed for unlawful reasons.¹¹⁰⁷

Further, being entitled to ensure the correct functioning of their responsibilities towards the material that is disseminated within their platforms, this research recommends that the proposed hosting ISSP supervisory authority should impose fines to hosting ISSPs in cases of non-compliance. This means that in cases where a hosting ISSP does not deploy

¹¹⁰⁴ F. Pasquale, *Black Box Society: The secret algorithms that control money and information* (Harvard University Press 2015) 3; F. Romero-Moreno, "Notice and stay down' and social media: amending Article 13 of the Proposed Directive on Copyright" (2018) 33 *International Review of Law, Computers and Technology* 183.

¹¹⁰⁵ M. Husovec, "How Europe Wants to Redefine Global Online Copyright Enforcement" in T. Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer Law International 2019) 516-517.

¹¹⁰⁶ Part I Concluding remarks.

¹¹⁰⁷ Case C-203/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* (2016) ECLI:EU:C:2016:970.

the appropriate measures to prevent the dissemination of infringing material, as well as not publishing transparency reports or not offering counter-notifications options, the hosting ISSP would be subject to the imposition of fines. This power to impose fines, as Laidlaw comments, would strengthen the status of the hosting ISSP supervisory authority.¹¹⁰⁸ In support of this claim, it has been found that the role of the Information Commissioner's Office has been empowered since it took on the duty to impose penalties on companies for breach of their duties.¹¹⁰⁹

Finally, another enforcement duty recommended for the proposed hosting ISSP supervisory authority is the adjudication of disputes. This means that right holders would resort to the hosting ISSP supervisory authority in order to protect their rights against hosting ISSPs that host their material without their permission. On the one hand, the attribution of adjudicative duties could be warranted. This is because, as explored in chapter 2 and chapter 3 respectively, the outdated approach under the ECD and the problematic approach under the DSMD might give rise to legal uncertainty among right holders whose rights have been violated but no redress has been achieved in the courts' legal arena.

On the other hand, the proposed hosting ISSP supervisory authority could rely on existing authorities that deal with hosting ISSP secondary infringements in Greece and Italy. Regardless of the flaws identified, such authorities could be seen as having the merit of being easy to implement and administer. This advantage seems to attract right holders who resort to those authorities when they seek redress for the violation of their rights. Consider, for instance, the Greek Committee on intellectual property violations. Following its establishment in 2017, the Committee has issued five decisions so far. The first two decisions, 1/ 2018¹¹¹⁰ and 2/2018,¹¹¹¹ confirmed the compliance of hosting providers and website operators with the request to take down infringing content from their online

¹¹⁰⁸ E. Laidlaw, "Are We Asking Too Much from Defamation Law? Reputation Systems, ADR, Industry Regulation and Other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age: Proposal for Reform" (2017) 51 is available at <<http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw.pdf>> last accessed 28 December 2019.

¹¹⁰⁹ E. Laidlaw, "Are We Asking Too Much from Defamation Law? Reputation Systems, ADR, Industry Regulation and Other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age: Proposal for Reform" (2017) 51 is available at <<http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw.pdf>> last accessed 28 December 2019; E. Laidlaw, "Internet Gatekeepers, Human Rights and Corporate Social Responsibilities" (PhD thesis 2012) 237.

¹¹¹⁰ OPI<https://www.opi.gr/images/epitropi/apofaseis/edppi_1_2018.pdf> last accessed 26 December 2019.

¹¹¹¹ OPI<https://www.opi.gr/images/epitropi/apofaseis/edppi_2_2018.pdf> last accessed 26 December 2019.

platforms. The third decision, 3/2018, ordered for the first time the blocking of 38 websites whose purpose was to provide links that enabled internet users to view unauthorized films.¹¹¹² These websites offered classified links with the titles of the films that redirected internet users to third party websites and permitted them to watch the films. Taking into consideration the massive scale of copyright infringements that have lasted for a long period of time and the popularity of those websites to internet users, the Committee ordered the blocking of the entire websites for 3 years. In case of non-compliance, fines of 850 euros for every day have been imposed. The fourth decision, 4/2019, confirmed the compliance of the hosting providers and website operators with the request of right holders to remove the unlawful material¹¹¹³ while the fifth decision, 5/2019, ordered the termination of access to websites that provided hyperlinks with unauthorized music files.¹¹¹⁴

These five decisions undoubtedly could provide a promising example of a supervisory authority that adjudicates disputes between right holders and hosting ISSPs.

To ascribe enforcement duties on supervisory authorities is not a novelty, however. As demonstrated below, a number of supervisory authorities at European level are already entrusted with enforcement duties, for example the Data Protection Authorities. These duties may vary from investigative powers to the imposition of sanctions in cases of non-compliance. For instance, the Spanish DPA imposed fines on Facebook for processing the personal data of its users without complying with the Spanish Data Protection Act.¹¹¹⁵ The fine imposed reached up to €1.2 million for data protection violations. In Greece, the Greek DPA has dealt with a number of cases for illegal transmission of patients' data to insurance companies.¹¹¹⁶ More specifically, there was a case where an insurance company accessed the medical record file of a patient without his consent and denied him compensation. For this action, the insurance company was fined € 20.000.

¹¹¹² OPI<https://www.opi.gr/images/epitropi/apofaseis/edppi_3_2018.pdf> last accessed 26 December 2019.

¹¹¹³ OPI< https://opi.gr/images/epitropi/apofaseis/edppi_4_2019.pdf> last accessed 26 December 2019.

¹¹¹⁴ OPI<https://opi.gr/images/epitropi/apofaseis/edppi_5_2019.pdf> last accessed 26 December 2019.

¹¹¹⁵ C. O' Donoghue and K. Albrecht, "Spanish DPA fines Facebook €1.2 million for data protection infringements" (Reed Smith, 26 September 2017) <<https://www.technologylawdispatch.com/2017/09/privacy-data-protection/spanish-dpa-fines-facebook-e1-2-million-for-data-protection-infringements/>> last accessed 26 December 2019.

¹¹¹⁶ ARTICLE 29 - DATA PROTECTION WORKING PARTY, "Recent examples of enforcement actions carried out by data protection authorities" (January 2005) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp101a_en.pdf> last accessed 26 December 2019.

By the same token, the Competition Law Authorities' main goal is to enforce competition law. This means that they either carry out investigations for cartel violations or adjudicate disputes and impose fines. For instance, according to the report on an academic view on the roles and tools of National Competition Authorities, the National Competition Authorities in the majority of the countries can go to the business premises of the company and conduct control while in Poland a court warrant is required so as to enable the national competition authority to investigate.¹¹¹⁷ Furthermore, upon finding that a company does not comply with competition law rules, the authority may impose fines that vary regarding the gravity of the violation. Consider, for example, in Germany the Federal Cartel Office can impose fines in cases of breach of national or European competition rules which could amount up to 10 % of their yearly profits.¹¹¹⁸ The gravity and the duration of the breach are also taken into consideration in the imposition of fines. Finally, in France, the French Competition Authority can impose a fine of 10% of their yearly profits and if the company continues to breach the European competition rules, a daily fine of 5 % may be imposed as well.¹¹¹⁹

However, the proposed hosting ISSP supervisory authority would not be limited to enforcing intellectual property rights online. Indeed, it is recommended that this authority provides a mechanism for complaints for internet users or online consumers whose rights have been violated by content management policies or consumers who have been deceived in online auction platforms.

B. Complaints' mechanism for internet users and online consumers

Following the recommendation on enforcement duties of the proposed hosting ISSP supervisory authority, it is suggested that a complaints' mechanism is created for users or consumers whose rights are endangered. Their rights could be restricted either because hosting ISSPs wrongfully remove legitimate content that users have uploaded on the platforms or because counterfeit goods have reached end-consumers. This suggestion is primarily based on Article 17 of the DSMD which, as mentioned at the outset of this chapter, dictates in Article 17 (9) that "Member States shall provide that online content-sharing service providers put in place an effective and expeditious complaint and redress

¹¹¹⁷ Economic and Monetary Affairs Committee, "Report on an academic view on the Role and Powers of National Competition Authorities" (2016) 23.

¹¹¹⁸ Ibid.

¹¹¹⁹ Ibid.

mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them.”

This complaints mechanism would ensure to a greater extent the protection of internet users and online consumers, as well as enhance their trust which is considered a cornerstone for e-commerce services.¹¹²⁰ Indeed, Barral-Vinals outlines that “e-commerce will only grow if consumers have confidence in it.”¹¹²¹ This implies that the trust of consumers towards the online sales is contingent upon the hosting ISSPs and in particular the appropriate safeguards that hosting ISSPs could offer to online consumers when they make their purchase online.

However, as commented in chapter 3, it has been observed that hosting ISSPs conclude agreements with right holders.¹¹²² Such agreements include terms that are often one-sided and neglect internet users’ fundamental rights. A pertinent example can be found in YouTube platform that dismisses any counter-notification for content that belongs to right holders with whom YouTube has entered into contractual agreements.¹¹²³

What is more, in the terms and conditions of hosting ISSPs, they are subject to limited liability. This means that if they remove any users’ material, they are not liable towards them. Consider, for instance, the example of YouTube. Having a look at the terms and conditions of YouTube, there is an explicit section for Limitation of Liability of YouTube towards its users.¹¹²⁴ More specifically, it is noted that YouTube is not responsible towards its users for “any loss or damage that was not, at the time that this Agreement was formed between you and YouTube, a reasonably foreseeable consequence of YouTube or its

¹¹²⁰ H. Hallikainen and T. Laukkanen, “National culture and consumer trust in e-commerce” (2018) 38 *International Journal of Information Management* 97-106; P. J. Dittrich, “Online Platforms and how to regulate them: an EU overview” (2018)) Jacques Delors Institute 28.

¹¹²¹ Barral-Vinals, “Enforcing e-consumer protection beyond alternative dispute resolution (ADR): ODR” in J. Devenney and M. Kenny (eds.), *European consumer protection : theory and practice* (Oxford University Press 2012) 93.

¹¹²² S. Jacques, K. Garstka and others, “An Empirical Study of the Use of Automated Anti-Piracy Systems and their Consequences for Cultural Diversity” (2018) 15 *Scripted* 308; A. Ramahlo, “Copyright law-making in the EU: what lies under the 'internal market' mask?” (2014) 9 *Journal of Intellectual Property Law & Practice* 224 where she notes that “...EU Copyright legislation that is partly industry-orientated, while other players seem to have fallen behind.”

¹¹²³ M. Perel and N. Elkin-Koren, “Accountability in algorithmic copyright enforcement” (2016) 19 *Stanford Technology Law Review* 473.

¹¹²⁴ YouTube, Terms of service <<https://www.youtube.com/static?gl=GB&template=terms>> last accessed 28 December 2019.

Affiliates breaching this Agreement.”¹¹²⁵ In a similar fashion, Facebook’s terms note that “..Provided that we have acted with reasonable skill and care, we do not accept responsibility for: losses not caused by our breach of these Terms or otherwise by our acts...”¹¹²⁶ Likewise, Instagram’s terms and conditions state that “ Instagram shall not, under any circumstances, be liable to you for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with use of the Instagram Platform..”¹¹²⁷ Finally, Amazon’s terms and conditions explicitly note that “ We and our affiliates and licensors will not be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages including damages for loss of profits, revenues, customers, opportunities, goodwill, use or data.”¹¹²⁸ This implies that hosting ISSPs do not have any legal responsibility for any direct or indirect losses of their online customers when they use their online services either for disseminating content or buying goods online. It is this limitation of liability of hosting ISSPs that diminishes the possibilities of internet users to seek redress and ask for damages against hosting ISSPs in case their content has erroneously been removed or they have been deceived by purchasing counterfeit goods online.

Further, any attempts that have been initiated by users against hosting ISSPs alleging erroneous removal of their content have failed. To my knowledge, such a case has not emerged at the European level so far. It is only in front of the US Courts where such cases have been brought and have been dismissed due to the binding contractual terms between the parties at stake. This was the case of *Lewis v YouTube* where Lewis brought legal proceedings against YouTube alleging breach of contract since YouTube terminated his YouTube channel account under the reason of violating its terms of service.¹¹²⁹ Yet, the Superior Court of California dismissed the case; concluding that a claim for damages is not valid. To the court’s reasoning, the non-commercial nature of plaintiff’s YouTube channel, along with YouTube’s the terms of service, preclude the request for damages. It

¹¹²⁵ YouTube, Terms of service, community guidelines are available at <<https://www.youtube.com/static?gl=GB&template=terms>> last accessed 28 December 2019.

¹¹²⁶ Facebook, legal terms are available at <<https://en-gb.facebook.com/legal/terms>> last accessed 15 April 2019.

¹¹²⁷ Instagram, legal terms are available at <<https://www.instagram.com/about/legal/terms/api/>> last accessed 28 December 2019.

¹¹²⁸ Amazon, legal terms available at < <https://aws.amazon.com/agreement/>> last accessed 28 December 2019.

¹¹²⁹ *Lewis v. YouTube LLC*, 197 Cal. Rptr. 3d 219 (2015).

could be assumed that a similar understanding could be equally applied at European level accordingly.

Finally, another reason that reinforces the need for a complaint's mechanism is the need for a higher degree of protection for online consumers. This is because, as Riefa has observed,¹¹³⁰ whilst in the brick and mortar environment buyers could bring legal proceedings against owners of marketplaces, there is not adequate legal protection for online consumers who decide to purchase goods online. This is because online marketplaces are not considered auction places. For instance, clause 2 of eBay's User agreement states that "eBay is not a traditional auctioneer."¹¹³¹ Likewise, Amazon, pursuant to clause 13, notes that "Amazon is not an auctioneer, neither is it an intermediary between the buyer and the seller."¹¹³² Instead, Amazon's business is based on providing a platform for sellers to display their goods and consumers to purchase and complete transactions online. In a similar fashion, etsy's seller's agreement presents its activities as "a marketplace where you can sell your handmade goods, vintage items, and craft supplies directly to buyers around the world."¹¹³³ Any reference to online marketplaces or a description of its services as auction places are not included.

Such a stance has been maintained in policy documents issued at the European as well as national level. Within the European context, the EU Commission's impact assessment on promoting fairness and transparency on hosting ISSPs refrains from treating online marketplaces as auction places. Rather it considers online marketplaces as marketplaces on which a commercial transaction between a customer and a business user takes place or online platforms bringing together users with the aim to "facilitate" commercial transactions.¹¹³⁴ In addition, at national level, UK authorities explicitly inform online consumers that online marketplaces are not considered auction places. In particular, the Office of Fair Trading warns consumers that current hosting ISSPs that facilitate the

¹¹³⁰ C. Riefa, "To be or not to be an auctioneer? Some thoughts on legal nature of online "ebay "auctions and the protection of consumers" (2008) 31 Journal of Consumer Policy 167.

¹¹³¹ eBay user agreement is available at <<https://www.ebay.com/help/policies/member-behaviour-policies/user-agreement?id=4259>> last accessed 29 December 2019.

¹¹³² Amazon, seller participation agreement <<https://sellercentral-europe.amazon.com/forums/t/who-is-contract-between/8636>> last accessed 29 December 2019.

¹¹³³ Etsy seller agreement <<https://www.etsy.com/legal/sellers/>> last accessed 29 December 2019.

¹¹³⁴ EU Commission Staff Working Paper, "Impact assessment on Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, Online Services, Including E-Commerce, in the Single Market" COM (2018) 238 final.

purchase of goods online do not fulfill the requirements of traditional auctions.¹¹³⁵ This means that such hosting ISSPs do not have the strict legal obligations auctioneers have and thus it is difficult for online consumers to hold them liable in case of misconduct. Along similar lines, the Department of Trade and Industry clarifies that online auctions or internet auctions are just a term to refer to websites where buyers place goods and consumers select to buy them.¹¹³⁶ In any case, the consumers must not consider them auction places when they purchase goods from their platforms.

However, as discussed at the outset of this chapter, it is not only the DSMD that envisages the establishment of a mechanism for the disputes between hosting ISSPs and internet users and consumers. Indeed, a growing body of academic scholarship encourages the creation of such a mechanism. For instance, a recommendation for such a mechanism has been expressed by Laidlaw, but not without skepticism. Within the context of search engines, she highlights the need to establish an independent complaints mechanism as a safeguard against the manipulation of search results rankings.¹¹³⁷ For instance, she argues that Ofcom in the UK illustrates a representative example since it entails a complaints mechanism.¹¹³⁸ Ofcom acts as a regulator for broadcasting sector and focuses on the protection of consumers' privacy rights and ensures the right functioning of broadcasting standards. In particular, the complaints mechanism enables the consumers to submit a complaint in cases when broadcasters do not comply with the rules. Upon submission of the complaint and within 15 working days, Ofcom primarily assess the complaints and decide whether it should be evaluated further. If so, after informing the broadcaster, Ofcom opens an investigation which should be concluded within 50 working days.¹¹³⁹

¹¹³⁵ C. Riefa, "To be or not to be an auctioneer? Some thoughts on legal nature of online "ebay "auctions and the protection of consumers" (2008) 31 *Journal of Consumer Policy* 175.

¹¹³⁶ C. Riefa, "To be or not to be an auctioneer? Some thoughts on legal nature of online "ebay "auctions and the protection of consumers" (2008) 32 *Journal of Consumer Policy* 175.

¹¹³⁷ E. Laidlaw, "Private Power, Public Interest: An Examination of Search Engine Accountability" (2008) 17 *International Journal of Information Technology and Law* 143-144.

¹¹³⁸ *Ibid*, in particular Laidlaw notes that "The complexity and concerns regarding an OFCOM structure are far more than indicated herein. Such complexities are exacerbated if one attempts to apply it to the internet, because of the political ramifications of attempting public regulation of a transnational communications network. However, at this stage a fundamental question is whether a complaints mechanism is better run by the industry, with government involvement, or by international collaboration and so on. OFCOM is merely one example of a quasi-governmental approach. It is advantageous in binding the industry to the Code, and the threat of licence removal is significant to deter certain behaviour. Whether it is effective, or used for that matter, is uncertain as OFCOM is still in its infancy."

¹¹³⁹ Ofcom, "General procedures for investigating breaches of broadcast licences" (2017) is available at <https://www.ofcom.org.uk/data/assets/pdf_file/0019/31942/general-procedures.pdf> last accessed 29 December 2019.

Along similar lines, Fiala and Husovec conducted an experiment based on empirical studies whose purpose was to suggest an alternative dispute resolution model for users whose content has been removed by hosting ISSPs. Focusing only on content removals, the two researchers recommended the development of an independent external body for handling the complaints of removals of material within the hosting ISSPs.¹¹⁴⁰ According to the study, the creator of a video can submit a counter-notice to the independent body, termed as an alternative dispute resolution mechanism (ADR) and after paying a fee. This means that the costs of the submission are undertaken by the internet users. However, if the body decides that the removal was unfair, the hosting ISSP must pay back the creator's fee as well as extra costs to the ADR.¹¹⁴¹ In this light, the creators have incentives to submit counter notices since their complaints will be meticulously evaluated. In addition, the fees they pay for the counter-notice are returned to them.¹¹⁴² With regard to hosting ISSPs, the ADR mechanism gives them incentives to review more carefully the allegedly infringing material¹¹⁴³ and take into consideration the fair use principle before removing the content.

Such a stance has been maintained by Tessier and others who, in their report for the hosting ISSPs' coalition, recommended the establishment of an independent agency, which they named the Agency for Trust in the Digital Platform Economy.¹¹⁴⁴ More specifically, this body would be entrusted with a mediator role that would deal with users' and consumers' complaints against hosting ISSPs while at the same time it would promote a dialogue between hosting ISSPs and users-consumers. In addition, the staff of this independent agency would have the appropriate expertise to evaluate the comments and attempt to give a solution.

In the light of the above, an optimal complaints' mechanism offered by the proposed hosting ISSP supervisory authority could operate as follows: under the condition that the user has submitted a counter-notification requesting the reinstatement of the content that has been removed and the hosting ISSP has either ignored its claim or rejected it, the

¹¹⁴⁰ L. Fiala and M. Husovec, "Using experimental evidence to design optimal notice and takedown process" (2018) TILEC Discussion Paper 7.

¹¹⁴¹ Ibid.

¹¹⁴² Ibid.

¹¹⁴³ Ibid.

¹¹⁴⁴ M. Tessier, J. Herzog and L. Madzou, "Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us Official Outcome of the UN IGF Dynamic Coalition on Platform Responsibility*, (United Nations Internet Governance Forum 2018) 182.

user/ consumer can resort to the complaints mechanism of the proposed hosting ISSP supervisory authority. It is suggested that this complaints' mechanism follows the EU Commission's Directive¹¹⁴⁵ and Regulation¹¹⁴⁶ on alternative dispute resolution mechanisms.¹¹⁴⁷ The level of success of those alternative dispute resolution schemes has been outlined by the EU Commission's report in 2017 which reveals that users' complaints to the alternative dispute mechanism reached 3000 per month in 2017 with online consumers from Germany and the United Kingdom being the pioneers.¹¹⁴⁸ In similar fashion, another report conducted by the EU Commission in 2019 on assessing the alternative dispute resolution mechanism confirms the findings of the report of 2017 and outlines that such mechanism "has become an integral part of the EU's toolbox for the public and private enforcement of consumer law."¹¹⁴⁹ Indeed, it has been found that over 4500 users have submitted complaints about online purchases per month in 2018.

That extrajudicial systems for disputes include a number of principles such as the independence of the body that deals with the disputes, transparent, effective, fast, non-costly and fair procedures, as well as decisions compatible with the consumer protection framework. In this way, internet users whose material has been removed and whose counter-claim has been ignored or rejected could be given the option to submit their complaints against hosting ISSPs to this mechanism. Alongside this, online consumers could also be entitled to resort to this mechanism for complaints against hosting ISSPs that circulate infringing material.¹¹⁵⁰

¹¹⁴⁵ Council Directive (EU) 2013/11/EU of the European parliament and of the Council on Alternative Dispute Resolution for consumers (2013) OJ L 165.

¹¹⁴⁶ Council Regulation (EU) No 524/2013 of the European parliament and of the Council on online dispute resolution for consumers (2013) OJ L 165.

¹¹⁴⁷ See also out-of-court settlement of consumer disputes is available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l32031&from=EN>,> last accessed 28 December 2019; see also Consumer access to justice (Green Paper) is available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l32023&from=EN>> last accessed 28 December 2019.

¹¹⁴⁸ EU Commission, "Report on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes" COM (2017) 744 final.

¹¹⁴⁹ EU Commission, "Report on the application of Directive 2013/11/EU of the European Parliament and of the Council on alternative dispute resolution for consumer disputes and Regulation (EU) No 524/2013 of the European Parliament and of the Council on online dispute resolution for consumer disputes" COM (2019) 425 final 17.

¹¹⁵⁰ J. Devenney, "The legacy of the Cameron-Clegg coalition programme of reform of the law on the supply of goods, digital content and services to consumers"(2018) 6 Journal of Business Law 488 where Devenney argues that in relation to clear consumer rights "much will depend on, for example, dissemination of information on rights to consumers, consumer education and redress mechanisms and assistance."

Therefore, it is possible to argue that with this complaints' mechanism it would be more likely that users' fundamental rights would be safeguarded, thus avoiding the extent of their violation. In addition, it is likely that this mechanism would offer a higher degree of consumer protection, thus reaching the goals of consumer protection laws. Such goals address the need for consumer laws to adapt to the digital age,¹¹⁵¹ as set out in the Communication of consumer law, as well as enable consumers to "enjoy a high common level of protection across the Union",¹¹⁵² as per Recital 7 of the Preamble of the Consumer Directive of 2011/83/EU.

However, apart from the enforcement duties and resolution of disputes between internet users -consumers and hosting ISSPs that the proposed hosting ISSP supervisory authority should have, another role of the proposed hosting ISSP supervisory authority should be an educative one.

C. Promoting user-consumer awareness

To inform users about the negative implications of piracy is also an important policy initiative that the proposed hosting ISSP supervisory authority could offer.

The promotion of awareness among users would have merits with regard to the limitation of piracy and enhancement of creativity. This is because users would be informed about the negative impact on authors and creators, such as the economic loss that the transmission of their work without their permission might cause, as well as the imposed fines in cases where users upload, download or exchange unauthorized material.¹¹⁵³ In this sense, users would be encouraged to refrain from illicit activities and thus turn to lawful alternatives.

This understanding has been outlined in a number of studies conducted by private stakeholders. For instance, the Irdeto Global Consumer Piracy survey reports that 45% of

¹¹⁵¹ EU Commission, "A European Consumer Agenda - Boosting confidence and growth" COM(2012) 225 final <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0225&from=EN>> last accessed 28 December 2019.

¹¹⁵² Council Directive (EC) 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 is available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&from=EN>> last accessed 28 December 2019.

¹¹⁵³ Electronic Frontier Foundation, "How SOPA Affects Students, Educators, and Libraries" (14 December 2011) is available at <<https://www.eff.org/deeplinks/2011/12/how-sopa-affects-students-and-educators>> last accessed 28 December 2019.

the individuals who participated in their survey stated that they would refrain from exchanging unauthorized works online after being made aware of the high revenue losses to creators.¹¹⁵⁴

Such awareness campaigns have already shown positive results in other sectors too.¹¹⁵⁵ A representative example can be found in the campaigns against teenage smoking.¹¹⁵⁶ These initiatives have had a positive result since it has been found that they have persuaded around 522,000 smokers to cease smoking in the long term.

At policy level, with regard to copyright infringements, member states have endorsed education campaigns that inform individuals of the negative impact of copyright violations. The UK Government's funded program¹¹⁵⁷ is a representative example of users' awareness of the implications of illegal downloading.¹¹⁵⁸ This initiative is called "Get it right from a genuine site"¹¹⁵⁹ and is part of the Creative Content UK campaign. Its aim is to make users aware of the time and efforts creators invest in their works and as it appears it has already positive outcomes. Indicatively, the pioneers of this initiative report that "We are very pleased with the progress of the campaign to date and as awareness continues to build, we expect to see strong results for the creative sectors in the coming year."¹¹⁶⁰

Moreover, the importance of promoting awareness of the circulation of unlawful material is exemplified by initiatives introduced by copyright representatives as well as hosting ISSPs. For instance, the International Federation of the Phonographic Industry (IFPI) reports demonstrate a handful of initiatives in different countries designed to inform

¹¹⁵⁴ Irdeto, "Nearly half of consumers around the globe are willing to stop or watch less pirated video content" (8 March 2017) is available at <<https://irdeto.com/news/nearly-half-of-consumers-around-the-globe-are-willing-to-stop-or-watch-less-pirated-video-content/>> last accessed 28 December 2019.

¹¹⁵⁵ J. M. Crotty, "Education Is Best Weapon Against Web Piracy, not SOPA"(Forbes, 31 January 2012) is available at <<https://www.forbes.com/sites/jamesmarshallcrotty/2012/01/31/better-than-sopa-public-education-best-weapon-against-web-piracy/#76f84b504228>> last accessed 28 December 2019.

¹¹⁵⁶ Public education campaigns reduce tobacco is available at <<https://www.tobaccofreekids.org/assets/factsheets/0051.pdf>> last accessed 28 December 2019.

¹¹⁵⁷ Ernesto, "UK Anti-Piracy 'Education' Campaign Launched, Quietly" (Torrentfreak, 1 December 2015) is available at <<https://torrentfreak.com/uk-anti-piracy-education-campaign-launched-quietly-151201/>> last accessed 28 December 2019; Get it right from a genuine site is available at <<https://www.getitrightfromagenuinesite.org/>> last accessed 28 December 2019.

¹¹⁵⁸ <http://www.copyrighthub.org/>

¹¹⁵⁹ <https://www.getitrightfromagenuinesite.org/>

¹¹⁶⁰ Ernesto, "UK Anti-Piracy 'Education' Campaign Launched, Quietly" (Torrentfreak, 1 December 2015) is available at <<https://torrentfreak.com/uk-anti-piracy-education-campaign-launched-quietly-151201/>> last accessed 28 December 2019; Get it right from a genuine site is available at <<https://www.getitrightfromagenuinesite.org/>> last accessed 28 December 2019.

users of the negative consequences of exchanging or downloading unauthorized music files. A spectrum of different countries is engaged in anti-piracy education campaigns, thus informing users about piracy and alternative legitimate ways to acquire music files, such as licensing.¹¹⁶¹

However, it is not only policy makers or copyright representatives who use user education as a weapon towards the decrease of piracy rates in the digital ecosystem. Indeed, hosting ISSPs have adopted policies on a voluntary basis in order to enhance awareness for uploading or sharing unauthorized material. For instance, YouTube's Copyright School¹¹⁶² is a tool that educates users on what is lawful to upload on their platform. While the Copyright School tutorial video is entertaining, it stresses the negative implications of piracy for users, focusing on the imposition of monetary damages to individual users and the termination of alleged infringer users' YouTube's accounts.

Further, with regard to online consumers, a similar initiative has been included in the EU Commission's Communication on New Deal for Consumers.¹¹⁶³ This Communication addresses the challenges that consumers face in the Digital Single Market. Amidst the initiatives undertaken by the European policymakers is the maintenance of consumer classroom tutorials which focus on informing consumers about their rights and how to protect them in contexts of online purchases in online marketplaces.

In the light of the above, this thesis argues that the proposed hosting ISSP supervisory authority should initiate education campaigns on the negative consequences of piracy on right holders and users/consumers. Such initiatives could be fostered by national governments and could entail educational material that would emphasize the importance of boosting creativity in the Digital Single Market along with the need for alternative legitimate ways to enjoy creative content online, such as the conclusion of licensing

¹¹⁶¹ The Recording Industry 2006 Piracy report on protecting creativity in music is available at <<https://www.ifpi.org/content/library/piracy-report2006.pdf>> last accessed 28 December 2019

IFPI Digital Music Report 2013: Engine of a digital world is available at <https://www.ifpi.org/downloads/dmr2013-full-report_english.pdf> last accessed 28 December 2019; IFPI Digital Music Report 2019: State of the industry is available at <<https://www.ifpi.org/downloads/GMR2019.pdf>> last accessed 28 December 2019; IFPI Global Music Report 2018 <<https://www.ifpi.org/downloads/GMR2018.pdf>> last accessed 28 December 2019.

¹¹⁶² YouTube Copyright School is available at <https://www.youtube.com/copyright_school> last accessed 28 December 2019.

¹¹⁶³ EU Commission, "Consumer Classroom" is available at <<https://www.consumerclassroom.eu/>> last accessed 16 April 2019; EU Commission, "A New Deal for Consumers" COM (2018) 183 final 14 is available at <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0183&from=EN>> last accessed 28 December 2019.

agreements. The same understanding could be equally applied to online consumers with regard to the protection of their rights against the circulation of counterfeit goods in the digital world.

In short, it is suggested that the proposed hosting ISSP supervisory authority should play an educative role. In parallel with its enforcement duties and users' complaints resolution, it should promote educational campaigns and awareness among users about the negative impact of piracy on right holders' rights and on creativity in general. Alongside this, education of consumers on the existing remedial mechanisms could offer them a higher degree of protection of their rights.

VI. Conclusion

This chapter has discussed the establishment of a hosting ISSP supervisory authority for copyright and trade mark infringements and has built on the findings of the previous chapters in order to justify this need. In particular, as elaborated in chapter 2, it has been found that the current legal framework under Article 14 of the ECD appears to be outdated and thus undermines right holders' interests, as well as poses serious threats for restricting the fundamental rights of internet users, hosting ISSPs. In addition, as presented in chapter 3, the legal framework that regulates the OCSSPs' liability DSMD seems to be problematic since while it favours copyright holders' interests, it interferes to the rights of OCSSPs and internet users.

In order to establish a robust legal framework that strikes a fair balance between the interests of the parties involved, chapter 4 recommended the creation of a co-regulatory regime that entails a set of responsibilities for hosting ISSPs. The aim of this would be to terminate or curb online infringements within their networks through which they should be accountable to a hosting ISSP supervisory authority.

In this regard, chapter 6 explored the normative considerations of a hosting ISSP supervisory authority. In contrast to the current legal framework under Article 14 of the ECD and Article 17 of the DSMD, it was argued that a hosting ISSP supervisory authority would enhance legal certainty to users, right holders and hosting ISSPs. It would promote access to justice for users and right holders while it would also enhance the rule of law by providing remedial mechanisms to internet users and online consumers.

Having discussed the normative considerations for creating such a hosting ISSP supervisory authority, this chapter moved on to the question of the principles and functions this hosting ISSP supervisory authority should have. In order to identify the principles, parallels with existing supervisory authorities at European level were drawn, such as Data Protection and Competition Law Authorities. With regard to the functions of a hosting ISSP supervisory authority, it was suggested that proportionality, consistency, accountability and independence would make this hosting ISSP supervisory authority's role and decisions legitimate.

Finally, chapter 6 suggested the functions that the proposed hosting ISSP supervisory authority should have. The first function concerned the enforcement of intellectual

property rights. In particular, it was argued that the hosting ISSP supervisory authority would verify the completion of the set of responsibilities of hosting ISSPs relating to the dissemination of infringing content within their platforms. Non-compliance with the set of responsibilities would amount to the imposition of fines. In addition, right holders could resort to this authority in order to enforce their rights. The second function of this hosting ISSP supervisory authority should be to examine complaints submitted by internet users whose material has been erroneously removed by hosting ISSPs, or online consumers who have been deceived by purchasing counterfeit goods from online marketplaces. The third function of the proposed hosting ISSP supervisory authority should address an educative role. This means that the authority would be assigned with the duty to promote awareness among internet users of the legal implications of online piracy for right holders. These include economic losses, legal consequences to those users who upload, download, and exchange material without permission, and information on existing remedies for those internet users whose content has been erroneously taken down. Moreover, information for online consumers should also be included with advice on how to protect themselves from fake goods online and existing mechanisms for safeguarding their rights.

Chapter 7: Conclusion

I. Introduction

The aim of this research was to flesh out a more balanced legislative framework to regulate hosting ISSPs' activities with regard to copyright and trade mark infringements that occur within their networks.

In view of the rapid technological developments, hosting ISSPs have transformed from pure communication tools and hosting providers to places where internet users can interact, be informed of a wide range of information available, and purchase goods. Yet, while hosting ISSPs have offered a number of different services to internet users/ online consumers and enabled right holders to reach a broader audience for their works and goods online,¹¹⁶⁴ their activities seem to attract copyright and trade mark violations. Indeed, summary responses of the EU Commission Public Consultation on the modernization of the enforcement of intellectual property rights demonstrates that the appearance of new hosting ISSPs has resulted to the increase of online piracy rates.¹¹⁶⁵

However, the current legislative tools, namely the ECD and the DSMD, seem inefficient. In particular, the current legal framework, as discussed in chapters 2 and 3, fail to protect the rights of intellectual property holders. Rather, as the findings indicate, both legislative tools might severely interfere with internet users' fundamental rights to access information as well as pose serious risks to hosting ISSPs' rights to conduct business as pursuant to Article 16 of the EU Charter of Fundamental Rights.

Therefore, this thesis suggests a new legislative framework for hosting ISSPs. Such a legislative framework, as discussed in chapter 1 of this thesis, balances the different interests at stake. Indeed, this understanding has been outlined in the *Scarlet v Sabam* ruling¹¹⁶⁶ where it was noted that "Member States must [...] take care to rely on an

¹¹⁶⁴ A. Bridy and D. Keller, "U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry" (31 March 2016) 14-15.

¹¹⁶⁵ EU Commission, "Public Consultation on the evaluation and modernisation of the legal framework for the enforcement of intellectual property rights: Summary of responses" (14 September 2016) 8.

¹¹⁶⁶ Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

interpretation of the directives which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order.”¹¹⁶⁷

In this context, this chapter summarizes the research findings, presents the set of recommendations, and offers an epilogue. I should also note here that the aim of this chapter is to outline the main research findings of this thesis and recommendations, and not to provide a detailed analysis of them. Such a detailed analysis has already been presented in the precedent chapters of this work.

II. Research Findings

As noted in chapter 1, the main research question to be addressed reads as following:

How should the legal framework of hosting ISSPs' liability be shaped in order to safeguard intellectual property right holders' rights as well as the interests of internet users/ consumers and hosting ISSPs?

In order to answer this research question, this thesis was divided into two main parts. The first Part, namely chapters 2 and 3, critically evaluated the legislative framework that regulates hosting ISSPs' liability for copyright and trade mark infringements, namely the ECD and the DSMD.

More specifically, in chapter 2, it was argued that the legal framework with regard to hosting ISSPs' liability for trade mark infringements under the ECD is outdated. In this respect, it was noted that Article 14 of the ECD introduces a secondary liability regime for hosting ISSPs with regard to trade mark infringements, which requires the element of knowledge in order to attribute liability to hosting ISSPs. As many commentators have argued, the introduction of a secondary liability regime in 2000 was welcome. This is because the requirement of knowledge could be used by hosting ISSPs as a defense in cases of legal proceedings against them. However, while this understanding has its own merits from a theoretical point of view, in practice this is far from reality.

As the findings indicate, this is mainly due to three factors. Firstly, Article 14 of the ECD failed to provide a definition for hosting ISSPs' liability. On the contrast, it offers defences to hosting ISSPs in order to escape liability. In other words, this implies that the legal

¹¹⁶⁷ Case C-275/06, *Promusicae* (2008) ECR I-00271, para. 70.

provisions specify only the requirements that shelter hosting ISSPs from liability and state what hosting ISSPs should not do in order to escape from liability.

Secondly, the national implementation of the ECD also failed. It was noted that the three jurisdictions this research looked at follow verbatim the ECD and thus follow its rationale by offering defences to hosting ISSPs rather than offering the circumstances under which hosting ISSPs could be held liable. What is more, it was noted that EU member states fail to give concrete guidance with regard to the interpretation of the defences that hosting ISSPs would use in order for them not to be liable for the infringements that accrue within their networks. For example, with regard to the requirement of knowledge, the English legal system states that only a competent notice that allocates the precise location of the infringing content could obtain knowledge of the illicit activity, while the French legal system endorses the concept of the diligent economic operator.

Thirdly, in not defining hosting ISSPs' liability along with the heterogenous interpretations of the requirements of knowledge and expeditious removal of the allegedly infringing content, EU member states were forced to resort to their national tortious secondary liability doctrines in order to attribute liability to hosting ISSPs for intellectual property violations committed by their users. Interestingly, even though it was noted that national tortious secondary liability doctrines could offer a definition for hosting ISSPs' liability, a number of problematic issues were identified.

In particular, it was noted in chapter 2 that EU member states' courts faced discrepancies in order to apply tortious secondary liability doctrines to hosting ISSPs' activities. Indeed, secondary tortious liability rules in some jurisdictions treat hosting ISSPs as primary infringers. For instance, the joint-tortfeasance doctrine, which has an application in the English and German legal systems, considers the hosting ISSP as a primary infringer of the tortious act.¹¹⁶⁸ This doctrine therefore might raise concerns with regard to the appropriateness of applying joint-tortfeasance doctrines into the hosting ISSPs' activities. In addition, tortious secondary liability doctrines impose a duty of care which can only be assessed on a case by case basis. Yet, the imposition of a duty of care on hosting ISSPs has been subject to intense debate since Article 15 of the ECD explicitly prohibits the imposition of monitoring obligations to hosting ISSPs.

¹¹⁶⁸ Chapter 2 Section IV C. 1, 2.

Finally, another problematic issue is that tortious secondary liability rules differ from jurisdiction to jurisdiction, thus creating a patchwork of miscellaneous tort law doctrines and thus accentuating the existing legal uncertainty. As the findings indicate, based on the analysis of the three most representative EU jurisdictions, the French tort law system extends the direct breach of tort law provisions to additional actors and imposes a duty of care on hosting ISSPs which forces them to deploy preventive measures and mechanisms in order to eliminate future infringements online.¹¹⁶⁹ In similar fashion, the German legal system based on case law shapes the notion of disturber liability and imposes a reasonable duty of care on hosting ISSPs.¹¹⁷⁰ With regard to the English legal system, although UK courts apply the doctrine of joint-torfeasance within the context of hosting ISSPs' activities, to attribute a duty of care for hosting ISSPs towards the infringements online seems not to be applicable.¹¹⁷¹ As corollary, in chapter 2, it was concluded that the current legal framework under Article 14 of the ECD undermines the rights of intellectual property holders while at the same time it subordinates the rights of hosting ISSPs and internet users.

In light of this finding, in chapter 3, the narrative continued to the second legislative tool that regulates OCSSPs' liability for copyright infringements, which is the DSMD. The DSMD¹¹⁷² is relatively new since it was voted in on the 26th March 2019 by the EU Parliament. Accordingly, any assumption with regard to its implications rest on a theoretical basis. Yet, as the findings in Chapter 3 indicate, Article 17 of the DSMD, which regulates the liability of OCSSPs for copyright infringements, is controversial because it entails an array of problematic features.

Firstly, it was noted in chapter 3 Section III A. that a problematic feature of Article 17 of the DSMD is the introduction of primary liability rules. In particular, Article 17 (1) states that an OCSSP performs an act of communication to the public or an act of making available of copyrighted content to the public. The imposition of primary liability rules goes against the rationale of secondary liability theories that have been the cornerstone of e-commerce since 2000 and that safeguarded the operation of business for many hosting ISSPs and internet as a space for exchanging information between internet users.

¹¹⁶⁹ Chapter 2 Section IV C. 3.

¹¹⁷⁰ Chapter 2 Section IV C. 2.

¹¹⁷¹ Chapter 2 Section IV C. 1.

¹¹⁷² Chapter 3 Section I.

This is because the defence of knowledge, which is a requisite for triggering secondary liability rules, enabled them to escape from liability in cases where intellectual property owners were bringing lawsuits against them alleging violation of their rights. Indeed, as discussed in chapter 2, as per Article 14 of the ECD, hosting ISSPs can escape liability if they expeditiously remove the infringing content that they have been made aware of. In contrast, primary liability rules, which are now endorsed in Article 17 of the DSMD, do not require the element of knowledge. In other words, this means that under Article 17 of the DSMD, OCSSPs would be held liable for any copyright infringement that occur within their networks.

In order to escape from liability, OCSSPs have two options. Pursuant to Article 17 (4) of the DSMD, OCSSPs must either make best efforts to seek to conclude licensing agreements or to terminate the dissemination as well as prevent the reappearance of copyright infringements. However, it was noted that both requirements present challenges. On the one hand, the conclusion of licensing agreements seems impossible. Indeed, even though the full licensing of the circulated content can only be achieved via umbrella licenses, such extended collective licenses that are issued by collective societies cover only works of their members.¹¹⁷³ On the other hand, it was noted that a notice and stay down mechanism has been introduced without identifying what it entails and without defining its limits.¹¹⁷⁴ Indeed, it is questionable whether the notice and stay down system requires the implementation of filtering technological tools. What is more, the limits of this notice and stay down mechanism might be subject to different interpretations. Indeed, it is questionable whether this system points to the emergence of copyright infringements of the same nature or copyright infringements by the same user or copyright infringements of the same nature by different users or copyright infringements of the same nature by the same user.¹¹⁷⁵

Secondly, another problematic aspect addresses Article 17 (8) of the DSMD which explicitly prohibits general monitoring obligations. It was noted in chapter 3 Section III. E that this paragraph lacks practical significance since Article 17 (4) of the DSMD requires OCSSPs to prevent the reemergence of unlawful content online. The prevention of

¹¹⁷³ J. P. Quintais, "The New Copyright in the Digital Single Market Directive: A Critical Look" (2019) 1 European Intellectual Property Review 19.

¹¹⁷⁴ Chapter 3 Section III. D.

¹¹⁷⁵ This is the so called Kerntheorie and has been discussed in chapter 2 IV. B. 1; see also in *Case C-494/15 - Tommy Hilfiger Licensing* (2016) ECLI:EU:C: 2016:528, para. 34.

reappearance of unlawful content can either be achieved via filtering tools or human review.

Finally, the problematic framework of Article 17 of the DSMD culminates with the creation of a redress mechanism by OCSSPs as well as the creation of an out of court body that would address any potential disputes between OCSSPs and internet users. This is because, as the findings indicate in chapter 3 Section III. F, if those self-and out of court mechanisms are established without a specific set of principles, such as for instance the principles of accountability, consistency, proportionality, the principles of due process and the right to access to justice for internet users, as enshrined in the EU Charter of Fundamental Rights and the European Convention of Human Rights, would be jeopardised.

However, as discussed in chapter 3 Section IV, it is not only Article 17 of the DSMD that appears to be problematic. Indeed, it is the intersection of Article 17 of the DSMD with Article 14 of the ECD that is also problematic. Firstly, it was argued that a divide in the existing trend of case law might incur since there might be cases where hosting ISSPs that do not fall within the definition of OCSSPs provide services that fall under the scope of Article 17 of the DSMD.

Secondly, Article 17 of the DSMD is considered *lex specialis* to Article 14 of the ECD. However, a dual liability regime would occur. Secondary liability rules would apply in the case of trade mark infringements within the networks of hosting ISSPs and primary liability rules would be applicable for OCSSPs in case of copyright violations within their networks. This dual liability regime is contradictory since the rationale of both liability regimes is diametrically opposite. As presented in chapter 3 Section IV, the rationale of secondary liability rules is to enable hosting ISSPs to avoid liability under the defense of lack of knowledge of the illicit activity. It is this rationale that permitted e-commerce to thrive and enabled European Digital Single Market to compete with its US counterparts. In contrast to secondary liability rules, primary liability rules do not offer the defense of lack of knowledge. Indeed, under the regime of primary liability, once the infringement takes place, OCSSPs would be subject to liability.

What is more, this dual liability regime would split the burden of proof for the parties at stake. Under Article 14 of the ECD, right holders must provide evidence that they identified the infringing content and sent a valid notice to hosting ISSPs entail the precise allocation of the allegedly infringing content. In contrast, under Article 17 of the DSMD

that includes a notice and stay down regime, OCSSPs must demonstrate that they deployed all the preventive mechanisms to terminate the dissemination of unauthorized content within their networks as well as prevent its reappearance in the future.

As elaborated in chapter 3 IV, this understanding might lead to the creation of a monopoly in the field of OCSSPs. For instance, popular OCSSPs would be empowered in the Digital Single Market since they have already developed their own technological tools and thus own the technological know-how to terminate online infringements. What is more, given that the burden of proof rests on the OCSSPs to prove that they undertook all the necessary measures to stop the infringements, many new OCSSPs will be hesitant to enter the Digital Single Market since they would prefer to invest in other business model with lower burden of proof in the context of liability. Therefore, the main aim of the European policymakers, namely to facilitate e-commerce players and boost innovation within the Digital Single Market would be in peril.

On the basis of this analysis, it is questionable what the implications of an outdated and problematic framework under the ECD and the DSMD would be for the parties whose interests are involved. Therefore, it was necessary to examine the implications of both legislative tools to intellectual property holders, internet users and hosting ISSPs.

Firstly, it was noted in the Concluding remarks of Part I that legal uncertainty might pose a serious interference to the business model of hosting ISSPs. This is the case of dual use technologies which can “be used to violate third parties’ rights as well as promote social beneficial uses.”¹¹⁷⁶ Indeed, in order to be exonerated from liability, hosting ISSPs might be forced to undertake expensive precautionary measures and thus their right to conduct business as per Article 16 of the EU Charter of Fundamental Rights would be disrupted. In this vein, new hosting ISSPs that wish to enter the Digital Single Market would be hesitant. Therefore, one of the core elements of the Digital Single Market, which is the creation of new business models, would be jeopardised at supranational and national level.¹¹⁷⁷

¹¹⁷⁶ G. Frosio, “Why keep a dog and bark yourself? From intermediary liability to responsibility” (2017) Centre for International Intellectual Property Studies 8.

¹¹⁷⁷ J. Scott Marcus, G. Petropoulos and T. Yeung, “Contribution to Growth: The European Digital Single Market Delivering economic benefits for citizens and businesses” (2019) IMCO Committee 11 is available at <[http://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU\(2019\)631044_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2019/631044/IPOL_STU(2019)631044_EN.pdf)> last accessed 28 December 2019; EU Commission, “A Digital Single Market Strategy for Europe” COM (2015) 192 final 3.

Secondly, legal uncertainty might encroach upon internet users' fundamental right of freedom of expression, as per Article 11 of the EU Charter of Fundamental rights. Being subject to liability rules, hosting ISSPs might act as "overzealous police officers."¹¹⁷⁸ Subsequently, this could lead to an over-enforcement of rights online or the blocking of websites without adequate investigation of the allegedly illicit activities that might occur. Therefore, this outcome might limit the amount of information available online and thus restrict users' right to information.

Thirdly, legal uncertainty might interfere to intellectual property holders' rights. The lack of definition of hosting ISSPs' liability, along with a patchwork of diverse tortious secondary liability doctrines under the ECD liability regime, might result to an uncertain enforcement of intellectual property rights. As corollary, intellectual property holders might not be able to successfully seek redress for the violation of their rights and thus compensate their losses in cases of intellectual property infringements. What is more, under Article 17 of the DSMD, intellectual property holders might find difficulties in seeking redress for their damages too. As discussed in chapter 3 Section III A, it is questionable how intellectual property holders might seek redress for the infringements of their rights within the platforms that fall outside the scope of Article 17 of the DSMD but provide services that fall within the meaning of giving "the public access to copyright-protected works or other protected subject matter uploaded by its users."

In the light of the above, the outdated legal framework that regulates the hosting ISSPs' liability under Article 14 of the ECD, the problematic legal framework that regulates the sub-types of hosting ISSPs, namely OCSSPs' liability under Article 17 of the DSMD, as well as the negative implications on the interests of the parties involved, could set out the normative justifications for Part II of this thesis. Subsequently, Part II put forward a set of recommendations for a new regulatory framework for hosting ISSPs with regard to copyright and trade mark infringements.

III. Recommendations

The set of recommendations that could be included in a new legal reform to achieve a more balanced legal framework to regulate hosting ISSPs' liability was articulated in Part

¹¹⁷⁸ D. Rowland, U. Kohl and A. Charlesworth, *Information Technology Law* (5th ed, Routledge 2017) 87.

II. This new framework is based on a set of responsibilities for hosting ISSPs that would be accountable to a hosting ISSP supervisory authority.

From a normative perspective, in chapter 4 Section II it was argued that hosting ISSPs nowadays do not merely host content stored by their users. Rather, their new role is extended to those of information gatekeepers, creators of public policies, enforcers and adjudicators of intellectual property rights. Yet, these new roles cannot be compromised with hosting ISSPs' private interests. Hosting ISSPs are private corporations with business partners and interests and this might lead them to adopt a lower standard for protecting internet users' rights.¹¹⁷⁹ In this light, the establishment of a responsibility framework for ISSPs might offer a greater degree of protection for the rights of internet users/ online consumers.

However, apart from the normative considerations that warrant the ascription of a responsibility framework for hosting ISSPs, there is a strong theoretical background upon which a responsibility framework based on co-regulation for hosting ISSPs could be based. This new framework could draw upon two regulatory theories for the internet. More specifically, as discussed in chapter 4, Reidelberg's theory and Lessig's theory envisage a co-regulatory model within the digital ecosystem. In this light, from the perspective of Reidelberg's theory, the state could regulate online activities of users/ consumers with the cooperation of hosting ISSPs. Further, from the perspective of Lessig's theory governmental authorities could ascribe a set of responsibilities to hosting ISSPs with the aim to terminate the circulation of unauthorised content and counterfeit goods in the digital world. Building upon the above regulatory theories of the internet, it seems that governmental authorities could also endorse the establishment of a hosting ISSP supervisory authority. Without restricting the access of intellectual property holders to the courts, the proposed hosting ISSP supervisory authority could impose sanctions to hosting ISSPs for illicit activities that might take place online.

Having discussed the normative considerations and theoretical underpinnings for imposing a responsibility framework for hosting ISSPs through which they would be accountable to a proposed hosting ISSP supervisory authority, a set of responsibilities for hosting ISSPs were presented. More specifically, in chapter 4 it was argued that a duty of

¹¹⁷⁹ O. Lysnkey, "Regulation by Platforms: The Impact on Fundamental Rights" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018) 92.

care should be imposed on hosting ISSPs with regard to the dissemination of infringing content within their networks. Such a duty of care amounts to the responsibility of hosting ISSPs to terminate the dissemination of infringing content and also prevent its reappearance.

However, the imposition of a duty of care does not come without criticism. Firstly, it has been argued that the duty of care contravenes with Article 14 of the ECD which states that hosting ISSPs' nature is passive. Yet, this argument is not solid. This is because, as the findings indicate, a growing trend in case law treats hosting ISSPs as active entities. For instance, it was noted in chapter 4 that a number of judgements at European and national level confirm this tendency.

Moreover, it was argued that a duty of care is outside the rationale of the ECD that, in Article 15 of the ECD, prohibits the adoption of general monitoring obligations. This thesis argued that a duty of care does not amount to general monitoring obligations. Rather, as stated in Recital 48 "This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply duties of care, which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities." Otherwise, there would be no reason to state in the preamble of the ECD that a duty of care could be imposed overall.

Further, it has been argued that a duty of care would amount to the implementation of filtering-based technology or human review of the content that is disseminated online. However, it shall be up to the hosting ISSPs to decide which option fits better with their business model.

This means that if filtering-based technology would be preferred, hosting ISSPs would not be able to argue that they lack knowledge of the illicit activities online. This is a very likely scenario which could make hosting ISSPs subject to liability rules. This thesis argued that the adoption of proactive measures would not result to the liability of hosting ISSPs. In order to avoid this outcome, chapter 4 IV. D i referred to the US legal system and examined the principle of the Good Samaritan clause. It has been suggested that a similar principle could also be embedded in the proposed responsibility framework for hosting ISSPs in order to avoid any serious interference with the right of hosting ISSPs to conduct business, as set forth in Article 16 of the EU Charter of Fundamental Rights.

However, although the imposition of the Good Samaritan clause could safeguard hosting ISSPs' fundamental right to business, the imposition of a duty of care might pose risks to internet users' rights. For instance, although filtering technology is highly sophisticated and a small margin of error may be incurred with regard to the removal of infringing content, a risk to censorship of the content that users have uploaded is apparent.

Accordingly, to avoid this outcome, in chapter 5 it was noted that a transparency obligation should be implemented in hosting ISSPs' activities with regard to the removal of infringing content or counterfeit goods. However, even though many commentators argue that transparency might increase the transaction costs of hosting ISSPs, this thesis argued that a transparency obligation would have merits not only for users' fundamental rights but also for hosting ISSPs' interests.

With regard to users' fundamental rights, a transparency obligation would enhance the rule of law and due process. Indeed, as explained in chapter 5 IV, users will be provided with information relating to the removal of their content and thus they would be able to ascertain whether hosting ISSPs have complied with the rules. Also, in the context of transparency, users would be able to challenge the decision of removal if they do not agree. Moreover, the transparency obligation might enhance the trust of internet users since they would be aware of the thresholds that triggered the removal of their content and whether this decision was based on legitimate reasoning. Finally, consumers' trust towards the online sales in general would be increased since the provision of information would make consumers aware as to how the online market places supervise the circulation of goods online as well as their methods to combat pirated goods.

Nevertheless, the introduction of a transparency obligation would not only safeguard users' rights but also induce hosting ISSPs to adopt better methods. Given that their practices would be disclosed to their internet users/ online consumers, hosting ISSPs would be incentivised to conduct a prior examination of their practices before they put them into practice and evaluate their results. Hence, transparency would eliminate any errors or malfunctions in the practices that hosting ISSPs adopt and thus improve the principles of good governance.

Chapter 5 argued that, however necessary a transparency obligation might be, it is crucial to identify the limits within which such a transparency obligation would be exercised. Otherwise, the potential advantages a transparency obligation might have, would lead to

adverse results for hosting ISSPs. It was suggested that a transparency obligation would be required in different contexts. In this respect, it was recommended that a partial transparency obligation should be imposed with the introduction of a right to explanation so that users can request more information about the removal of their content while at the same time hosting ISSPs' algorithm would not be disclosed and thus their business model would be safeguarded. Moreover, it was recommended that a transparency obligation should be applicable to the terms of service of hosting ISSPs. This means that users would be notified when their content has been removed and would be able to challenge the removal via the counter-notification procedures of hosting ISSPs. As a result, the right to a fair trial and the right to appropriate remedy of internet users/online consumers would be safeguarded. Finally, a transparency obligation should include the issue of transparency reports. Those reports would inform the users about the removals related to unauthorized content or fake goods per country as well as the specific reasons that trigger their removal.

Finally, chapter 6 presented the last recommendation to complete a responsibility framework for hosting ISSPs based on co-regulation, namely the establishment of a hosting ISSP supervisory authority. This recommendation has already been instigated at the European as well as national level. For instance, an authority envisaged in Article 17 (9) of the DSMD states that "Member States shall also ensure that out-of-court redress mechanisms are available for the settlement of disputes." Although Article 17 (9) of the DSMD does not entail any precise guidance as to the principles and functions of this authority, it offers a hint of such an authority. What is more, as the findings indicate in chapter 6, a number of national member states have already created such authorities that deal with disputes between hosting ISSPs and right holders. To my knowledge, so far Greece, Italy, England and Spain have initiated similar authorities. Although certain flaws in the operation of such authorities were identified, this does not mean that they are not a good start.

Accordingly, the creation of an ISSP supervisory authority was recommended in chapter 6. Building upon the previous chapters, the proposed hosting ISSP supervisory authority would function through a number of principles. Such principles concern the independence of the authority, the consistent and proportionate decisions it would issue and the accountability it should have towards a hierarchically superior administrative body. Further, the proposed supervisory authority would enforce intellectual property

rights online, offer a complaints mechanism for users and promote awareness to users and consumers for online piracy. With regard to the enforcement of intellectual property rights, the current legal framework under Article 14 of the ECD and Article 17 of the DSMD does not offer adequate protection for the rights of content owners and brand owners. In this light, the proposed ISSP supervisory authority would provide to right holders a better redress mechanism in order to safeguard their rights.

Further, the proposed ISSP supervisory authority would offer a complaints' mechanism for internet users and online consumers and would be accessible to those internet users and online consumers whose counter-notifications have been dismissed or ignored by hosting ISSPs. In this sense, a complaints' mechanism for users would enhance the right of users to access justice since they would be able to submit a complaint against the hosting ISSP to the proposed ISSP supervisory authority. Following this, the complaint of the user would be thoroughly examined and a fine would be imposed to the hosting ISSP if the removal lacks legitimate basis.

Moreover, the proposed ISSP supervisory authority should also play an educative role. As explored in chapter 6 V. C, in parallel with its enforcement duties and users' complaints resolution, educational campaigns and promotion of awareness among users about the detrimental effect of piracy on right holders' rights as well as about the access to remedy mechanisms would have merits.

Therefore, on the basis of the recommendations provided, a responsibility framework based on a co-regulatory approach might offer a more balanced framework for the rights of all the parties at stake, namely intellectual property holders, internet users and hosting ISSPs. This balanced framework would be in accordance with the existing EU case law that advocates in favor of an equilibrium between the different interests at stake. In addition, this framework would be in accordance with the rationale of the secondary liability regime where the requirement of knowledge is substantial part and enables hosting ISSPs to use it as a defense in order to escape from liability.

In the light of the above, the recommendations detailed in this thesis would impact policy-making in relation to the regulatory framework of hosting ISSPs and assist European policy makers in crafting a more robust legal framework that considers the interests of all parties involved.

IV. Epilogue

A. *Note for Brexit*

This research started after the Brexit Referendum. Whether or not UK leaves the European Union, the consideration of this set of recommendations would assist the UK policy makers in the UK Intellectual Property Office to establish a more robust legal framework with regard to hosting ISSPs. The example of the UK legislation and case law in view of the hosting ISSPs' liability was drawn in order to demonstrate the fragmented EU legislative framework under the ECD which was transposed in the UK national legal system in 2000 and continues to be in force. With regard to the DSMD, there are no initiatives, to my knowledge, for implementing the DSMD into UK national legal system.

B. *Note for the DSMD*

This research started in September 2016 and coincided with the release of the Proposal for a Copyright in the Digital Single Market Directive. As many scholars warned me, given that hosting ISSPs' liability is a cutting-edge issue, many amendments and unexpected changes in the suggested provisions were to be anticipated until the final draft of the Copyright in the Digital Single Market Directive. However, I decided to accept this challenge and write a thesis on the regulatory framework of hosting ISSPs for copyright and trade mark infringements, including a critical evaluation of the whole legislative procedure by which the DSMD was adopted on the 26th of March. Due to the novelty of this Directive, case law at European as well as national level that would provide more clarifications on Article 17 of the DSMD had not yet been established. For this reason, given the lack of case law with regard to Article 17 of the DSMD, my critical analysis rests on the problematic features of Article 17 of the DSMD and its correlation with Article 14 of the ECD.

Appendix

I. European Commission's Proposal for a Copyright in the Digital Single Market Directive on the 14th September 2016

Article 13

Use of protected content by information society service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users

1. Information society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users shall, in cooperation with rightholders, take measures to ensure the functioning of agreements concluded with rightholders for the use of their works or other subject-matter or to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate and proportionate. The service providers shall provide rightholders with adequate information on the functioning and the deployment of the measures, as well as, adequate reporting on the recognition and use of the works and other subject-matter.

2. Member States shall ensure that the service providers referred to in paragraph 1 put in place complaints and redress mechanisms that are available to users in case of disputes over the application of the measures referred to in paragraph 1.

3. Member States shall facilitate, where appropriate, the cooperation between the information society service providers and rightholders through stakeholder dialogues to define best practices, such as appropriate and proportionate content recognition technologies, taking into account, among others, the nature of the services, the availability of the technologies and their effectiveness in light of technological developments.

II. EU Council text 25 May 2018

Article 13

Use of protected content by online content sharing service providers

1. Member States shall provide that an online content sharing service provider performs an act of communication to the public or an act of making available to the public when it gives the public access to copyright protected works or other protected subject matter uploaded by its users. An online content sharing service provider shall obtain an authorisation from the rightholders referred to in Article 3(1) and (2) of Directive 2001/29/EC in order to communicate or make available to the public works or other subject matter. Where no such authorisation has been obtained, the service provider shall prevent the availability on its service of those works and other subject matter, including through the application of measures referred to in paragraph 4. This subparagraph shall apply without prejudice to exceptions and limitations provided for in Union law. Member States shall provide that when an authorisation has been obtained, including via a licensing agreement, by an online content sharing service provider, this authorisation shall also cover acts of uploading by the users of the service falling within Article 3 of Directive 2001/29/EC when they are not acting on a commercial basis.

2. Deleted.

3. When an online content sharing service provider performs an act of communication to the public or an act of making available to the public, it shall not be eligible for the exemption of liability provided for in Article 14 of Directive 2000/31/EC for unauthorised acts of communication to the public and making available to the public, without prejudice to the possible application of Article 14 of Directive 2000/31/EC to those services for purposes other than copyright relevant acts.

4. In the absence of the authorisation referred to in the second subparagraph of paragraph 1, Member States shall provide that an online content sharing service provider shall not be liable for acts of communication to the public or making available to the public within the meaning of this Article when: (a) it demonstrates that it has made best efforts to prevent the availability of specific works or other subject matter by implementing effective and proportionate measures, in accordance with paragraph 5, to prevent the availability on its services of the specific works or other subject matter identified by rightholders and for which the rightholders have provided the service with relevant and necessary information for the application of these measures; and (b) upon notification by rightholders of works or other subject matter, it has acted expeditiously to remove or disable access to these works or other subject matter and it demonstrates that it has

made its best efforts to prevent their future availability through the measures referred to in point (a).

5. The measures referred to in point (a) of paragraph 4 shall be effective and proportionate, taking into account, among other factors: (a) the nature and size of the services, in particular whether they are provided by a microenterprise or a small-sized enterprise within the meaning of Title I of the Annex to Commission Recommendation 2003/361/EC, and their audience; (b) the amount and the type of works or other subject matter uploaded by the users of the services; (c) the availability and costs of the measures as well as their effectiveness in light of technological developments in line with the industry best practice referred to in paragraph 8.

6. Member States shall ensure that online content sharing service providers and rightholders cooperate with each other in a diligent manner to ensure the effective functioning of the measures referred to in point (a) of paragraph 4 over time. Online content sharing service providers shall provide rightholders, at their request, with adequate information on the deployment and functioning of these measures to allow the assessment of their effectiveness, in particular information on the type of measures used and, where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements.

7. Member States shall ensure that the measures referred to in paragraph 4 are implemented by the online content sharing service provider without prejudice to the possibility for their users to benefit from exceptions or limitations to copyright. For that purpose, the service provider shall put in place a complaint and redress mechanism that is available to users of the service in case of disputes over the application of the measures to their content. Complaints submitted under this mechanism shall be processed by the online content sharing service provider in cooperation with relevant rightholders within a reasonable period of time. Rightholders shall duly justify the reasons for their requests to remove or block access to their specific works or other subject matter. Member States shall endeavour to put in place independent bodies to assess complaints related to the application of the measures.

8. The Commission and the Member States shall encourage stakeholder dialogues to define best practices for the measures referred to in point (a) of paragraph 4. Member States shall also endeavour to establish mechanisms to facilitate the assessment of the

effectiveness and proportionality of these measures and provide the Commission regularly with information on those mechanisms. The Commission shall, in consultation with online content sharing service providers, rightholders and other relevant stakeholders and taking into account the results of the stakeholder dialogues and the national mechanisms, issue guidance on the application of the measures referred to in point (a) of paragraph 4.

III. EU Parliament text 26 June 2018

Article 13

Use of protected content by information society service providers storing and/or giving access to significant amounts of works and other subject-matter uploaded by their users

1. Information society service providers that store and/or provide to the public access to copyright-protected works or other subject-matter uploaded by their users, thereby going beyond the mere provision of physical facilities and performing an act of communication to the public, shall conclude fair and balanced licensing agreements with any requesting rightholders. Under the terms of the agreements, such service providers shall, in cooperation with rightholders, take measures to ensure the effective and transparent functioning of the agreements concluded with rightholders for the use of their works or other subject matter

Where, in the absence of a request from the rightholder, no licensing agreements are concluded pursuant to the first subparagraph, or where information society service providers that store significant amounts of copyright-protected works or other subject-matter and/or provide to the public access thereto are eligible for the liability exemption provided for in Article 14 of Directive 2000/31/EC, those providers shall take measures to prevent the availability on their services of works or other subject-matter identified by rightholders through the cooperation with the service providers. Those measures, such as the use of effective content recognition technologies, shall be appropriate, proportionate and compliant with the relevant industry standards. The service providers shall provide rightholders with adequate and timely information on the functioning and the deployment of the measures, as well as, when relevant, adequate reporting on the recognition and use of the rightholders' works and other subject-matter. Rightholders shall provide the information society service provider with the relevant and necessary

data to allow the effective functioning of the measures deployed by the provider in accordance with this Article.

2. Member States shall ensure that the service providers referred to in paragraph 1 put in place effective mechanisms for rightholders to request licences and complaints and redress mechanisms that are available to users in case of disputes over the application of the measures referred to in paragraph 1, in particular regarding the possible application of an exception or limitation to any rights covering the content concerned. When such a mechanism is activated, any remuneration accruing from the disputed content during the course of the procedure shall not be distributed to either party until such time as the dispute has been resolved under the mechanism.

The complaints and redress mechanism established pursuant to the first subparagraph shall ensure that users and rightholders have access to sufficient information on the relevant exceptions and limitations that may apply in relation to content affected by the measures referred to in paragraph 1.

Any complaint filed by a user under the mechanism referred to in the first subparagraph shall be processed by the relevant rightholder within a reasonable period of time. The rightholder shall duly justify his or her decision with regard to the complaint.

2a. Where information society providers take the measures referred to in paragraph 1, such measures shall be in full compliance with Directive 95/46/EC and Directive 2002/58/EC. Measures to prevent the unauthorised making available of copyright-protected works or other subjectmatter shall be limited to specifically identified and duly notified works and shall not involve active monitoring of the entire data of each user of the service.

3. Member States shall facilitate, where appropriate, the cooperation between the information society service providers and rightholders through stakeholder dialogues to define best practices, such as appropriate and proportionate content recognition technologies, taking into account, inter alia, the nature of the services, the availability and affordability of the technologies and their effectiveness in respect of the range of types of content and in light of technological developments. In cooperation with the Member States, the Commission shall encourage the exchange of best practice across the Union

regarding the results of any cooperation established pursuant to paragraph 1 of this Article.

Member States shall encourage industry-led solutions to address sector-specific issues and the effective enforcement of existing measures to tackle piracy, including raising awareness of legal means of accessing copyright-protected works or other subject matter.

3a. Member States shall provide that disputes between rightholders and information society providers concerning the application of paragraph 1 of this Article may be submitted to an alternative dispute resolution mechanism.

Member States shall create or designate an impartial body with relevant expertise to assist the parties in the resolution of their dispute under the mechanism provided for in the first subparagraph. No later than ... [date mentioned in Article 21(1)] Member States shall notify to the Commission the body referred to in subparagraph 2.

IV. EU Parliament text 12 September 2018

Article 13

Use of protected content by online content sharing service providers storing and giving access to large amounts of works and other subject-matter uploaded by their users

1. Without prejudice to Article 3(1) and (2) of Directive 2001/29/EC, online content sharing service providers perform an act of communication to the public. They shall therefore conclude fair and appropriate licensing agreements with right holders.

2. Licensing agreements which are concluded by online content sharing service providers with right holders for the acts of communication referred to in paragraph 1, shall cover the liability for works uploaded by the users of such online content sharing services in line with the terms and conditions set out in the licensing agreement, provided that such users do not act for commercial purposes. 2a. Member States shall provide that where right holders do not wish to conclude licensing agreements, online content sharing service providers and right holders shall cooperate in good faith in order to ensure that unauthorised protected works or other subject matter are not available on their services. Cooperation between online content service providers and right holders shall not lead to preventing the availability of non-infringing works or other protected subject matter,

including those covered by an exception or limitation to copyright. 2b. Member States shall ensure that online content sharing service providers referred to in paragraph 1 put in place effective and expeditious complaints and redress mechanisms that are available to users in case the cooperation referred to in paragraph 2a leads to unjustified removals of their content. Any complaint filed under such mechanisms shall be processed without undue delay and be subject to human review. Right holders shall reasonably justify their decisions to avoid arbitrary dismissal of complaints. Moreover, in accordance with Directive 95/46/EC, Directive 2002/58/EC and the General Data Protection Regulation, the cooperation shall not lead to any identification of individual users nor the processing of their personal data. Member States shall also ensure that users have access to an independent body for the resolution of disputes as well as to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright rules.

3. As of [date of entry into force of this directive], the Commission and the Member States shall organise dialogues between stakeholders to harmonise and to define best practices and issue guidance to ensure the functioning of licensing agreements and on cooperation between online content sharing service providers and right holders for the use of their works or other subject matter within the meaning of this Directive. When defining best practices, special account shall be taken of fundamental rights, the use of exceptions and limitations as well as ensuring that the burden on SMEs remains appropriate and that automated blocking of content is avoided.

Article 13a. Member States shall provide that disputes between successors in title and information society services regarding the application of Article 13(1) may be subject to an alternative dispute resolution system. Member States shall establish or designate an impartial body with the necessary expertise, with the aim of helping the parties to settle their disputes under this system. The Member States shall inform the Commission of the establishment of this body no later than (date mentioned in Article 21(1)).

Article 13b. Use of protected content by information society services providing automated image referencing Member States shall ensure that information society service providers that automatically reproduce or refer to significant amounts of copyright-protected visual works and make them available to the public for the purpose of indexing and referencing conclude fair and balanced licensing agreements with any requesting rightholders in order to ensure their fair remuneration. Such remuneration

may be managed by the collective management organisation of the rightholders concerned.

V. Compromised Text after the trialogues' negotiations 20 February 2019

Article 17

Use of protected content by online content sharing service providers

1. Member States shall provide that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users. An online content-sharing service provider shall therefore obtain an authorisation from the rightholders referred to in Article 3(1) and (2) of Directive 2001/29/EC, for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter.

2. Member States shall provide that when an authorisation has been obtained, including via a licensing agreement, by an online content sharing service provider, this authorisation shall also cover acts carried out by users of the services falling within Article 3 of Directive 2001/29/EC when they are not acting on a commercial basis or their activity does not generate significant revenues.

3. When an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in this Directive, the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article. The first subparagraph of this paragraph shall not affect the possible application of Article 14(1) of Directive 2000/31/EC to those service providers for purposes falling outside the scope of this Directive.

4. If no authorisation is granted, online content-sharing service providers shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter, unless the service providers demonstrate that they have: (a) made best efforts to obtain an authorisation, and (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from, their websites the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).

5. In determining whether the service provider has complied with its obligations under paragraph 4, and in light of the principle of proportionality, the following elements, among others, shall be taken into account: (a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers

6. Member States shall provide that, in respect of new online content-sharing service providers the services of which have been available to the public in the Union for less than three years and which have an annual turnover below EUR 10 million, calculated in accordance with Commission Recommendation 2003/361/EC20, the conditions under the liability regime set out in paragraph 4 are limited to compliance with point (a) of paragraph 4 and to acting expeditiously, upon receiving a sufficiently substantiated notice, to disable access to the notified works or other subject matter or to remove those works or other subject matter from their websites . Where the average number of monthly unique visitors of such service providers exceeds 5 million, calculated on the basis of the previous calendar year, they shall also demonstrate that they have made best efforts to prevent further uploads of the notified works and other subject matter for which the rightholders have provided relevant and necessary information.

7. The cooperation between online content-sharing service providers and rightholders shall not result in the prevention of the availability of works or other subject matter uploaded by users, which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation. Member

States shall ensure that users in each Member State are able to rely on any of the following existing exceptions or limitations when uploading and making available content generated by users on online content-sharing services: (a) quotation, criticism, review; (b) use for the purpose of caricature, parody or pastiche.

8. The application of this Article shall not lead to any general monitoring obligation. Member States shall provide that online content-sharing service providers provide rightholders, at their request, with adequate information on the functioning of their practices with regard to the cooperation referred to in paragraph 4 and, where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements.

9. Member States shall provide that online content-sharing service providers put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them.

Where rightholders request to have access to their specific works or other subject matter disabled or those works or other subject matter removed, they shall duly justify the reasons for their requests. Complaints submitted under the mechanism provided for in the first subparagraph shall be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review. Member States shall also ensure that out-of-court redress mechanisms are available for the settlement of disputes. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies. In particular, Member States shall ensure that users have access to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright and related rights.

This Directive shall in no way affect legitimate uses, such as uses under exceptions or limitations provided for in Union law, and shall not lead to any identification of individual users nor to the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679.

Online content-sharing service providers shall inform their users in their terms and conditions that they can use works and other subject matter under exceptions or limitations to copyright and related rights provided for in Union law.

10. As of ...[date of entry into force of this Directive] the Commission, in cooperation with the Member States, shall organise stakeholder dialogues to discuss best practices for cooperation between online content-sharing service providers and rightholders. The Commission shall, in consultation with online content-sharing service providers, rightholders, users' organisations and other relevant stakeholders, and taking into account the results of the stakeholder dialogues, issue guidance on the application of this Article, in particular regarding the cooperation referred to in paragraph 4. When discussing best practices, special account shall be taken, among other things, of the need to balance fundamental rights and of the use of exceptions and limitations. For the purpose of the stakeholder dialogues, users' organisations shall have access to adequate information from online content-sharing service providers on the functioning of their practices with regard to paragraph 4.

VI. Final text of the Copyright in the Digital Single Market Directive as voted by the EU Parliament on the 26th of March 2019

Article 17

Use of protected content by online content-sharing service providers

1. Member States shall provide that an online content-sharing service provider performs an act of communication to the public or an act of making available to the public for the purposes of this Directive when it gives the public access to copyright-protected works or other protected subject matter uploaded by its users. An online content-sharing service provider shall therefore obtain an authorisation from the rightholders referred to in Article 3(1) and (2) of Directive 2001/29/EC, for instance by concluding a licensing agreement, in order to communicate to the public or make available to the public works or other subject matter.

2. Member States shall provide that, where an online content-sharing service provider obtains an authorisation, for instance by concluding a licensing agreement, that authorisation shall also cover acts carried out by users of the services falling within the

scope of Article 3 of Directive 2001/29/EC when they are not acting on a commercial basis or where their activity does not generate significant revenues.

3. When an online content-sharing service provider performs an act of communication to the public or an act of making available to the public under the conditions laid down in this Directive, the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article. The first subparagraph of this paragraph shall not affect the possible application of Article 14(1) of Directive 2000/31/EC to those service providers for purposes falling outside the scope of this Directive.

4. If no authorisation is granted, online content-sharing service providers shall be liable for unauthorised acts of communication to the public, including making available to the public, of copyright-protected works and other subject matter, unless the service providers demonstrate that they have: (a) made best efforts to obtain an authorisation, and (b) made, in accordance with high industry standards of professional diligence, best efforts to ensure the unavailability of specific works and other subject matter for which the rightholders have provided the service providers with the relevant and necessary information; and in any event (c) acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from, their websites the notified works or other subject matter, and made best efforts to prevent their future uploads in accordance with point (b).

5. In determining whether the service provider has complied with its obligations under paragraph 4, and in light of the principle of proportionality, the following elements, among others, shall be taken into account: (a) the type, the audience and the size of the service and the type of works or other subject matter uploaded by the users of the service; and (b) the availability of suitable and effective means and their cost for service providers.

6. Member States shall provide that, in respect of new online content-sharing service providers the services of which have been available to the public in the Union for less than three years and which have an annual turnover below EUR 10 million, calculated in accordance with Commission Recommendation 2003/361/EC²⁰, the conditions under the liability regime set out in paragraph 4 are limited to compliance with point (a) of paragraph 4 and to acting expeditiously, upon receiving a sufficiently substantiated notice, to disable access to the notified works or other subject matter or to remove those works or other subject matter from their websites . Where the average number of

monthly unique visitors of such service providers exceeds 5 million, calculated on the basis of the previous calendar year, they shall also demonstrate that they have made best efforts to prevent further uploads of the notified works and other subject matter for which the rightholders have provided relevant and necessary information.

7. The cooperation between online content-sharing service providers and rightholders shall not result in the prevention of the availability of works or other subject matter uploaded by users, which do not infringe copyright and related rights, including where such works or other subject matter are covered by an exception or limitation. Member States shall ensure that users in each Member State are able to rely on any of the following existing exceptions or limitations when uploading and making available content generated by users on online content-sharing services: (a) quotation, criticism, review; (b) use for the purpose of caricature, parody or pastiche.

8. The application of this Article shall not lead to any general monitoring obligation. Member States shall provide that online content-sharing service providers provide rightholders, at their request, with adequate information on the functioning of their practices with regard to the cooperation referred to in paragraph 4 and, where licensing agreements are concluded between service providers and rightholders, information on the use of content covered by the agreements.

9. Member States shall provide that online content-sharing service providers put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them.

Where rightholders request to have access to their specific works or other subject matter disabled or those works or other subject matter removed, they shall duly justify the reasons for their requests. Complaints submitted under the mechanism provided for in the first subparagraph shall be processed without undue delay, and decisions to disable access to or remove uploaded content shall be subject to human review. Member States shall also ensure that out-of-court redress mechanisms are available for the settlement of disputes. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies. In particular, Member States

shall ensure that users have access to a court or another relevant judicial authority to assert the use of an exception or limitation to copyright and related rights.

This Directive shall in no way affect legitimate uses, such as uses under exceptions or limitations provided for in Union law and shall not lead to any identification of individual users nor to the processing of personal data, except in accordance with Directive 2002/58/EC and Regulation (EU) 2016/679. Online content-sharing service providers shall inform their users in their terms and conditions that they can use works and other subject matter under exceptions or limitations to copyright and related rights provided for in Union law.

10. As of ...[date of entry into force of this Directive] the Commission, in cooperation with the Member States, shall organise stakeholder dialogues to discuss best practices for cooperation between online content-sharing service providers and rightholders. The Commission shall, in consultation with online content-sharing service providers, rightholders, users' organisations and other relevant stakeholders, and taking into account the results of the stakeholder dialogues, issue guidance on the application of this Article, in particular regarding the cooperation referred to in paragraph 4. When discussing best practices, special account shall be taken, among other things, of the need to balance fundamental rights and of the use of exceptions and limitations. For the purpose of the stakeholder dialogues, users' organisations shall have access to adequate information from online content-sharing service providers on the functioning of their practices with regard to paragraph 4.

Bibliography

I. Primary sources

A. *EU Legislation*

AI White Paper, “Artificial Intelligence at the service of the citizen” is available at <<https://ai-white-paper.readthedocs.io/en/latest/>> last accessed 9 January 2019.

Article 29 Working Party “Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679” adopted on 3 October 2017.

Article 29 Working Party, “Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679” (2018) 25.

Article 29 Working Party, “Guidelines on consent under Regulation 2016/679” (2018) 5.

Article 29 Working Party, “Opinion 4/2007 on the concept of personal data” (WP 136) 20 June 2007.

Article 29- Data Protection Working Party, “Guidelines for identifying a controller or processor’s lead supervisory authority” adopted on 13 December 2016.

Article 29 – Data Protection Working Party, “Recent examples of enforcement actions carried out by data protection authorities” adopted on January 2005.

Article 29 – Data Protection Working Party, “WP 37: Privacy on the Internet - An integrated EU Approach to On-line Data Protection” adopted on 21 November 2000.

ARTICLE 19, “Germany: Responding to ‘hate speech: Country report” (2018) is available at <<https://www.article19.org/wp-content/uploads/2018/07/Germany-Responding-to-%E2%80%98hate-speech%E2%80%99-v3-WEB.pdf>> last accessed 24 April 2019.

ARTICLE 19, “Germany: The Act to Improve Enforcement of the Law in Social Networks” (2017) is available at <<https://www.article19.org/wp-content/uploads/2017/09/170901-Legal-Analysis-German-NetzDG-Act.pdf>> last accessed 11 January 2019.

Citizens' summary EU action plan on “enforcing intellectual property rights” (2015) is available at < <file:///C:/Users/br918285/Downloads/CS-EN.pdf>> last accessed 24 April 2019.

Council Directive (EC) 2000/31 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] O.J. L 178.

Council Directive (EC) 2001/29 on the harmonisation of certain aspects of copyright and related rights in the information society (2001) O.J. L 167.

Council Directive (EC) 2004/48/EC on the enforcement of intellectual property rights (2004) O.J. L 157.

Council Directive (EC) 2003/33/EC on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products (2003) O.J. L 152.

Council Directive (EC) 2019/790/EC of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (2019) OJ L 130.

Council Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities (2018) OJ L 303.

Council Directive (EU) 2013/11/EU of the European parliament and of the Council on Alternative Dispute Resolution for consumers (2013) OJ L 165.

Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (2016) O.J. L 119.

Council Regulation (EU) No 524/2013 of the European parliament and of the Council on online dispute resolution for consumers (2013) OJ L 165.

Committee on Economic and Monetary Affairs, “On the overview and structure of financial supervision and regulation in the U.S Report of the Committee on Economic and Monetary Affairs on the overview and structure of financial supervision and regulation in the U.S” (2015) <http://www.europarl.europa.eu/RegData/etudes/STUD/2015/492470/IPOL_STU%282015%29492470_EN.pdf> last accessed 15 December 2018.

Committee of Ministers, “Recommendation to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters” CM/ Rec (2008).

Committee of Ministers, “Recommendation to member states on measures to promote the public service value of the Internet” CM/ Rec (2007).

Committee of Ministers, “Recommendation to member States on the roles and responsibilities of internet intermediaries” CM/Rec (2018).

Committee of Ministers, “Guide to good practice in respect of domestic remedies (adopted by the Committee of Ministers on 18 September 2013)” <https://www.echr.coe.int/Documents/Pub_coe_domestics_remedies_ENG.pdf> last accessed 7 January 2019.

Communications Decency Act, 47 U.S.C. §230.

Department for Digital, Culture, Media and Sport, “Centre for data ethics and innovation consultation”(June 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715760/CDEI_consultation_1_.pdf> last accessed 9 January 2019.

Digital Millennium Copyright Act, H.R. 2281, 105th Cong. (1998).

Data Protection Act 1998.

Danish Government, “Strategy for Denmark’s Digital Growth” (2018) is available at <https://eng.em.dk/media/10555/digital-growth-strategy-report_uk_web-1.pdf> last accessed 9 January 2019.

E-Commerce Regulations 2002.

EDPS, "Report on Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit" (2017) 12.

Estonian Government "Prime minister: to implement artificial intelligence, countries need a unified approach and ability to adapt" (16 October 2018) <<https://www.valitsus.ee/en/news/prime-minister-implement-artificial-intelligence-countries-need-unified-approach-and-ability>> last accessed 9 January 2019.

Economic and Monetary Affairs Committee, "Report on an academic view on the Role and Powers of National Competition Authorities" (2016) 23.

EU Agency for Fundamental rights, "Report on freedom to conduct a business: exploring the dimensions of a fundamental right" (2015).

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02.

EU Council text, Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market - Agreed negotiating mandate, Interinstitutional File: 2016/0280 (COD).

EU Commission, "Public Consultation on the evaluation and modernization of the legal framework for the enforcement of intellectual property rights: Summary of responses" (2016).

EU Commission, "Public Consultation on the role of online intermediaries: Summary of responses" (2016).

EU Commission, "Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce: Summary of response" (2010).

EU Commission, "Towards a renewed consensus on the enforcement of Intellectual Property Rights: An EU Action Plan Strasbourg" COM (2014) 392 final.

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

EU Commission, "A New Deal for Consumers" COM (2018) 183 final.

EU Commission, "Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit good via the internet" COM (2017) 430 final.

EU Commission, "A Digital Single Market Strategy for Europe" COM (2015) 192 final.

EU Commission, "Recommendation on measures to effectively tackle illegal content online" COM (2018) 1177 final.

EU Commission, "Digital Single Market Creating a Digital Single Market European Commission actions since 2015" (2018).

EU Commission, "Study on the role of intermediaries - Summary of the public consultation" (2016).

EU Commission, "A balanced IP enforcement system responding to today's societal challenges" (2017) 430 final.

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

EU Commission, "Behavioural Study on the transparency of online platforms- Executive summary" (2018).

EU Commission, "Tackling illegal content online: Towards an enhanced responsibility of online platforms" COM (2017) 555 final.

EU Commission, "Towards a modern, more European copyright framework" COM (2015) 626 final.

EU Commission, "Online platforms and the Digital Single Market opportunities and challenges for Europe" COM (2016) 0288 final.

EU Commission, "Memorandum of Understanding on the online sale of counterfeit goods" (2016) is available at <
[file:///C:/Users/krokida/Downloads/MoU_21.06.2016%20\(1\).pdf](file:///C:/Users/krokida/Downloads/MoU_21.06.2016%20(1).pdf)> last accessed 27
October 2019.

EU Commission, “Report on the functioning of the European Online Dispute Resolution platform established under Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes” COM (2017) 744 final.

EU Commission Staff Working Paper, “Piracy Watch List” SWD (2018) 492 final.

EU Commission Staff Working Paper, “Online Services, Including E-Commerce, in the Single Market” SEC (2011) 1641 final.

EU Commission Staff Working Document, “A Digital Single Market Strategy for Europe- Analysis and Evidence” COM (2015) 192 final.

EU Commission Staff Working Paper, “Impact assessment on Proposal for a Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services, Online Services, Including E-Commerce, in the Single Market” COM (2018) 238 final.

EU Commission Staff Working Paper, “Overview of the functioning of the Memorandum of Understanding on the sale of counterfeit goods via the internet” SWD(2017) 430 final
6

EU Commission’s Directorate-General for Communications Networks, Content and Technology, “Algo: aware; Raising awareness on algorithms” (2018).

EU Commission, “Overview of the legal framework of notice and action procedures in Member States SMART 2016/0039” (2018).

EU Commission, “Notice on cooperation within the Network of Competition Authorities” (2004/C 101/03).

EU Parliament, “Legislative resolution of 17 April 2019 on the proposal for a regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online” (COM(2018)0640 – C8-0405/2018 – 2018/0331(COD)).

EU Parliament, “Copyright in the Digital Single Market, Amendments adopted by the European Parliament on 12 September 2018 on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market” (COM (2016) 0593- C8-0383/2016- 2016/0280 (COD)).

European Intellectual Property Office, “Online copyright infringement in the European Union: music, films and TV (2017-2018), trends and drivers (November 2019).

European Patent Office and OECD, “Report on trends in trade in counterfeit and pirated goods” (2019).

European Patent Office and the European Union Intellectual Property Office, “ A joint project on IPR-intensive industries and economic performance in the European Union” (2019).

European Securities and Markets Authority, “Final report on Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions: The AML/CFT Colleges Guidelines ESMA” (2019) 5.

General Secretariat of the Council on “Draft Directive of the European Parliament and of the Council on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, Joint statements (15 April 2019).

Government of the Netherlands, “Dutch Digitization Strategy” (2018) <<https://www.government.nl/documents/reports/2018/06/01/dutch-digitalisation-strategy>> last accessed 11 January 2019.

Greek Intellectual Property Law 4481/2017

HM Government, “UK Government Response to EU public consultation on Digital Platforms: Including the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy” (2016).

Human Rights Council of the United Nations, “Resolution on the Promotion, Protection and Enjoyment of Human Rights on the Internet” (2012) is available at <<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/082/83/PDF/G1408283.pdf?OpenElement> > last accessed 31 October 2019.

Information Commissioner’s Office, “The principles” are available at<<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general->

[data-protection-regulation-gdpr/principles/storage-limitation/](#)> last accessed 22 April 2019.

Intellectual Property Office, “IP Crime and Enforcement Report 2018-2019” (2019) 54

Loi no 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique, Art. 6-I-5.

Mandate of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (24 July 2018).

Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (13 June 2018).

Ministry of National Development, “NTD/N&A procedures regulated in law (Hungary)” is available

at <<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32318&no=6>> last accessed 1 March 2019.

OECD, “The economic and social role of internet intermediaries” (2010).

OECD, “The Economic Impact of Counterfeiting and Piracy” (2008).

OECD, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” (2013).

Propriete Industrielle et economie numerique, “Part 1: A law for a digital French Republic – online platforms” is available at < <http://www.dreyfus.fr/en/new-technologies/part-1-a-law-for-a-digital-french-republic-online-platforms/>> last accessed 9 January 2019.

Regolamento in materia di tutela del diritto d’autore sulle reti di comunicazione elettronica e procedure elettronica e procedure attuative ai sensi del decreto legislativo 9 April 3 2003, N. 7 is available at < http://www.librari.beniculturali.it/export/sites/dgbid/it/documenti/Eventi/2014/35.REGOLAMENTO_AGCOM.pdf> last accessed 10 May 2019.

Report of the Special Rapporteur, “On the promotion and expression of the right to freedom of expression” (The United Nations General Assembly, 16 May 2011) is available at <

https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

> last accessed 9 April 2019.

Spanish legislative approach to notice and action procedures is available at <<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32315&no=3>> last accessed 1 March 2019.

United Nations Office on Drugs and Crime, “The Globalization of Crime: A Transnational Organized Crime Threat Assessment” (2010) is available at <https://www.unodc.org/res/cld/bibliography/the-globalization-of-crime-a-transnational-organized-crime-threat-assessment_html/TOCTA_Report_2010_low_res.pdf> last accessed on 27 March 2019.

White Paper, “Chinese courts and internet judiciary” (2019) 66 is available at <http://wlf.court.gov.cn/upload/file/2019/12/03/11/40/20191203114024_87277.pdf> last accessed 18 December 2019.

World Economic Forum, “Report on the Global Governance of Online Consumer Protection and E-commerce Building Trust” (2019).

World Economic Forum, “White Paper on The Global Governance of Online Consumer Protection and E-commerce Building Trust” (2019) is available at <http://www3.weforum.org/docs/WEF_consumer_protection.pdf> last accessed 20 April 2019.

B. European Court of Human Rights Case Law

Ahmet Yildirim v Turkey (18 December 2012) Application no. 3111/10.

Delfi AS v Estonia (16 June 2015) Application no. 64569.

Neij and Sunde Kolmisoppi v. Sweden (19 February 2013) Application no. 40397.

Anheuser-Busch Inc v. Portugal (11 January 2007) Application no. 73049/01.

C. Court of Justice of the European Union Case Law

Case C-362/14, *Maximilian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.

Case C-324/09, *L’Oreal SA V eBay Int’l AG* [2011] E.C.R. I-6011.

Case C-203/15, *Tele2 Sverige* [2015] ECLI:EU:C:2016:970.

Case C-162/97, *Nilsson* [1998] ECR I- 7477.

Case C-288/12, *Commission v Hungary* [2014] ECLI:EU:C:2014:237.

Case C- 324/09, Opinion of Advocate General Jääskinen, *L’Oréal v eBay International* (2011) ECR I-06011.

Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (2014) ECLI:EU:C:2014:317.

Case C-610/15, *Stichting Brein v Ziggo BV and XS4ALL Internet BV* (2017) ECLI:EU:C:2017:456.

Case C-484/14 - *Mc Fadden* (2016) ECLI:EU:C:2016:689.

Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* [2011] ECR-I 11959.

Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV* (2012) ECLI:EU:C:2012:85.

Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU* (2008) ECR I-00271.

Case C- 236/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (2010) ECR I-02417.

Case C- 237/08, *Google France SARL v Viaticum SA and Luteciel SARL* (2010) ECR I-02417.

Case C- 238/08, *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (2010) ECLI:EU:C:2010:159.

Case C-610/15, *Opinion of AG Szpunar on Ziggo/ The Pirate Bay* (2017) ECLI:EU:C:2017:99.

Case C-70/10, Opinion of AG Cruz Villalon on *Scarlet Extended SA v Société Belge des auteurs compositeurs et éditeurs (SABAM)* (2011) ECLI:EU:C:2011:255.

Case C-324/09, *L’Oreal SA V eBay Int’l AG* (2011) ECR. I-6011.

Case C-324/09, Opinion of Advocate General Jääskinen on *L’Oréal v eBay International* (2010) ECLI:EU:C:2010:757.

Case C-466/12, *Nils Svensson and Others v Retriever Sverige AB* (2014) EU:C:2014:76.

Case C-279/13, *BestWater; C More Entertainment AB v Linus Sandberg* (2015) EU:C:2015:199.

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

Case C-275/06, *Promusicae* (2008) ECR I-00271.

Case C 494/15, *Tommy Hilfiger Licensing* (2016) ECLI:EU:C:2016:528.

D. UK Case Law

Cartier v BskyB (2014) EWHC 3354 (Ch) 264.

Amstrad CBS Songs v. Amstrad [1988] UKHL 15 (12 May 1988).

FAPL v BT (2017) EWHC 480.

OBG Ltd v Allan [2007] UKHL 21.

Football Dataco Ltd & Ors v Stan James Plc & Ors [2013] EWCA Civ 27.

L’Oreal S.A v eBay International AG [2009] EWHC 1094 (Ch).

Design Technica Corporation v. Google [2009] EWHC 1765 (QB).

Twentieth Century Fox v. Newzbin Ltd [2010] EWHC 608 (Ch).

Falcon v Famous Players [1926] 2 KB 474.

CBS Inc v. Ames Records and Tapes [1981] 2 All ER 812.

Cartier International AG v British Sky Broadcasting Ltd [2016] ETMR 43.

CBS Songs v. Amstrad [1988] UKHL 15.

Dramatico Entertainment Ltd & Ors v British Sky Broadcasting Ltd & Ors [2012] EWHC 268 (Ch).

Golden Eye (International) Ltd and others v. Telefonica UK Ltd [2012] EWHC 723 (Ch).

E. Irish Case Law

High Court, EMI v Eircom [2009] IEHC 411.

F. US Case Law

Stratton Oakmont, Inc and Daniel Porush v Prodigy Services Company (Supreme Court, Nassau County, New York, Trial IAS Part 34. May 24, 1995)

Viacom International, Inc. v YouTube Inc, 676 F.3d 19 (Court of Appeals, Second Circuit 2012)

Gershwin Publishing Corp v Columbia Artists Mgmt, Inc, 443 F. 2d 1159, 1162 (2D Cir. 1971)

Fonovisa, Inc. v. Cherry Auction, Inc, 76 F. 3d 259 (9th Cir. 1996)

A&M Records, Inc. v. Napster Inc, 239 F 3d 1004 (9th Cir. 2001)

Lewis v. YouTube LLC, 197 Cal. Rptr. 3d 219 (2015)

Song fi, Inc. v. Google, Inc., 108 F. Supp. 3d 876 (N.D. Cal.2015)

Bartholomew v YouTube, LLC. 17 Cal. App 5th 1217, 1226-1227 (2017)

Packingham v. North Carolina 582 U.S. (19 June 2017)

Sony Corp of Am. v Universal City Studios Inc, 464 U.S. 417, 220 U.S.P.Q. (BNA) 665 (1984).

G. Belgian Case Law

eBay v. Lancôme [2008] (Brussels Commercial Court).

H. Spanish Case Law

Audiencia Provincial Sentencia A.P.S. Madrid Jan [2014] (Provincial Court Sentence).

Ajoderse.com [2003] (Spanish Supreme Court).

I. Italian Case Law

Delta TV v Google and YouTube [2017] (Turin Court of First Instance).

J. French Case Law

Lacoste/Multimania, Eterel and Cybermedia [1999] (Tribunal de Grande Instance de Nanterre).

Hermes v. eBay [2008] (Tribunal de Grande Instance de Troyes).

eBay Inc v. LVMH [2012] (Cour de Cassation of France).

Madame L. c/ les sociétés Multimania [1999] (Tribunal de Grande Instance de Nanterre).

Google Inc. c. Les Films de la Croisade, Goatworks Films [2011] (Cour d'appel de Paris).

Google v Viaticum et Luteciel [2005] (Cour d'appel de Versailles).

Cons P v Monsieur G. [2005] (Tribunal de Grande Instance de Paris).

SARL Zadig Productions, Jean-Robert Viallet et Mathieu Verboud c. Sté Google Inc. et AFA [2007] (Tribunal de Grande Instance de Paris).

Christian C., Nord Ouest Production c. Dailymotion, UGC Images [2007] (Tribunal de Grande Instance de Paris).

TF1 v YouTube [2012] (Court of First Instance Paris)

TF1 v Dailymotion [2014] (Court of Appeal Paris)

Sedo GmbH v Hotel Meridien, Stephane H [2008] (Cour de Cassation).

SARL Publison System v SARL Google France [2009] (Court of Appeal of Paris).

La société Google France c. la société Bach films (L'affaire Clearstream) [2012] (Cour de Cassation).

K. Swedish Case Law

Sweden v Neij et al. [2009] (Stockholms County Council).

Rebecka Jonsson v Les Éditions de l'Avenir SA [2016] (Attunda District Court).

L. German Case Law

Bundesgerichtshof, *05 Ricardo v. Rolex, SA*, 30 April 2008- I ZR 73/2007.

Bundesgerichtshof, *Vorschaubilder III*, 21. September 2017 - I ZR 11/16.

Bundesgerichtshof, *Internetversteigerung I*, 11 March 2004, I ZR 304/01.

Bundesgerichtshof, *Internetversteigerung II*, 19 April 2007, I ZR 35/04.

Bundesgerichtshof, *Internetversteigerung III*, 30 April 2008, I ZR 73/05.

Bundesgerichtshof, *Constanze II*, 6 July 1954, I ZR 38/532.

Bundesgerichtshof, *Jugendgefährdende Medien bei eBay*, 12 July 2007, I ZR 18/04.

Bundesgerichtshof, *Rapidshare III*, 15 August 2013, I ZR 80.

Oberlandesgericht Düsseldorf, *Rapidshare I*, 27 April 2010, I-20 U 166/09.

Oberlandesgericht Düsseldorf, *Rapidshare II*, 21 December 2010, I-20 U 59/10.

Oberlandesgericht Hamburg, 13 May 2013, 5 W 41/13.

Landesgericht Hamburg, 20 April 2012, 310 O 461/10.

M. Greek Case Law

Decision no 5249/2014, Court of First Instance of Athens.

Decision no 1909/2017, Court of Appeal of Athens.

Decision of OPI (Οργανισμός Πνευματικών Δικαιωμάτων)

is available at <https://www.opi.gr/images/epitropi/apofaseis/edppi_1_2018.pdf> last accessed 26 December 2019.

Decision of OPI (Οργανισμός Πνευματικών Δικαιωμάτων)

Decision of OPI (Οργανισμός Πνευματικών Δικαιωμάτων) is available at <https://www.opi.gr/images/epitropi/apofaseis/edppi_2_2018.pdf> last accessed 26 December 2019.

Decision of OPI (Οργανισμός Πνευματικών Δικαιωμάτων) is available at <https://www.opi.gr/images/epitropi/apofaseis/edppi_3_2018.pdf> last accessed 26 December 2019.

Decision of OPI (Οργανισμός Πνευματικών Δικαιωμάτων) is available at <https://opi.gr/images/epitropi/apofaseis/edppi_4_2019.pdf> last accessed 26 December 2019.

Decision of OPI (Οργανισμός Πνευματικών Δικαιωμάτων) is available at <https://opi.gr/images/epitropi/apofaseis/edppi_5_2019.pdf> last accessed 26 December 2019.

II. Secondary sources

A. Books and book chapters

Angelopoulos C, *European intermediary liability in copyright: a tort-based analysis* (Kluwer Law International 2016).

Balkin RP and Davis JLR, *Law of Torts* (2nd ed, Butterworths 2002).

Barral-Vinals I, “Enforcing e-consumer protection beyond alternative dispute resolution (ADR): ODR” in James Devenney and Mel Kenny (eds.), *European consumer protection : theory and practice* (Oxford University Press 2012).

Benabou V, “The Chase: The French Insight into the “Three strikes” System” in Irini Stamatoudi (ed.), *Copyright Enforcement and the Internet* (Kluwer Law International 2010).

Belli L and Zingales N, “Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police” in Luca Belli and Nicolo Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018).

Berendschot H, "Summary and analysis of Case C-494/15" in Huib Berendschot and Karel Janssens (eds.), *Landmark IP decisions of the European Court of Justice 2014-2018* (ELS Belgium 2019) 139-144.

Birks P, "Civil Wrongs: A New World" in F M B Reynolds and Peter Birks (eds.), *Butterworths Lectures 1990–1991* (1991).

Bowen H R, *Social Responsibilities of the Businessman* (University of Iowa Press 2013).

Broeders D and Taylor L, "Does Great Power Come with Great Responsibility? The Need to Talk about Corporate Political Responsibility" in Mariarosaria Taddeo and Luciano Floridi (eds.), *The responsibilities of online service providers* (Springer 2017).

Brownsword R, *Rights, Regulation and the technological revolution* (2008).

Buijze A, *The Principle of transparency in EU Law* (Unpublished PhD Thesis 2013).

Calhoun C J, *Dictionary of the social sciences* (New York: Oxford University Press 2000).

Caroll B, "A History of Corporate Social Responsibility: Concepts and Practices" in Andrew Crane, Dirk Matten, Abigail McWilliams, Jeremy Moon and Donald S. Siegel (eds.), *The Oxford Handbook of Corporate Social Responsibility* (Oxford University Press 2009).

Dinwoodie G B, "A comparative analysis of the secondary liability of online service providers" in Graeme B. Dinwoodie (ed.), *Secondary Liability of Internet Service Providers* (Springer 2016).

De Filippi P and Bourcier D, "Three-Strikes' Response to Copyright Infringement: The Case of Hadopi" in Francesca Musiani, Derrick L. Cogburn, Laure DeNardis and Nanette Levinson (eds.), *The Turn to Infrastructure in Internet Governance* (Palgrave-Macmillan 2016).

Downie R S, "Collective responsibility" in Stacey Hoffman (ed.), *Collective responsibility: Five decades of debate in theoretical and applied ethics* (1992).

Edwards L, "With Great Power Comes Great Responsibility? The Rise of Platform Liability" in Lilian Edwards (ed.), *Law, Policy and the Internet* (Hart Publishing 2019).

Fischman Afori O, "Universal measures in the service of global challenges: proportionality, blocking orders, and online intermediaries as hybrid bodies" in Tatiani Synodinou,

Pluralism or Universalism in international copyright law (Kluwer Law International 2019) 657.

Frabboni M, "File-sharing and the role of intermediaries in the marketplace" in Irini Stamatoudi (ed.), *Copyright enforcement and the Internet* (Kluwer Law International 2010).

Frosio G and Husovec M, "Accountability and Responsibility of Online Intermediaries" in Giancarlo Frosio (ed.), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press, forthcoming 2020).

Frosio G, "Algorithmic enforcement online" in Paul Torremans (ed.), *Intellectual Property and Human Rights* (4th edition, Kluwer Law International forthcoming 2020).

Garstka K, "Guiding the Blind Bloodhounds: How to Mitigate the Risks art. 17 of Directive 2019/790 Poses to the Freedom of Expression" in Paul Torremans (ed.), *Intellectual Property and Human Rights* (Kluwer Law and Business forthcoming 2020).

Geiger C, "Fundamental Rights as Common Principles of European (and International) Intellectual Property Law" in Matthias Leistner (ed.), *Common principles of European Intellectual Property Law* (Mohr Siebeck 2012).

Giampiero G, *National Governments and Control of the Internet: A Digital Challenge* (2005).

Gibblin R, *Code Wars: 10 Years of P2P software litigation* (Edward Elgar 2011).

Goldstein G and Hugenholtz B, *International Copyright: Principles, Law and Practice* (Oxford University Press 2010).

Guadamuz A, "Internet Regulation" in Lilian Edwards (ed.), *Law, policy and the internet* (Hart Publishing Oxford 2019).

Guadamuz A, "Developments in Intermediary Liability" in Andrej Savin and Jan Trzaskowski (eds.) *Research Handbook on EU Internet Law* (Edward Elgar 2014).

Guadamuz A, *Networks, Complexity and Internet Regulation: Scale Free Law* (Edward Elgar 2011)

Hart L A and Honore' T, *Causation in the Law* (2nd ed, Oxford 1985).

Holland H B, "Section 230 of the CDA: Internet Exceptionalism as a Statutory Construct" in Berin Szoka and Adam Marcus (eds), *The next digital decade: Essays on the future of the Internet* (TechFreedom 2011).

Hughenoltz P B, "Codes of Conduct and Copyright enforcement in cyberspace" in Irini Stamatoudi (ed.), *Copyright enforcement and the Internet* (Kluwer Law International 2010).

Husovec M, *Injunctions Against Intermediaries in the European Union: Accountable but not liable* (Cambridge University Press 2017).

Husovec M, "How Europe Wants to Redefine Global Online Copyright Enforcement" in Tatiani Synodinou (ed.), *Pluralism or Universalism in International Copyright Law* (Kluwer Law International 2019).

Jougleux P, "The role of internet intermediaries in copyright law online enforcement" in Tatiani Synodinou, Philippe Jougleux, Christianna Markou and Thalia Prastitiou (eds.), *EU Internet Law: Regulation and Enforcement* (Springer 2017) 273.

Karapapa S and McDonagh L, *Intellectual Property Law* (Oxford University Press 2019).

Katsh E and Rabinovich-Einy O, *In Digital Justice: Technology and the Internet of Disputes* (Oxford University Press 2017).

Kulk S, *Internet Intermediaries and Copyright Law: EU and US perspective* (Kluwer Law International 2019).

Kuczerawy A, *Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards* (Intersentia 2018).

Kuczerway A, "General Monitoring obligations: a new cornerstone of Internet Regulation in the EU?" in KU Leuven Centre for IT and IP Law (ed.), *Rethinking IT and IP Law* (Intersentia 2019).

Laddie H, Prescott P, Vitoria M and Speck A, *The Modern Law of Copyright and Designs* (3rd ed, Butterworths 2000).

Laidlaw E, "Notice-and-Notice-Plus: A Canadian Perspective beyond the Liability and Immunity Divide" in Giancarlo Frosio (ed.), *The Oxford Handbook of Intermediary Liability Online* (Oxford University Press 2020, Forthcoming).

Laidlaw E, "Internet Gatekeepers, Human Rights and Corporate Social Responsibilities" (PhD Thesis 2012).

Leistner M, "Common Principles of Secondary Liability?" in Ansgar Ohly (ed.), *Common Principles of European Intellectual Property Law* (Mohr Siebeck 2012).

Leistner M, "Intermediary liability in a global world" in Tatiani Synodinou (ed.), *Pluralism and Universalism in international copyright law* (Kluwer Law International 2019).

Lenearts K and Van Nuffel P, *European Union Law* (2011).

Lessig L, *Code and other Laws of cyberspace* (1999).

Lessig L, *Code: version 2.0* (2006).

Lichtman D, "Copyright as Information Policy: Google Book Search from a Law and Economics Perspective" in Josh Lerner and Scott Stern (eds.), *Innovation Policy and The Economy* (2008).

List C and Pettit P, *Group agency: The possibility, design, and status of corporate agents* (Oxford University Press 2011).

Litman J, *Digital Copyright: Revising Copyright Law for the Information Age* (New York, Prometheus Books 2001)

Lodder A, "Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market" in Arno Lodder and Andrew Murray (eds), *EU Regulation of E-Commerce: A commentary* (2017).

Luetge C, "Responsibilities of OSPs from a Business Ethics Point of View" in Mariarosaria Taddeo and Luciano Floridi, *Responsibilities of internet service providers* (Springer 2016).

Lynskey O, "Regulation by Platforms: The Impact on Fundamental Rights" in Luca Belli and Nicolo Zingales (eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (2018).

Mardsen C, *Internet co-regulation* (Cambridge University Press 2011).

Marsoof A, *Internet intermediaries and trade mark rights* (Routledge 2019).

Matthews P and Malek H M, *Disclosure* (5th ed, Sweet and Maxwell 2012).

McIvor C, *Third Party Liability in Tort* (Hart Publishing 2006).

McKinnon R, *Consent of the Networked: The Worldwide struggle for Internet Freedom* (2012).

Murray A, *Information Technology Law: The law and society* (Oxford University Press 2009).

Nissenbaum H, "Accountability in a Computerized Society," in Batya Friedman (ed.), *Human Values and the Design of Computer Technology* (Cambridge University Press 1997).

Pasquale F, *The Black Box Society – The Secret Algorithms that Control Money and Information* (2015).

Revolidis I, "Internet intermediaries and copyright enforcement in the EU: In search of a balanced approach" in Marcelo Corrales, Mark Fenwick and Nikolaus Forgó (eds.), *New Technology, Big Data and the Law* (2017).

Riefa C, *Consumer Protection and Online Auction Platforms: Towards a Safer Legal Framework (Markets and the Law)* (Ashgate 2015).

Riordan J, "Website Blocking Injunctions under United Kingdom and European Law" in Graeme Dinwoodie (ed.), *Secondary liability of internet service providers* (Springer 2017).

Riordan J, *The liability of internet intermediaries* (Oxford University Press 2016).

Rosen F, "Reading Hume Backwards: Utility as the Foundation of Morals," in Frederick Rosen (ed.), *Classical Utilitarianism from Hume to Mill* (Routledge 2003).

Rowland D, Kohl U and Charlesworth A, *Information Technology Law* (4th ed, Routledge 2011).

Ruben E, "The internet, consumer protection and practical knowledge" in Jane Winn, *Consumer Protection in the Age of the 'Information Economy'* (2006) 37.

Sadeghi M, "The Knowledge Standard for ISP Copyright and Trademark Secondary Liability: A Comparative Study on the Analysis of US and EU Laws" (Unpublished PhD Thesis 2013).

Schack H, "Täter und Störer: Zur Erweiterung und Begrenzung der Verantwortlichkeit durch Verkehrspflichten im Wettbewerbs- und Immaterialgüterrecht" in *Festschrift für Dieter Reuter zum 70. Geburtstag am 16. Oktober 2010* (De Gruyter 2010).

Shapiro L, *The control revolution: How the internet is putting individuals in charge and changing the world we know* (New York: Public Affairs 2000).

Schruers M, "Copyright, Intermediaries and Architecture" in Francesca Musiani, Derrick L. Cogburn, Laure DeNardis, Nanette Levinson (eds.), *The Turn to Infrastructure in Internet Governance* (Palgrave-Macmillan 2016).

Schwarze J, *European Administrative law* (2006).

Sorensen M J, "Draft Model Rules on Online Intermediary Platforms" in Bram Devolder (ed.), *The Platform Economy: Unravelling the Legal Status of Online Intermediaries* (Intersentia 2019) 182.

Stalla-Bourdillon S, "Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well" in Mariarosaria Taddeo and Luciano Floridi (eds.) *The Responsibilities of Online Service Providers* (Springer 2017).

Storskrubb E, "Access to Justice in European Comparative Law" in Francesco Francioni (ed.), *Access to Justice as a Human Right* (2007).

Strowel A, "The Graduated response in France: Is it the good reply to online copyright infringements?" in Irini Stamatoudi (ed.), *Copyright Enforcement and the Internet* (Kluwer Law International 2010).

Taddeo M and Floridi L, "The Moral Responsibilities of Online Service Providers" in Mariarosaria Taddeo and Luciano Floridi (eds.), *The Responsibilities of Online Service Providers* (Springer 2017).

Tessier M, Herzog J and Madzou L, "Regulation at the Age of Online Platform-Based Economy: Accountability, User Empowerment and Responsiveness" in Luca Belli and Nicolo Zingales (eds.), *Platform regulations- How to regulate them and how they regulate us* (2018).

Trimble M, "Geoblocking and Evasion of Geoblocking – Technical Standards and the Law" in Ramon Lobato and James Meese, *Geoblocking and Global Video Culture* (2016).

Tusikov N, *Chokepoints: Global private regulation on the Internet* (2017).

Van Dam C, *European Tort Law* (Oxford University Press 2007).

Wang J, *Regulating Hosting ISPs' responsibilities for copyright infringement: The freedom to operate in the US, EU and China* (Springer 2018).

Watkins D and Burton M, *Research Methods in Law* (Routledge 2017).

Weber R, "The legitimacy and accountability of the Internet's governing institutions" in Ian Brown (ed.), *Research Handbook on Governance of the Internet* (2013).

Williams G, *Joints Torts and Contributory Negligence* (Stevens & Sons Ltd 1951).

Yoo C, *The dynamic Internet: How technology, users and businesses are transforming the network* (2014).

B. Articles in journals and conferences and reports

Addink G H and ten Berge B J M, "Study on Innovation of Legal Means for Eliminating Corruption in the Public Service in the Netherlands" (2007) Netherlands Comparative Law Association 12.

Angelopoulos C, "On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market" (2017) 1.

Angelopoulos C and Smet S, "Notice and Fair Balance: How to reach a compromise between fundamental rights in European Intermediary Liability" (2016) 8 Journal Media of Law 266.

Angelopoulos C, "Filtering the Internet for copyrighted content in Europe" (2009) IRIS 3.

Angelopoulos C, "Beyond the safe harbors: harmonizing substantive intermediary liability for copyright infringement in Europe" (2013) 3 Intellectual Property Quarterly 254.

Angelopoulos C and Quintais J P, "Fixing copyright reform: a better solution to online infringement" (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 153.

Ahlert C, Marsden C and Yung C, "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation" (2014) is available at <<http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf>> last accessed 1 March 2019.

Alves S, Capiou J and Sinclair A, "Principles for the Independence of Competition Authorities" (2015) 11 Competition Law Journal 15-16.

Amadei X, "Standards of liability for Internet for Internet Service Providers: A comparative study of France and the United States with a specific focus on copyright, defamation and illicit content" (2002) 35 Cornell International Law Journal 204.

Arnold M, Darmon E, Dejean S and Penard T, "Graduated Response Policy and the Behavior of Digital Pirates: Evidence from the French Three-Strike (Hadopi) Law" (2014) Working Papers 14-07 3.

Balkin J, "Old-School/New-School Speech Regulation" (2014) 127 Harvard Law Review 2309.

Balkin J, "The Future of Free Expression in a Digital Age" (2009) 36 Pepperdine Law Review 437.

Baratta R, "Complexity of EU Law in the domestic implementing process" (2014) 2 The Theory and Practice of Legislation 296.

Barazza S, "Secondary liability for IP infringement: converging patterns and approaches in comparative case law" (2012) 7 Journal of Intellectual Property Law and Practice 882.

Barcelo R J and Koelman K, "Intermediary liability in the E-Commerce Directive: so far so good, but it's not enough" (2000) 16 Computer Law and Security Report 235.

Bartholomew M and Tehranina J, "The secret life of legal doctrine: the divergent evolution of secondary liability in trademark and copyright law" (2006) 21 Berkeley Technology Law Journal 1419.

Barzilai- Nahon K, "Toward a theory of network gatekeeping: a framework for exploring information control" (2008) 59 Journal of the American Society for Information Science and Technology 1493.

Belli L and Sappa C, "The Intermediary Conundrum: Cyber-regulator, cyber-police or both?" (2017) 8 Intellectual Property Information and Technology and Electronic Commerce 185.

Benhamou Y, "Compensation of Damages for Infringements of Intellectual Property Rights in France, Under Directive 2004/48/EC and its Transposition Law – New Notions?" (2009) 40 International Review of Intellectual Property and Competition Law 126.

Ben-Shahar O and Schneider C E, "The Failure of Mandated Disclosure" (2011) 159 University of Pennsylvania Law Review 647.

Blevins J, "Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms" (2013) 34 Cardozo Law Review 1829.

Bonadio E, "File-Sharing, Copyright and Freedom of Speech" (2010) 33 European Intellectual Property Review 620.

Boroughf B, "The Next Great YouTube: Improving Content ID to foster creativity, cooperation and fair compensation" (2014) 25 Albany Law Journal of Science and Technology 8.

Bohte S M, Langdon W B and La Poutre H, "On Current Technology for Information Filtering and User Profiling in Agent-Based Systems, Part I: A Perspective" (2000) 9.

Bridy A, "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement" (2010) 89 Oregon Law Review 101.

Bridy A and Keller D, "U.S. Copyright Office Section 512 Study: Comments in Response to Notice of Inquiry" (2016) 14-15.

Brill J, "Transparency, Trust, and Consumer Protection in a Complex World" Keynote Address Before Coalition for Networked Information Fall 2015 Membership Meeting (15 December 2015).

Bunting M, "Keeping Consumers Safe Online Legislating for platform accountability for online content" (2018) *Communications Chambers* 20-27, 33.

British and Irish Legal Education and Technology Association, "Written evidence for the House of Lords, The Internet: To Regulate or Not to Regulate? Summary of Response" (2018) 1.

Bucher T, "The algorithmic imaginary: exploring the ordinary effects of Facebook algorithms" (2017) 20 *Information, Communication and Strategy* 40.

Caplan R, Donovan J, Hanson L and Matthews J, "Algorithmic Accountability: A primer" (2018) 7.

Carrier M A, "Copyright and Innovation: The Untold Story" (2012) 891 *Wisconsin Law Review* 923-49

Carsten U, "Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective" (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 116

Carty H, "Joint tortfeasance and assistance liability" (1999) 19 *Legal studies* 10.

Center for Democracy and Technology, "Chile's notice and takedown system for copyright protection: an alternative approach" (August 2012).

Cerf V G, "First, do no harm" (2011) 24 *Philosophy & Technology* 463.

Chadelaine P, "Copyright User Rights and Remedies: An access justice perspective" (2018) *Laws* 7-10.

Cheung C, Chiu P and Lee M, "Online social networks: Why do students use facebook?" (2011) 27 *Computers in Human Behaviour* 1337.

Chen S, "Corporate Responsibilities in Internet-Enabled Social Networks" (2009) 90 *Journal of Business Ethics* 523.

Citron D, "Technological Due Process" (2008) 85 Washington University Law Review 1253-1254.

Citron Keats D and Wittes B, "The Internet Will Not Break: Denying Bad Samaritans Section 230 Immunity" (2017) University of Maryland Legal Studies Research Paper No. 2017-22 17.

Citron Keats D and Pasquale F, "The Scored Society: Due Process for Automated Predictions" (2014) 89 Washington Law Review 19.

Coase R, 'The Problem of Social Cost' (1960) 3 Journal of Law and Economics 1, 19.

Cohen J, "The Regulatory State in the Information Age" (2016) 17 Theoretical Inquiries in Law 6.

Daly M, "Life after Grokster: analysis of US and European approaches to file-sharing" (2007) 29 European Intellectual Property Review 2.

Davies P, "Accessory liability for assisting torts" (2011) 70 The Cambridge Law Journal 353.

Davies P, "Accessory liability: protecting intellectual property rights" (2011) 4 Intellectual Property Quarterly 390.

De Gregorio G, "Expressions on Platforms: Freedom of Expression and ISP liability in the European Digital Single Market" (2018) 2 CoRe 214.

Devenney J, "The legacy of the Cameron-Clegg coalition programme of reform of the law on the supply of goods, digital content and services to consumers"(2018) 6 Journal of Business Law 488

EU Commission, "EU study on the New rules for a new age? Legal analysis of a Single Market for the Information Society 6. Liability of online intermediaries" (2009) 24.

Edwards L and Waelde C, "Online Intermediaries and Liability for Copyright Infringement" (2005) WIPO 2.

Edwards L, "Privacy, security and data protection in smart cities: a critical EU law perspective" (2016) 2 European Data Protection Law Review 48.

Edwards L, "Should ISPs be compelled to become Copyright Cops?" (2009) 19 Magazine of the Society for Computers and Law 29.

Diakopoulos N, "Algorithmic accountability reporting: on the investigation of black boxes" (2013) Town Center for Digital Journalism 14.

Dittrich P J, "Online platforms and how to regulate them: an overview" (2018) Jacques Delors Institute Policy Paper No. 227 5.

Eberle E, "The Methodology of Comparative Law" (2011) 16 Roger Williams University Law Review 52.

Economides N, "The Economics of networks" (1996) 14 International Journal of Industrial Organization 673.

Economides N, "The Economics of Trademarks" (1988) 78 Trademark Reporter 523.

Edwards L and Veale M, "Slave to the algorithm? Why a right to an explanation is probably not the remedy you are looking for" (2016) 16 Duke Law and Technology Review 18.

Elkin-Koren N, Nahmias, Y and Perel M, "Is It Time to Abolish Safe Harbor? When Rhetoric Clouds Policy Goals" (2020) 31 Stanford Law & Policy Review, Forthcoming 1.

Erikson K and Kretschmer M, "Empirical approaches to intermediary liability" (2019) 6 Create Working Paper 2, 4, 7.

Farano M, "Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and US Approaches" (2012) TTLF Working Paper 47.

Ferrel O C and Ferrel L, "The Responsibility and Accountability of CEOs: The Last Interview with Ken Lay" (2010) Journal of Business Ethics 11.

Fiala L and Husovec M, "Using experimental evidence to design optimal notice and takedown process" (2018) TILEC Discussion Paper 7.

Fisher W, "CopyrightX: Lecture 11.1, Supplements to Copyright: Secondary Liability" (18 February, 2014) is available at <
https://cyber.harvard.edu/people/tfisher/cx/CopyrightX_Lecture11_Illustrations.pdf >
last accessed 31 October 2019.

French High Council for Literary and Artistic Property, "Mission to Link Directives 2000/31 and 2001/29 – Report and Proposals" (2016) 7 Journal of Intellectual Property, Information Technology and E-Commerce Law 70.

Friedman L W and Friedman H, "The New Media Technologies: Overview and Research Framework" (2008) SSRN electronic Journal 1.

Friedmann D, "Sinking the Safe Harbour with the legal certainty of strict liability in sight" (2014) 9 Journal of Intellectual Property Law and Practice 148-155.

Frosio G, "Why Keep a Dog and Bark Yourself? From Intermediary Liability to Responsibility" (2017) 26 International Journal of Law and Information Technology 7-12.

Frosio G, "Reforming intermediary liability in the platform economy: a European Digital Single Market Strategy" (2017) 112 Northwestern University Law Review 43.

Frosio G and Mendis S, "Monitoring and filtering: European reform or Global trend?" (2019) Center for International Intellectual Property Studies Research Paper 21.

Frosio G, "Reforming the C-DSM Reform: a user-based copyright theory for commonplace creativity" (2019) is available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3482523 last accessed 19 November 2019.

Gardner J, "The Many Faces of the Reasonable Person" (2015) Sweet and Maxwell 563.

Garstka K, "Looking above and beyond the blunt expectation: specified request as the recommended approach to intermediary liability in cyberspace" (2016) 7 European Journal of Law and Technology 1.

Giannopoulou A, "Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality" (2012) 3 European Journal for Law and Technology 1.

Giblin R, "Evaluating Graduated Response" (2014) 37 Columbia Journal of Law and the Arts 147.

Gill L, Redeker D and Gasser U, "Towards Digital Constitutionalism? Mapping attempts to craft an Internet Bill of Rights" (2015) 80 The International Communication Gazette 302.

Ginsburg J C, "Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs" (2008) 50 Arizona Law Review 591.

Global Information Society Watch, "The Internet and corruption: Transparency and accountability online" (2012) 26.

Goldberg J and Zipursky B, "Tort Law and Responsibility" (2013) Fordham Law Legal Studies Research Paper 7.

Goldman E, "Search Engine Bias and the Demise of Search Engine Utopianism" (2006) 8 Yale Journal Law and Technology 189.

Goold P, "Unbundling the tort of copyright infringement" (2016) 102 Virginia Law Review 1842.

Grise K, "After the storm—examining the final version of Article 17 of the new Directive (EU) 2019/790" (2019) 14 Journal of Intellectual Property Law & Practice 887.

Guerra-Pujol, F E and Martínez-García, Orlando I, "Does the Prisoner's Dilemma Refute the Coase Theorem?" (2013) 47 John Marshall Law Review 2.

Hallikainen H and Laukkanen T, "National culture and consumer trust in e-commerce" (2018) 38 International Journal of Information Management 97.

Hamdan A, "Gatekeeper liability" (2005) 77 Southern California Law Review 98.

Hanretty C and Koop C, "Shall the law set them free? The formal and actual independence of regulatory agencies" (2012) 7 Regulation and Governance 3.

Hays T, "The evolution and decentralisation of secondary liability for infringements of copyright-protected works: Part 1" (2006) 12 European Intellectual Property Review 617.

Heaven D, "Not like us: Artificial Minds we can't understand" (2013) New Scientist 32-35.

Helman L and Parchomovsky G, "The best available technology standard" (2011) 111 Columbia Law Review 1230.

Hilty R and Moscon V, "Modernisation of the EU Copyright Rules Position Statement of the Max Planck Institute for Innovation and Competition" (2018) Max Planck for Innovation and Competition Research Paper 99.

Hoeren T and Yankova S, "The Liability of Internet Intermediaries – The German Perspective" (2012) 43 International Review of Intellectual Property and Competition Law 501.

Horten M, "Content responsibility: The looming cloud of uncertainty for internet intermediaries" (2016) Center for Democracy and Technology 12- 13.

Hurwitz J, "Trust and Online Interaction" (2013) 161 University of Pennsylvania Law Review 1593.

Husovec M and Leenes R, "Study on the role of online intermediaries Summary of the public consultation: a study prepared for the European Commission DG Communications Networks, Content & Technology" (2016) is available at <file:///C:/Users/krokida/Downloads/Studyontheroleofonlineintermediaries-Summaryofthepublicconsultation.pdf> last accessed 23 April 2019.

Husovec M, "Accountable, Not Liable: Injunctions Against Intermediaries" (2016) TILEC Discussion Paper 36.

Husovec M, "Injunctions against Innocent Third Parties: The case of Website Blocking"(2016) 4 Journal of Intellectual Property, Information Technology and E-Commerce Law 116.

Husovec M, "The promises of algorithmic copyright enforcement" (2018) 42 Columbia Journal of Law and Arts 59.

Husovec M and Quintais J P, "How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms" (1 October 2019) is available https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011&download=yes last accessed 16 October 2019.

Husztí-Orbán K, "Countering Terrorism and Violent Extremism Online: what role for social media platforms?" in L. Belli and N. Zingales (eds.), *Platform Regulations: How Platforms are regulated and how they regulate us* (2018) 204.

Introna L, "Algorithms, Governance and Governmentality: on governing academic writing" (2016) 41 *Science, Technology and Human Values* 17.

Introna L and Nissenbaum H, "Shaping the web: Why the Politics of search engines matters" (2000) 13 *The Information Society* 169.

Ibrahim D, "Venture impact: the economic importance of venture capital-backed companies to the US Economy" (2012) 65 *Vanderbilt Law Review* 1.

Jacques S, Garstka K, Hviid M and Street J "Automated anti-piracy systems as copyright enforcement mechanism: a need to consider cultural diversity" (2018) 40 *European Intellectual Property Review* 218.

Jondet N, "The silver lining in Dailymotion's copyright cloud" (2008) *Juriscom. Net* 2.

Jones J, "Internet pirates walk the plank with article 10 kept at bay: Neij and Sunde Kolmisoppi v Sweden" (2013) 35 *European Intellectual Property Review* 5.

Kaleda S, "The role of the principle of effective judicial protection in relation to website blocking injunctions" (2017) 8 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 7.

Karapapa S, "The requirement for a "new public" in EU copyright law" (2017) 42 *European Law Review* 63.

Karapapa S and Borghi M, "Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm" (2015) 23 *International Journal of Law and Information Technology* 261-289.

Kaspersen H, "Liability of Providers of the Electronic Highway" (2006) 12 *Computer Law and Security Report* 290.

Katyal N K, "Criminal Law in Cyberspace" (2001) 149 *University of Pennsylvania Law Review* 1097.

Kiat Boon Seng D, "The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices" (2014) 18 *Virginia Journal of Law and Technology Association* 369.

Kleinschmidt B, "An International Comparison of ISP's Liabilities for Unlawful Third-Party Content" (2010) 18 International Journal of Law and Information Technology 332.

Köhler C and Burmeister K, "Copyright liability on the Internet today in Europe (Germany, France, Italy and the E.U.)" (1999) 21 European Intellectual Property Review 485.

Kochanowski J, "The 'reasonable man' standards in continental law" (2007) 1 The Journal of Legislative studies 1.

Kraakman R H, "Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy" (1986) 2 Journal of Law, Economics and Organization 61.

Kroll J and others, "Accountable algorithms" (2017) 165 University of Pennsylvania Law Review 640.

Kulesza J, "Due diligence in international internet law" (2014) Journal of Internet Law 28.

Kulk S and Borgesius F Z, "Filtering for Copyright Enforcement in Europe after the Sabam Cases" (2012) 11 European Intellectual Property Law Review 791.

Kuner C and others, "Machine learning with personal data: is data protection law smart enough to meet the challenge?" (2017) 7 International Data Privacy Law 1.

Laidlaw E, "A framework for identifying Internet information gatekeepers" (2010) 24 International Review of Law, Computers and Technology 264.

Laidlaw E, "Private Power, Public Interest: An Examination of Search Engine Accountability" (2009) 17 International Journal of Law and Information Technology 113.

Laidlaw E, "Are We Asking Too Much from Defamation Law? Reputation Systems, ADR, Industry Regulation and Other Extra-Judicial Possibilities for Protecting Reputation in the Internet Age: Proposal for Reform" (2017) is available at <http://www.lco-cdo.org/wp-content/uploads/2017/07/DIA-Commissioned-Paper-Laidlaw.pdf> > last accessed 31 October 2019.

LaFontaine A, "Adventures in software licensing: SCO v. IBM and the future of the open source model" (2006) 4 Journal on Telecommunications and High Technology Law 449.

Landes W M and Lichtman D, 'Indirect Liability for Copyright Infringement: An Economic Perspective (2003) 16 Harvard Journal of Law and Technology 409.

Landes W and Lichtman D, "Indirect Liability for Copyright Infringement: Napster and Beyond" (2003) 16 The Journal of Economic Perspectives 20.

(St.) Alphonsus Liguori, *Theologia Moralis*. 4 volumes. ed. by L. Gaude (Rome: Ex Typographia 1912) 357 is available at <https://archive.org/details/theologiamoralis01inligu> accessed 21 November 2017.

Lee E, "Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten" (2016) 49 U.C. Davis Law Review 1066

Leistner M, "Structural aspects of secondary provider liability in Europe" (2014) 9 Journal of Intellectual Property Law and Practice 75.

Leistner M, "Störerhaftung und mittelbare Schutzrechtsverletzung" (2010) GRUR-Beilage zu Heft 1.

Leistner M, "Copyright law on the internet in need of reform: hyperlinks, online platforms and aggregators" (2017) 12 Journal of Intellectual Property Law & Practice 136.

Levinson D, "Collective sanctions" (2003) 56 Stanford Law Review 365.

Lichtman D and Posner E, "Holding Internet Service Providers Accountable" (2006) 14 Supreme Court Economic Review 221.

Lodder A and Van der Meulen N, "Evaluation of the Role of Access Providers: Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time" (2013) 4 JIPITEC 130.

Lovejoy N, "Standards for determining when ISPs have fallen out of Section 512(A)" (2013) 27 Harvard Journal of Law and Technology 257.

Lynskey O, "Control over personal data in a digital age: Google Spain v AEPD and Mario Costeja Gonzalez" (2015) 78 Modern Law Review 522.

Lynskey O, "Regulating "Platform Power" (2017) LSE Law, Society and Economy Working Paper 3.

Lynskey O, "The Europeanisation of data protection law" (2016) 19 Cambridge Yearbook of European Legal Studies 252.

Mansell R, "Platforms of power" (2015) 43 Intermedia 20-24.

Mayer-Schonberger V, "Demystifying Lessig" (2008) 4 Wisconsin Law Review 713.

Mac Sithigh D, "The road to responsibilities: new attitudes towards internet intermediaries" (2019) 29 Information and Communications Technology Law 18.

Malgieri G and Comandè G, "Why a right to legibility of automated decision-making exists in the General Data Protection Regulation" (2017) 7 International Data Privacy Law 254.

Mann R and Belzley S, "The promise of internet intermediary liability" (2005) 47 William and Mary Law Review 26.

Manner M, Siniketo T and Polland U, "The Pirate Bay ruling" (2009) 20 Entertainment Law Review 198.

Marsoof A, "Notice and take down: a copyright perspective" (2015) 5 Queen Mary Journal of Intellectual Property Law 24.

Martens B, "JRC Technical Support reports: An economic policy perspective on online platforms" (2016) Institute for prospective technological studies digital economy working paper 34.

Marchill M, Neuberger C and Schindler F, "Transparency on the Net: Functions and Deficiencies of Internet Search Engines" (2003) 5 The Journal of policy, regulation and strategy 52.

Margoni T and Perry M, "Online intermediary liability and privatized enforcement: the Content ID case" (2016) The Tenth International Conference on Digital Society and eGovernments 36.

Mateus M, "Why should National Competition Authorities be Independent and how should they be Accountable?" (2007) 3 European Competition Journal 21.

McDougal M S, "Law as a Process of Decision: A Policy-Oriented Approach to Legal Study" (1956) 1 Natural Law Forum 67.

Mimler M, "First things first: German Federal High Court provides guidance on ISP liability in online copyright infringement cases" (2016) 11 Journal of Intellectual Property Law and Practice 485.

Montagnani M L and Trapova A, "Safe harbours in deep waters: a new emerging liability regime for Internet Intermediaries in the Digital Single Market" (2018) 26 International Journal of Law and Information Technology 294.

Monti G, "Independence, interdependence and legitimacy: the EU Commission, National Competition Authorities, and the European Competition Network" (2014) Working Paper 3.

Moohr G S, "The crime of copyright infringement: an inquiry based on morality, harm and criminal theory" (2009) 83 Boston University Law Review 731.

Mulgan R, "Accountability issues in the New Model of Governance" (2008) Discussion Paper 8.

Narveson J, "Collective responsibility" (2002) Journal of Ethics 179-198.

Lecture by Sjoera Nas, Bits of Freedom "The Multatuli Project ISP Notice & take down" (2004) is available at <<https://www-old.bof.nl/docs/researchpaperSANE.pdf> > last accessed 1 March 2019.

Nissenbaum H, "Computing and Accountability" (1994) 37 Communications of the ACM 76.

Nordemann J B, "Report for Liability of Online Service Providers for Copyrighted Content-Regulatory Action needed?" (2017) IMCO Committee is available at <[http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA\(2017\)614207_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf) > last accessed 31 October 2019.

Nordemann J B, "Internet Copyright Infringement: Remedies against Internet Intermediaries- The European Perspective on Host and Access Providers" (2012) 59 Journal of the Copyright Society of the USA 773.

Nordemann J B, "Liability for Copyright Infringements on the Internet: Host Providers (Content Providers) – The German Approach" (2011) 2 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 37.

Noto La Diega G, "Against the Dehumanisation of Decision-Making: Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection and Freedom of Information" (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 23.

OECD, "The Economic Impact of Counterfeiting and Piracy"(2008) is available at <<http://www.oecd.org/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm>> last accessed 27 March 2019.

OECD, "The economic and social role of internet intermediaries" (2010) 9 is available at <<https://www.oecd.org/internet/ieconomy/44949023.pdf>> last accessed 25 April 2019.

Ohly A, "The broad concept of "communication to the public" in recent CJEU judgements and the liability of intermediaries: primary, secondary or unitary liability?" (2018) 13 Journal of Intellectual Property Law and Practice 670.

Okoye A, "Theorising Corporate Social Responsibility as an Essentially Contested Concept: Is a Definition Necessary?" (2009) 89 Journal of Business Ethics 613.

Online censorship, "Report on unfriending censorship: insights from four months of crowdsourced data on social media censorship" (2016) 17.

Oswald L, "International issues in secondary liability for intellectual property rights infringement" (2008) 45 American Business Law Journal 247.

Oxford Economics, "The economic impact of the UK film industry" (June 2010) is available at <<https://www.bfi.org.uk/sites/bfi.org.uk/files/downloads/economic-impact-of-the-uk-film-industry-2010-06.pdf>> last accessed 30 April 2019.

Oxera, "Report on behalf of Google on the economic impact of safe harbours on Internet intermediary start-ups" (2015) 10 is available at <<https://www.oxera.com/getmedia/cba1e897-be95-4a04-8ac3-869570df07b1/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.aspx?ext=.pdf>> last accessed 29 October 2019.

Papadaki E, "Hyperlinking, making available and copyright infringement: lessons from European national courts" (2017) 8 *European Journal of Law and Technology* 2-14.

Parti K and Marin L, "Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A comparative analysis on blocking measures and internet providers' removal of illegal internet content" (2013) 9 *Journal of Contemporary European Research* 149.

Pasquale F, "Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries" (2014) 104 *Northwest University Law Review* 173.

Pasquale F, "Restoring transparency to automated authority" (2011) *Seton Hall Research Paper* 254.

Peguera M, "The DMCA Safe Harbors and their European Counterparts: a comparative analysis of some common problems" (2008) 32 *Columbia Journal of Law and the Arts* 482.

Peguera M, "Internet Service Providers' Liability in Spain: Recent Case Law and Future Perspectives" (2010) 10 *Journal of Intellectual Property, Information Technology and E-Commerce Law* 159

Perel M and Elkin-Koren N, "Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement" (2017) 69 *Florida Law Review* 181.

Perel M and Elkin-Koren N, "Accountability in Algorithmic Copyright Enforcement" (2016) 19 *Stanford Technology Law Review* 483.

Phililips J, "Three Strikes.....and then?" (2009) 4 *Journal of Intellectual Property Law and Practice* 521.

Pilutik S, "eBay's Secondary Trademark Liability Problem and its VeRO Program" (2007) is available at <<http://www.cs.cmu.edu/~dst/Secrets/E-Meter/eBay-VERO-pilutik.html>>

last accessed 27 December 2019

Posner R A, "Guido Calabresi's 'The Costs of Accidents': A Reassessment" (2005) *University of Chicago Law School* 12.

Poort J and Quintais J P, "Global online piracy study" (2018) *University of Amsterdam* 50, 51.

Quintais J P, "Untangling the hyperlinking web: In search of the online right of communication to the public" (2018) *The Journal of World Intellectual Property* 408.

Quintais J P, "The New Copyright in the Digital Single Market Directive: A Critical Look" (2019) 1 *European Intellectual Property Review* 19.

Radon, "Counterfeit Luxury Goods Online: An Investigation of Consumer Perceptions" (2012) 4 *International Journal of Marketing Studies* 74.

Ramahlo A, "Copyright law-making in the EU: what lies under the 'internal market' mask?" (2014) 9 *Journal of Intellectual Property Law and Practice* 224.

Du Rausas M P and others, "Report of McKinsey Global Institute, Internet matters, the net's sweeping impact on growth, jobs, and prosperity" (2011) is available at < https://www.mckinsey.com/~media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/Internet%20matters/MGI_internet_matters_exec_summary.ashx > last accessed 31 October 2019.

Rendas T, "How Playboy Photos Compromised EU Copyright Law: The GS Media Judgment" (2017) 20 *Journal of Internet Law* 11.

Reuters Institute for the Study of Journalism, "Reuters Institute Digital News Report 2016" (2016) is available at < <http://media.digitalnewsreport.org/wp-content/uploads/2018/11/Digital-News-Report-2016.pdf?x89475> > last accessed 31 October 2019.

Reuters Institute for the Study of Journalism, "Reuters Institute Digital News Report 2019" (2019) is available at < https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2019-06/DNR_2019_FINAL_0.pdf > last accessed 28 December 2019.

Romero-Moreno F, "Notice and stay down and social media: amending Article 13 of the Proposed Directive on Copyright" (2019) 33 *International Review of Law, Computers and Technology* 187.

Rosati E, "The CJEU Pirate Bay judgment and its impact on the liability of online platforms" (2017) 12 *European Intellectual Property Review* 748.

Rosati E, "GS Media and Its Implications for the Construction of the Right of Communication to the Public within EU Copyright Architecture" (2017) 54 Common Market Law Review 1242.

Rosati E, "Why a Reform of Hosting Providers' Safe Harbour is Unnecessary Under EU Copyright Law" (2016) 38 European Intellectual Property Law Review 668.

Rubenstein W, "The concept of equality of in civil procedure" (2002) 23 Cardozo Law Review 1.

Sander B, "Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation" (2020) 43 Fordham International Law Journal 939.

The Santa Clara Principles on Transparency and Accountability in Content Moderation is available at https://newamericadotorg.s3.amazonaws.com/documents/Santa_Clara_Principles.pdf > last accessed on 12 March 2019.

Sartori G, "Providers Liability: From the e-commerce directive to the future: In depth analysis" (2017) IMCO Committee is available at [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA\(2017\)614179_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf) > last accessed 31 October 2019.

Sauter W, "Proportionality in EU Law: A Balancing Act?" (2013) 2013 TILEC Discussion Paper 1.

Sawyer M S, "Filters, Fair Use & Feedback: User-Generated Content Principles and the DMCA" (2009) 24 Berkeley Technology Law Journal 380.

Schellekens M, "Liability of Internet Intermediaries: a slippery slope?" (2011) 8 SCRIPTed 154.

Senftleben M, "Content censorship and Council carelessness- Why the Parliament must safeguard the open, participative Web 2.0" (2018) 4 AMI 141.

Senftleben M and others, "The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform"(2016) 1-24.

Senftleben M, "Content censorship and Council carelessness – Why the Parliament must safeguard the open, participative web 2.01" (2018) 4 AMI - tijdschrift voor auteurs-, media- en informatierecht 139.

Senftleben M, "An uneasy case for notice and takedown: context-specific trade mark rights" (2012) VU Centre for Law and Governance 3.

Seng D, "Comparative analysis of the national approaches to the liability of internet intermediaries- Part I" (2010) WIPO 46.

Seltzer W, "Free speech unmoored in copyright's safe harbour: chilling effects of the DMCA on the first Amendment" (2010) 24 Harvard Journal of Law and Technology 172.

Sims C and Figueira E, "YouTube, google find safe harbour in New York Court" (2010) Communications Lawyer 3.

Škrinjar Vidović M, "Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities" (2015) Croatian Yearbook of European Law and Policy 262.

Spinello R A, "Secondary Liability in the Post Napster Era: Ethical Observations on MGM v. Grokster" (2005) 3 Journal of Information, Communication and Ethics in Society 12.

Spinello R A, "Intellectual Property: Legal and Moral Challenges of Online File Sharing" in Kenneth Einar Himma and Herman Tavani (eds.), *Handbook of Information and Computer Ethics* (2008) 553

Spindler G and Leistner M, "Secondary Copyright Infringement – New Perspectives from Germany and Europe" (2006) 37 International Review of Intellectual Property and Competition Law 788.

Stalla- Bourdillon S, "Online Monitoring, Filtering, Blocking... What is the Difference? Where to Draw the Line?" (2013) Southampton Research Paper 19.

Stalla-Bourdillon S and others, "Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society" (2016) 1-5.

Stanford report on “Similarities in Managing Supply Chain Sustainability and Intellectual Property” (2014) 4 is available at <
<https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/white-paper-vcii-sustainability-ip-supply-chains.pdf> > last accessed 31 October 2019.

Strathern M, “Improving ratings’: audit in the British University system” (1997) 5 European Review 308.

Synodinou T, “Intermediaries’ liability for online copyright infringement in the EU: evolutions and confusions” (2015) 31 Computer Law and Security Review 57-67.

Spoerri T, “On Upload-filters and other competitive advantages for big tech companies under Article 17 of the Directive on Copyright in the Digital Single Market” (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 173.

Stone Sweet A and Matthews J, “Proportionality Balancing and Global Constitutionalism” (2009) 47 Columbia Journal of Transnational Law 73.

Swiss Institute of Comparative Law, “Comparative study on filtering, blocking and take-down on illegal content on the Internet, Report commissioned by the Council of Europe” (2015) 5.

Taddeo M and Floridi L, "The Debate on the Moral Responsibilities of Online Service Providers"(2016) 22 Science and Engineering Ethics 1575.

Thompson M, “Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries” (2016) 18 Vanderbilt Journal of Entertainment and Technology Law 783.

Tsigkou C, “Notice-and-Takedown Procedure under Greek Intellectual Property Law 4481/2017” (2018) 9 Journal of Intellectual Property, Information Technology and E-Commerce Law 201.

Tuch A, “The limits of Gatekeeper liability” (2017) Washington and Lee Law Review Online 619.

Utting P, “Rethinking business regulation: from self-regulation to social control” (2005) Technology, Business and Society Programme-United Nations Research Institute for Social Development 5-6.

Van Couvering E, "Is relevance relevant? Market, Science and War: Discourses of search engine quality" (2007) 12 Journal of Computer-Mediated Communication 866.

Van Hoboken J, "Hosting intermediary services and illegal content online: an analysis of the scope of article 14 ECD in light of the developments in the online service landscape" (2018) 27 is available at <<https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en>> last accessed 5 November 2019.

Van Eecke P, "Online service providers and liability: A plea for a balanced approach" (2011) 48 Common Market Law Review 1483.

Van der Sloot B, "Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe" (2015) 6 Journal of Intellectual Property, Information Technology and E-Commerce Law 212.

Van Eecke P and Ooms B, "ISP Liability and the E-Commerce Directive: A growing trend toward greater responsibility for ISPs" (2007) 11 Journal of Internet Law 5.

Vedder A, "Accountability of and service providers – strict liability entering ethics?" (2001) 3 Ethics and Information Technology 71.

Verbiest T, Spindler G, Riccio G and Van der Perre A, "Study on the Liability of Internet Intermediaries: general trends in the EU" (2007) EU Commission study (MARKT/2006/09/E) is available at < https://ec.europa.eu/internal_market/e-commerce/docs/study/liability/> last accessed 31 October 2019.

Villeneuve N, "The Filtering Matrix: Integrated Mechanisms of Information Control and the demarcation of borders in cyberspace" (2006) 11 First Monday is available at < <https://journals.uic.edu/ojs/index.php/fm/article/view/1307/1227>> last accessed 10 May 2019.

Volkman C, "Trademark Use and Liability of Referencing Service In Keyword Advertising – Google AdWords and Trademark Law" (2011) 3 European Journal of Risk Regulation 450.

Von Dornum D, "The Straight and the Crooked: Legal Accountability in Ancient Greece" (1997) 97 Columbia Law Review 1483.

Von Blanckenburg K, "Google search abuses dominant position to illegally favour Google Shopping: an economic review of the EU decision" (2018) 20 Digital Policy, Regulation and Governance 211.

Wachter S, Mittelstadt B and Floridi L, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation" (2017) 7 International Data Privacy Law 76.

Wallberg K, "Notice and takedown of counterfeit goods in the Digital Single Market: a balancing of fundamental rights" (2017) 12 Journal of Intellectual Property Law and Practice 922.

Wexler R, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System" (2018) 70 Stanford Law Review 1383.

Wright C, "Actual versus legal control: Reading vicarious liability for copyright infringement into the Digital Millennium Copyright Act of 1998" (2000) 75 Washington Law Review 1005.

Wu F. T, "Collateral Censorship and the Limits of Intermediary Immunity" (2011) 87 Notre Dame Law Review 295-296.

Wyckoff A and Colecchia A, "The Economic and Social Impact of Electronic Commerce" (1992) OECD 12.

Yakowitz Bambauer J and Zarsky T, "The Algorithm Game" (2018) 94 Notre Dame Law Review 1.

Yu H, Xie L and Sanner S, "The Lifecycle of a Youtube Video: Phases, Content and Popularity" (2015) Proceedings of the Ninth International AAAI Conference on Web and Social Media 533.

Zerilli J, Knott A, Maclaurin J and Gavaghan C, "Transparency in Algorithmic and Human Decision-Making: Is there a double standard?" (2018) 9 Philosophy and Technology 5.

Zittrain J, "A History of Online Gatekeeping" (2006) 19 Harvard Journal of Law and Technology 253.

C. *Websites and Blogs*

Anderson N, "Verizon to forward RIAA warning letters (but that's all) Verizon looks set to forward RIAA copyright infringement notices to its ..." (ArsTechnica, 13 November 2009) is available at <<https://arstechnica.com/tech-policy/2009/11/verizon-to-forward-riaa-warning-letters-but-thats-all/>> last accessed 29 December 2019.

Anderson N, "Swedish court rules TPB admins too broke to pay damages" (Arstechnica, August 2009) is available at <<https://arstechnica.com/tech-policy/2009/08/swedish-court-rules-tpb-admins-too-broke-to-pay-damages/>> last accessed 29 December 2019.

Anderson M R, "Twenty years on from Deep Blue vs Kasparov: how a chess match started the big data revolution" (The Conversation, 11 May 2017) is available at <<https://theconversation.com/twenty-years-on-from-deep-blue-vs-kasparov-how-a-chess-match-started-the-big-data-revolution-76882>> last accessed 29 December 2019.

Andy, "YouTube's deal with universal blocks DMCA counter notices" (Torrentfreak, 5 April 2013) is available at <<https://torrentfreak.com/youtube-deal-with-universal-blocks-dmca-counter-notices-130405/>> last accessed 29 December 2019.

Andy, "Italian ISPs Say New Copyright Amendment Infringes Human Rights" (Torrentfreak, 27 July 2017) is available at <<https://torrentfreak.com/italian-isps-say-new-copyright-amendment-infringes-human-rights-170728/>> last accessed 29 December 2019.

Angelopoulos C, "CJEU Decision on Ziggo: The Pirate Bay Communicates Works to the Public" (Kluwer copyright blog, 30 June 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/06/30/cjeu-decision-ziggo-pirate-bay-communicates-works-public/>> last accessed 29 December 2019.

Angelopoulos C, "AG Szpunar in Stichting Brein v Ziggo: An Indirect Harmonisation of Indirect Liability" (Kluwer copyright blog, 23 March 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/03/23/ag-szpunar-stichting-brein-v-ziggo-indirect-harmonisation-indirect-liability/>> last accessed 29 December 2019.

Angelopoulos C, "EU Copyright Reform: Outside the Safe Harbours, Intermediary Liability capsizes into incoherence" (Kluwer copyright blog, 6 October 2016) is available at

<<http://copyrightblog.kluweriplaw.com/2016/10/06/eu-copyright-reform-outside-safe-harbours-intermediary-liability-capsizes-incoherence/>> last accessed 29 December 2019.

Angelopoulos C, “C-494/15 – Tommy Hilfiger: No Difference between Online and Real World Marketplaces for IP Enforcement” (Kluwer copyright blog, 10 August 2016) is available at < <http://copyrightblog.kluweriplaw.com/2016/08/10/c-49415-tommy-hilfiger-no-difference-online-real-world-marketplaces-ip-enforcement/>> last accessed 29 December 2019.

Belan A, “BREAKING NEWS: AGCOM issues the first fastissimo administrative blocking injunction” (IPKat, 24 April 2014) is available at <<http://ipkitten.blogspot.com/2014/04/breaking-news-agcom-issues-first.html>> last accessed 29 December 2019.

Bernal N, “EU Parliament approves sweeping digital copyright reforms” (The Telegraph, 12 September 2018) is available at <<https://www.telegraph.co.uk/technology/2018/09/12/eu-parliament-approves-sweeping-copyright-reforms-reshape-internet/>> last accessed 29 December 2019.

Berners-Lee T, “Commentary on Web architecture on Axioms of Web Architecture. Links and Law: Myths” is available at <<https://www.w3.org/DesignIssues/LinkLaw>> last accessed 29 December 2019.

Bickert M, “At Facebook we get things wrong – but we take our safety role seriously” (The Guardian, 22 May 2017) is available at <<https://www.theguardian.com/commentisfree/2017/may/22/facebook-get-things-wrong-but-safety-role-seriously>> last accessed 22 December 2019.

Boffey D, “Google fined record €2.4bn by EU over search engine results” (The Guardian, 27 June 2017) is available at <<https://www.theguardian.com/business/2017/jun/27/google-braces-for-record-breaking-1bn-fine-from-eu>> last accessed 29 December 2019.

Boscher H, “YouTube takes copyright law into their own hands with new policy on music infringement” (IPKat, 2 September 2019) is available at <<http://ipkitten.blogspot.com/2019/09/youtube-takes-copyright-law-into-their.html>> last accessed 29 December 2019.

Canada: Innovation, Science and Economic Development Canada, “Notice and Notice Regime” is available at <<http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca02920.html>> last accessed 29 December 2019.

Chee FY, “Privacy app maker files EU antitrust complaint against Google” (Reuters, 2 June 2015) is available at <<https://www.reuters.com/article/us-eu-google-antitrust/privacy-app-maker-files-eu-antitrust-complaint-against-google-idUSKBN00I1Z220150602>> last accessed 29 December 2019.

EU Commission, “Press release on State of the Union 2016: Commission proposes modern EU copyright rules for European culture to flourish and circulate” (Strasbourg 14 September 2016) is available at <http://europa.eu/rapid/press-release_IP-16-3010_en.htm> last accessed 29 December 2019.

EU Commission, “Press release on antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison-shopping service” (27 June 2017) is available at <https://europa.eu/rapid/press-release_MEX-17-1805_en.htm> last accessed 29 December 2019.

EU Commission, “Commission one step closer to restricting revenues of websites that breach intellectual property rights” (25 October 2016) is available at <https://ec.europa.eu/growth/content/commission-one-step-closer-restricting-revenues-websites-breach-intellectual-property-1_en> last accessed 27 December 2019.

EU Commission, “Press release on copyright reform clears final hurdle: Commission welcomes approval of modernised rules fit for digital age” (15 April 2019) is available at <https://europa.eu/rapid/press-release_IP-19-2151_en.htm> last accessed 27 December 2019.

EU Commission, “Press release on Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison-shopping service” is available at <http://europa.eu/rapid/press-release_IP-17-1784_en.htm> last accessed 29 December 2019.

EU Commission, “Joint statement by Vice-President Ansip and Commissioner Gabriel on the European Parliament's vote to start negotiations on modern copyright rules” (12

September 2018) is available at <http://europa.eu/rapid/press-release_STATEMENT-18-5761_en.htm> last accessed 29 December 2019.

EU Commission, “Press release on Court of Justice upholds independence of data protection authorities in case against Hungary” (8 April 2014) <http://europa.eu/rapid/press-release_MEMO-14-267_el.htm> last accessed 27 December 2019.

Chiou Th, “Greece: new notice and take down administrative mechanism for online copyright cases now in force” (IPKat, 5 March 2018) <<http://ipkitten.blogspot.com/2018/03/greece-new-notice-and-take-down.html>> last accessed 29 December 2019.

Crotty J M, “Education Is Best Weapon Against Web Piracy, not SOPA” (Forbes, 31 January 2012) is available at <<https://www.forbes.com/sites/jamesmarshallcrotty/2012/01/31/better-than-sopa-public-education-best-weapon-against-web-piracy/#76f84b504228>> last accessed 29 December 2019.

Dansby A, “Napster Files for Bankruptcy: Action part of Bertelsmann-initiated financial restructuring” (Rolling stone, 4 June 2002) is available at <<https://www.rollingstone.com/music/music-news/napster-files-for-bankruptcy-246468/>> last accessed 29 December 2019.

Datoo S, “France drops controversial 'Hadopi law' after spending millions: The 'three strikes' anti-piracy measure, introduced under Nicolas Sarkozy, would have cut off users' access to the internet” (The Guardian, 9 July 2013) is available at <<https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy>> last accessed 29 December 2019.

European Digital Rights (EDRi), “Leaked document: Does the EU Commission really plan to tackle illegal content online?” (21 September 2017) <<https://edri.org/leaked-document-does-the-eu-commission-actually-aim-to-tackle-illegal-content-online/>> last accessed 29 December 2019.

European Digital Rights (EDRI), “Spanish case law about hyperlinks” (23 April 2003) is available at <<https://edri.org/edriagramnumber7spanish-case-hyperlinks/>> last accessed 29 December 2019.

European Digital Rights (EDRI), “The Slide from “Self-Regulation” to “Corporate Censorship”” is available at <https://www.edri.org/files/EDRI_selfreg_final_20110124.pdf> last accessed 29 December 2019.

Electronic Frontier Foundation, “Section 230 of the Communications Decency Act 47 U.S.C. § 230: a Provision of the Communication Decency Act” is available at <<https://www.eff.org/issues/cda230>> last accessed 29 December 2019.

Electronic Frontier Foundation, “How SOPA Affects Students, Educators, and Libraries” (14 December 2011) is available at <<https://www.eff.org/deeplinks/2011/12/how-sopa-affects-students-and-educators>> last accessed 29 December 2019.

Electronic Frontier Foundation, “Lawrence Lessig Strikes Back Against Bogus Copyright Takedown: EFF Sues Liberation Music for Forcing Harvard Professor’s Video Off YouTube” (22 August 2013) is available at <<https://www.eff.org/press/releases/lawrence-lessig-strikes-back-against-bogus-copyright-takedown>> last accessed 29 December 2019.

Ernesto, “YouTube’s copyright protection is a total mess. Can it be fixed?” (Torrentfreak, 22 December 2018) is available at <<https://torrentfreak.com/youtubes-copyright-protection-system-is-a-total-mess-can-it-be-fixed-181222/>> last accessed 29 December 2019.

Ernesto, “UK Anti-Piracy ‘Education’ Campaign Launched, Quietly” (Torrentfreak, 1 December 2015) is available at <<https://torrentfreak.com/uk-anti-piracy-education-campaign-launched-quietly-151201/>> last accessed 30 October 2019.

Ernesto, “YouTube’s Deal with Universal Blocks DMCA Counter Notices” (Torrentfreak, 5 April 2013) is available at <<https://torrentfreak.com/youtube-deal-with-universal-blocks-dmca-counter-notice-130405/>> last accessed on 21 November 2019.

European Copyright Society, “Opinion on the Reference to the CJEU in Case C-466/12 Svensson” (15 February 2013) is available at

<<https://europeancopyrightsociety.org/opinion-on-the-reference-to-the-cjeu-in-case-c-46612-svensson/>> last accessed 10 May 2019.

Edwards J, "This child being abused in a cobalt mine is why Apple is trying to fix the mining business" (Business Insider UK, 14 May 2017) is available at <<http://uk.businessinsider.com/apple-cobalt-mine-child-labor-2017-5?r=UK&IR=T>> last accessed 29 December 2019.

Elgot J, "VW scandal: emissions cheats could face criminal charges" (The Guardian, February 2018) is available at <<https://www.theguardian.com/business/2018/feb/02/vw-scandal-emissions-cheats-could-face-criminal-charges>> last accessed 29 December 2019.

Engstrom E and Feamster N, "The limits of filtering: a look at the functionality and shortcomings of content detection tools"(2017) 17 is available at<<https://www.engine.is/the-limits-of-filtering>> last accessed 29 December 2019.

Ernesto, "PayPal starts banning VPN and SmartDNS services" (Torrentfreak, 5 February 2016) is available at <<https://torrentfreak.com/paypal-starts-banning-vpn-and-smartdns-services-160205/>> last accessed 29 December 2019.

Erikson K, "The EU copyright directive creates new legal uncertainties" (LSE Blog, 6 April 2019) is available at <<https://blogs.lse.ac.uk/businessreview/2019/04/06/the-eu-copyright-directive-creates-new-legal-uncertainties/>> last accessed 29 December 2019.

Fairless T, "EU Digital Chief Urges Regulation to Nurture European Internet Platforms: Speech illustrates policy makers' concerns over threat posed by U.S. tech companies to European industry" (Wall Street Journal, 14 April 2016) is available at <<https://www.wsj.com/articles/eu-digital-chief-urges-regulation-to-nurture-european-internet-platforms-1429009201>> last accessed 29 December 2019.

Hartmans A, "15 fascinating facts you probably didn't know about Amazon" (Business Insider, 23 August 2018) is available at <<https://www.businessinsider.com/jeff-bezos-amazon-history-facts-2017-4?r=US&IR=T#in-the-early-days-of-amazon-a-bell-would-ring-in-the-office-every-time-someone-made-a-purchase-and-everyone-would-gather-around-to-see-if-they-knew-the-customer-2>> last accessed 29 December 2019.

Hempel J, "UN Right to connectivity, Zuckerberg to the UN: the Internet belongs to everyone" (Wired, 28 September 2015) is available at <<https://www.wired.com/2015/09/zuckerberg-to-un-internet-belongs-to-everyone/>> last accessed 29 December 2019.

Hempel J, "Zuckerberg to the UN: The Internet Belongs to Everyone" (Wired, 28 September 2015) is available at < <https://www.wired.com/2015/09/zuckerberg-to-un-internet-belongs-to-everyone/>> last accessed 29 December 2019.

Hills M, "Survey: YouTube Is America's Most Popular Social Media Platform" (Forbes, 23 March 2018) is available at <<https://www.forbes.com/sites/meganhills1/2018/03/23/social-media-demographics/#59f74a57783a> > last accessed 29 December 2019.

Horten M, "Liability and responsibility: new challenges for Internet intermediaries" (LSE Media Policy Project Blog, 20 October 2016) is available at <<https://blogs.lse.ac.uk/mediapolicyproject/2016/10/20/liability-and-responsibility-new-challenges-for-internet-intermediaries/>> last accessed 29 December 2019.

Husovec M, "Compromising (on) the Digital Single Market? A Quick Look at the Estonian Presidency Proposal(s) on Art 13" (Kluwer copyright blog, 8 September 2017) is available at <<http://copyrightblog.kluweriplaw.com/2017/09/08/compromising-digital-single-market-quick-look-estonian-presidency-proposals-art-13/>> last accessed 29 December 2019.

Husovec M, "Why There Is No Due Process Online?: New Controversies in Intermediary Liability Law" (Balkan.com, 7 June 2019) is available at <<https://balkin.blogspot.com/2019/06/why-there-is-no-due-process-online.html>> last accessed 29 December 2019.

Hydra Greek mythology (Encyclopedia Britannica) is available at <<https://www.britannica.com/topic/Hydra-Greek-mythology>> last accessed 29 December 2019.

International Federation of the Phonographic Industry (IFPI), "Digital Music Report 2013: Engine of a digital world" is available at <https://www.ifpi.org/downloads/dmr2013-full-report_english.pdf> last accessed 29 December 2019.

International Federation of the Phonographic Industry (IFPI), “Digital Music Report 2019: State of the industry” is available at <<https://www.ifpi.org/downloads/GMR2019.pdf>> last accessed 29 December 2019.

International Federation of the Phonographic Industry (IFPI), “Global Music Report 2018” is available at <<https://www.ifpi.org/downloads/GMR2018.pdf> > last accessed 29 December 2019.

Information Commissioner’s Office, “ICO fines Uber £385,000 over data protection failings” (27 November 2018) is available at <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/>> last accessed 29 December 2019.

Infographique about the complaints procedure for copyright infringements online is available at <https://opi.gr/images/various/infographic_en.jpg > last accessed 29 December 2019.

Ingham T, “YouTube’s content ID fails to spot 20%-40% of music recordings” (Music Business worldwide, 13 July 2016) is available at <<https://www.musicbusinessworldwide.com/youtubes-content-id-fails-spot-20-40/>> last accessed 29 December 2019.

Investor relations, “Facebook Reports Fourth Quarter and Full Year 2018 Results” is available at <<https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx>> last accessed 29 December 2019.

Internet Governance Forum, “Dynamic Coalition on Platform Responsibility (DCPR)” is available at <<https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-platform-responsibility-dcpr>> last accessed 29 December 2019.

Irdeto, “Nearly half of consumers around the globe are willing to stop or watch less pirated video content” (8 March 2017) is available at <<https://irdeto.com/news/nearly-half-of-consumers-around-the-globe-are-willing-to-stop-or-watch-less-pirated-video-content/>> last accessed 29 December 2019.

Jacques S and Garstka K, “Automated anti-piracy systems: A call for further evidence-based policies” (Kluwer copyright blog, 4 April 2019) is available at <http://copyrightblog.kluweriplaw.com/2019/04/04/automated-anti-piracy-systems-a-call-for-further-evidence-based-policies/> last accessed 29 December 2019.

Jasserand C, “France: The Court of Cassation puts an end to the Notice and Stay Down Rule” (Kluwer copyright blog, 14 August 2012) is available at <http://copyrightblog.kluweriplaw.com/2012/08/14/france-the-court-of-cassation-puts-an-end-to-the-notice-and-stay-down-rule/> last accessed 29 December 2019.

Keller D, “DMCA classic, DMCA turbo: major new empirical research on notice and takedown operations” (The Center for Internet and Society, 20 April 2016) is available at <http://cyberlaw.stanford.edu/blog/2016/04/dmca-classic-dmca-turbo-major-new-empirical-research-notice-and-takedown-operations> last accessed 29 December 2019.

Keller D, “Filtering Facebook: introducing dolphins in the net, a new Stanford CIS White Paper – or- why internet uses and EU policymakers should worry about the Advocate General’s opinion in Glawischnig- Piesczek” (The Center for Internet and Society, 5 September 2019) is available at <https://cyberlaw.stanford.edu/blog/2019/09/filtering-facebook-introducing-dolphins-net-new-stanford-cis-white-paper-or-why> last accessed 29 December 2019.

Kiss J, “Mark Zuckerberg defends Facebook’s motives in free internet project in India” (The Guardian, 28 December 2015) is available at <https://www.theguardian.com/technology/2015/dec/28/mark-zuckerberg-facebook-india-internet-free-basics> last accessed 29 December 2019.

Kuczerawy A, “The EU Commission on voluntary monitoring: Good Samaritan 2.0 or Good Samaritan 0.5?” (KULeuven blog, 24 April 2018) is available at: <https://www.law.kuleuven.be/citip/blog/the-eu-commission-on-voluntary-monitoring-good-samaritan-2-0-or-good-samaritan-0-5/> last accessed 29 December 2019.

Letter of CEO Birkenstock Americas, “Amazon, our valued Birkenstock Retail Partners” is available at https://www.washingtonpost.com/news/business/wp-content/uploads/sites/8/2017/07/Amazon-retailer-letter-7.20.17.pdf?tid=a_inl&noredirect=on last accessed 29 December 2019.

Levi A, "Amazon's plan to fight counterfeiters will cost legit sellers a ton" (cnbc, 29 August 2016) is available at <<https://www.cnbc.com/2016/08/29/amazons-plan-to-fight-counterfeiters-will-cost-legit-sellers-a-ton.html>> last accessed 29 December 2019.

Lianos I and Botwright K, "Five ways to increase trust in e-commerce" (World Economic Forum, 22 March 2019) is available at <<https://www.weforum.org/agenda/2019/03/five-ways-to-restore-trust-in-e-commerce/>> last accessed 29 December 2019.

Matsa K E and Shearer E, "News Use Across Social Media Platforms 2018" (Pew Research Centre, 10 September 2018) is available at <<https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/>> last accessed 29 December 2019.

Moscon V, "The Council Negotiating Position on Article 13: Warning, Creators are also Part of the Game!!!" (Kluwer copyright Blog, 4 July 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/07/04/council-negotiating-position-article-13-warning-creators-also-part-game/>> last accessed on 29 December 2019.

Music Business Worldwide, "PRS deal with YouTube: what does it mean for songwriters?" (6 September 2009) is available at <<https://www.musicbusinessworldwide.com/prs-deal-with-youtube-what-does-it-mean-for-songwriters>> last accessed 29 December 2019.

Niklas J, "The regulatory future of algorithms" (LSE Media Policy Project Blog 15 August 2017) is available at <<http://blogs.lse.ac.uk/mediapolicyproject/2017/08/15/the-regulatory-future-of-algorithms/>> last accessed 29 December 2019.

Nordemann J B, "The German Bundesgerichtshof applies the latest CJEU case law on liability for linking to search engines" (Kluwer copyright blog, 6 March 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/03/06/german-bundesgerichtshof-applies-latest-cjeu-case-law-liability-linking-search-engines/>> last accessed 29 December 2019.

Nordemann J B, "Are preventive duties on hosting service providers in line with EU law? Some comments from a legal perspective on Art. 13 Draft DSM Directive and "upload filters" (Kluwer copyright blog, 28 June 2018) is available at <<http://copyrightblog.kluweriplaw.com/2018/06/28/preventive-duties-hosting-service>>

[providers-line-eu-law-comments-legal-perspective-art-13-draft-dsm-directive-upload-filters/?print=pdf](#)> last accessed 29 December 2019.

Nordemann J B, “YouTube is a hosting provider, but one with extensive duties of care, say two German Courts” (Kluwer copyright Blog, 6 November 2015) is available at <<http://copyrightblog.kluweriplaw.com/2015/11/06/youtube-is-a-hosting-provider-but-one-with-extensive-duties-of-care-say-two-german-courts/>> last accessed on 29 December 2019.

O’ Donoghue C and Albrecht K., “Spanish DPA fines Facebook €1.2 million for data protection infringements” (Reed Smith, 26 September 2017) <<https://www.technologylawdispatch.com/2017/09/privacy-data-protection/spanish-dpa-fines-facebook-e1-2-million-for-data-protection-infringements/>> last accessed 26 December 2019.

Ofcom, “General procedures for investigating breaches of broadcast licences”(2017) <https://www.ofcom.org.uk/_data/assets/pdf_file/0019/31942/general-procedures.pdf> last accessed 29 December 2019.

Oltermann P, “Tough new German law puts tech firms and free speech in spotlight” (The Guardian, 5 January 2018) <<https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight>> last accessed 29 December 2019.

O’ Reilly T, “ What is Web 2.0” (30 September 2005) is available at <<https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>> last accessed 29 December 2019.

Ortiz-Urculo, “Madrid court of appeals upholds YouTube’s liability safe harbor in Telecinco case” (Hogan Lovells website, 14 February 2014) is available at <<http://www.hlmediacomms.com/2014/02/14/safe-harbor-victory-telecincos-appeal-v-youtube-dismissed/>> last accessed 27 December 2019.

Out-Law.com, “Spain legislates for out-of-court copyright enforcement” (29 November 2018) is available at <<https://www.out-law.com/en/articles/2018/november/spain-out-of-court-copyright-enforcement/>> last accessed 29 December 2019.

Pasquale F, "Secret Algorithms Threaten the Rule of Law" (MIT Technology Review, 1 June 2017) <<https://www.technologyreview.com/s/608011/secret-algorithms-threaten-the-rule-of-law/>> last accessed 29 December 2019.

Press release BGH "Keine Urheberrechtsverletzung bei der Bildersuche durch Suchmaschinen" is available at <<http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=79566&linked=pm&Blank=1>> last accessed 29 December 2019.

Price R, "Google has been hit with a record-breaking €2.4 billion fine by the EU over its antitrust case" (UK Business Insider, June 2017) available at <<http://uk.businessinsider.com/eu-fines-google-record-breaking-antitrust-shopping-case-2017-6>> last accessed 29 December 2019.

Public education campaigns reduce tobacco is available at <<https://www.tobaccofreekids.org/assets/factsheets/0051.pdf>> last accessed 29 December 2019 last accessed 10 May 2019.

Quintais J P, "The New Copyright Directive: A tour d' horizon- Part II (of press publishers, upload filters and the real value gap)" (Kluwer copyright Blog, 17 June 2019) is available at <<http://copyrightblog.kluweriplaw.com/2019/06/07/the-new-copyright-directive-a-tour-dhorizon-part-i/>> last accessed 29 December 2019.

Reda J, "The text of Article 13 and the EU Copyright Directive has just been finalised" (Reda's website, 13 February 2019) is available at <<https://juliareda.eu/2019/02/eu-copyright-final-text/>> last accessed 29 December 2019.

Reda J, "Censorship machines are coming: It's time for the free software community to discover its political clout" (Reda's website, 6 April 2018) is available at <<https://juliareda.eu/2018/04/free-software-censorship-machines/>> last accessed 29 December 2019.

Reda J, "When filters fail: These cases show we can't trust algorithms to clean up the internet" (Reda's website, 28 September 2017) is available at <<https://juliareda.eu/2017/09/when-filters-fail/>> last accessed 29 December 2019.

Reda J, “Article 13 is back on – and it got worse, not better” (Reda’s website, 5 February 2019) is available at <<https://juliareda.eu/2019/02/article-13-worse/>> last accessed 29 December 2019.

Rosati E, “More on the Swedish application of GS Media” (IPKat, 15 December 2016) is available at <<http://ipkitten.blogspot.co.uk/2016/12/more-on-swedish-application-of-gs-media.html>> last accessed 29 December 2019.

Rosati E, “Italian court finds Google and YouTube liable for failing to remove unlicensed content (but confirms eligibility for safe harbour protection)” (IPKat, 20 April 2017) is available at <<http://ipkitten.blogspot.co.uk/2017/04/italian-court-finds-google-and-youtube.html>> last accessed 29 December 2019.

Rosati E, “Athens Court of Appeal applies CJEU GS Media linking decision and interprets ‘profit-making intention’ restrictively” (IPKat, 20 November 2017) is available at <<http://ipkitten.blogspot.co.uk/2017/11/athens-court-of-appeal-applies-cjeu-gs.html>> last accessed 29 December 2019.

Samuels, “Amazon May Have a Counterfeit Problem: The company is facing multiple lawsuits from brands who say it does not do enough to prevent fakes from being listed on its website” (The Atlantic, 20 April 2018) is available at <<https://www.theatlantic.com/technology/archive/2018/04/amazon-may-have-a-counterfeit-problem/558482/>> last accessed 29 December 2019.

Sandvig C, “Seeing the Sort: The Aesthetic and Industrial Defense of “The Algorithm” (Journal of the New Media Caucus) is available at <<http://median.newmediacaucus.org/art-infrastructures-information/seeing-the-sort-the-aesthetic-and-industrial-defense-of-the-algorithm/>> last accessed 29 December 2019.

Shipp J, “A more transparent and accountable Internet? Here’s how” (LSE Media Policy Project Blog, 24 May 2018) is available at <<https://blogs.lse.ac.uk/mediapolicyproject/2018/05/24/a-more-transparent-and-accountable-internet-heres-how/>> last accessed on 29 December 2019.

Smith S, “Birkenstock accuses Amazon of failure to tackle fake replicas”(The Telegraph, 22 December 2017) is available

at<<https://www.telegraph.co.uk/business/2017/12/22/birkenstock-accuses-amazon-failure-tackle-fake-replicas/>> last accessed 29 December 2019.

Stalla-Bourdillon S, “On Delfi v Estonia... Is it time to adopt a good-Samaritan style exemption? – Sophie Stalla-Bourdillon” (Inform’s Blog, 24 June 2015) is available at <<https://inform.org/2015/06/24/on-delfi-v-estonia-is-it-time-to-adopt-a-good-samaritan-style-exemption-sophie-stalla-bourdillon/>> last accessed 29 December 2019.

Starzak A, “When the Internet (Officially) Became the Public Square” (Cloudflare, 21 June 2017) is available at < <https://blog.cloudflare.com/internet-became-public-square/>> last accessed 29 December 2019.

Statista, “Most popular social networks worldwide as of April 2019, ranked by number of active users (in millions)” is available at < <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>> last accessed 29 December 2019.

Tassi P, “The Injustice Of The YouTube Content ID Crackdown Reveals Google's Dark Side” (Forbes, 19 December 2013) is available at <<https://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/#5336a67866c8>> last accessed 29 December 2019.

Venkant S, “When an algorithm isn’t” (Medium, 2 October 2015) <https://medium.com/@geomblog/when-an-algorithm-isn-t-2b9fe01b9bb5> last accessed 29 December 2019.

Warmann M, “Google is the 'judge and jury' in the right to be forgotten” (The Telegraph, 14 July 2014) is available at <<https://www.telegraph.co.uk/technology/google/10967211/Google-is-the-judge-and-jury-in-the-right-to-be-forgotten.html>> last accessed on 29 December 2019.