



UNIVERSITY OF MACEDONIA
DEPARTMENT OF APPLIED
INFORMATICS

DEMOCRITUS UNIVERSITY OF
THRACE
FACULTY OF LAW

INTERDISCIPLINARY POSTGRADUATE PROGRAM
MASTER OF SCIENCE IN LAW AND INFORMATICS

**DESIGNING AN EFFECTIVE COPYRIGHT ENFORCEMENT
STRATEGY FOR ONLINE CONTENT-SHARING SERVICE
PROVIDERS IN LIGHT OF THE DIRECTIVE (EU) 2019/790**

ALGORITHMIC ENFORCEMENT, EFFECTIVE PREVENTIVE MEASURES FOR
OCSSPS AND BALANCE BETWEEN COPYRIGHT AND FUNDAMENTAL RIGHTS

Master's Thesis

of

Chatsios Ioannis

Thessaloniki, October 2020

DESIGNING AN EFFECTIVE COPYRIGHT ENFORCEMENT STRATEGY FOR
ONLINE CONTENT-SHARING SERVICE PROVIDERS IN LIGHT OF THE
DIRECTIVE (EU) 2019/790

Chatsios Ioannis

LL.B. Faculty of Law, Democritus University of Thrace, Komotini, Greece, 2013
Master in Business Administration, American College of Thessaloniki, Greece, 2017

Master's Thesis

Submitted as a partial fulfillment of the requirements of

INTERDISCIPLINARY POSTGRADUATE PROGRAM
MASTER OF SCIENCE IN LAW AND INFORMATICS

Supervisor: Stavridou Sylvia, Assistant Professor of Commercial and Financial Law,
Democritus University of Thrace, Greece

Approved by the examining committee on 30/10/2020

Stavridou Sylvia

Babetas Georgios

Fouliras Panagiotis

.....

.....

.....

Chatsios Ioannis

Περίληψη

Η παρούσα έρευνα ασχολείται με το ζήτημα της ευθύνης των παρόχων υπηρεσιών διαδικτύου και ειδικότερα αυτών οι οποίοι παρέχουν υπηρεσίες δημοσίευσης ανταλλαγής περιεχομένου στους χρήστες τους. Συγκεκριμένα, προσεγγίζει το ζήτημα από τη σκοπιά των δικαιωμάτων πνευματικής ιδιοκτησίας, ιδίως όπως αυτά εξειδικεύονται στην πρόσφατη οδηγία 2019/790 της Ευρωπαϊκής Ένωσης. Το κεντρικό ζήτημα είναι η ανάλυση της αποτελεσματικότητας και νομιμότητας των μέσων που οι πάροχοι διαθέτουν για την αναγνώριση και τον περιορισμό της πρόσβασης σε περιεχόμενο που παραβιάζει τα πνευματικά δικαιώματα τρίτων. Ιδίως ασχολείται με τους αυτοματοποιημένους μηχανισμούς αναγνώρισης και διαχείρισης περιεχομένου που αποτελούν προωθούνται τόσο από την αγορά όσο και de facto από την Οδηγία, ως υψηλά πρότυπα επαγγελματικής ευσυνειδησίας

Οι μέθοδοι που οι πάροχοι χρησιμοποιούν για να αποκλείσουν την πρόσβαση σε περιεχόμενο που έχουν αναφορτώσει οι χρήστες τους και παραβιάζει τα πνευματικά δικαιώματα τρίτων, στην προσπάθειά τους να απαλλαγούν από την ευθύνη γι' αυτό, τοποθετούν θεμελιώδη ανθρώπινα δικαιώματα των χρηστών και του κοινού σε ευάλωτη θέση. Ταυτόχρονα τίθενται ζητήματα ανταγωνισμού και λογοδοσίας αναφορικά με τις επιλογές τους. Η φορτισμένη διαμάχη γύρω από την προσπάθεια εξισορρόπησης δικαιωμάτων και συμφερόντων προ της ψήφισης της οδηγίας είναι χαρακτηριστική και υπογραμμίζει την κλίση προς την πλευρά της δυσανάλογης καταστολής των δικαιωμάτων των χρηστών σε σχέση με τα δικαιώματα πνευματικής ιδιοκτησίας. Προσπάθησα να αναλύσω τα σημεία στα οποία οφείλει να σταθεί η περαιτέρω εξειδίκευση και ενσωμάτωση της οδηγίας στις επιμέρους εθνικές νομοθεσίες. Κάνοντας σχετική βιβλιογραφική επισκόπηση και μελετώντας περιπτώσεις των διαθέσιμων για τους παρόχους επιλογών σήμερα, των χαρακτηριστικών, των ορίων και των κινδύνων τους και προτείνοντας σχετικές λύσεις όπως ο συνδυασμός αυτοματοποιημένης αναγνώρισης και ανθρώπινου ελέγχου, η χειραφέτηση των χρηστών στη διαδικασία επιβολής της εφαρμογής της νομοθεσίας, η μεγαλύτερη διαθεσιμότητα στοιχείων και ο αποτελεσματικότερος μηχανισμός υποβολής καταγγελιών και επανόρθωσης. Παράλληλα ανέτρεξα στις αποφάσεις του ευρωπαϊκού δικαστηρίου οι οποίες διασαφηνίζουν έννοιες και ειδικότερα θέματα όπως αυτά προκύπτουν από τη λειτουργία των παρόχων σε επίπεδο πνευματικών ιδιοκτησίας.

Κατά την άποψη του γράφοντος η κατάσταση αναφορικά με τα πνευματικά δικαιώματα στο διαδίκτυο και τους κινδύνους που ελλοχεύουν με τις τελευταίες εξελίξεις σε νομοθετικό επίπεδο δεν διαφαίνεται όσο δυσοίωνα όσο εκφραζόταν στη διαμάχη που προηγήθηκε της ψήφισης του κειμένου της οδηγίας 2019/790, ωστόσο ο κίνδυνος για θεμελιώδη δικαιώματα του κοινού, για τον ανταγωνισμό αλλά και για τη δυσχέρεια αποζημίωσης των μικρών δημιουργών είναι

πραγματικοί και θα πρέπει να ληφθούν υπόψη από τα κράτη-μέλη καθώς θα ενσωματώσουν στην εθνική νομοθεσία την οδηγία.

Λέξεις Κλειδιά: ευθύνη παρόχων, πάροχος υπηρεσιών διαδικτύου, πάροχοι επιγραμμικών ενιαία ψηφιακή αγορά, παράνομο περιεχόμενο, πνευματική ιδιοκτησία, προσβολή πνευματικής ιδιοκτησίας, επιτροπή κατά της πειρατείας, απόσυρση περιεχομένου, διακοπή πρόσβασης, φίλτρα, Οδηγία 2019/790

Abstract

The present thesis examines the thorny issue of copyright enforcement for online service providers and the balancing of intellectual property with fundamental human rights in light of the recent Digital Single Market directive coming into force and the fierce debate it generated before its text was finalized. I attempted to examine the measures taken by online content-sharing service providers, including automated content recognition and decision-making systems, discuss their issues and ideate on feasible solutions with a view towards a fair and balanced copyright system.

From my point of view, the current situation is not as dire as is often presented. By using a combination of automated systems and human review in a transparent way that includes the empowerment of users and small rightholders in its implementation, the regime proposed by the DSM directive can be a blueprint for a fair solution for all parties. The limitations of current measures and market-based solutions and the practices of OCSSPs and large rightholders and relevant CJEU rulings illuminate the safeguards and considerations that need to be respected to that end.

For the sake of completeness and clarity I have performed a literature review of the research on ISP liability in a global scale, the measures of restricting access to online content and the effects of algorithmic enforcement on fundamental rights and the competition. The danger of a de facto imposition of general monitoring and overenforcement have been identified as the greatest issues among others, pointed out by several researchers recently. The CJEU has clarified several concepts and responded on problematic issues with regard to copyright and fundamental rights. Finally, and have also studied the cases of relevant market-based solutions and found a very limited range of alternative solutions for OCSSPs.

Technological developments and novel ways of media consumption evolve in an unprecedented pace which indicates that the conclusions of this study are by no means final, nor are the current legal provisions. However, I attempted to perform a comprehensive review and ideation taking all the conflicting interests into account in pragmatic terms in order for it to be relevant as member-states have yet to implement the directive into their national legislation.

Keywords: OCSSPs, ISP, ISP liability, intermediary liability, notice and takedown, algorithmic enforcement, user generated content website blocking, overenforcement, user generated content, DMCA

Acknowledgments

As this thesis marks the culmination of the Law and Informatics postgraduate program, I would like to take a moment to appreciate all the people that were with me throughout this intriguing and challenging period, which allowed me to discover new academic and professional interests and helped me grow on a personal level.

Firstly, I would like to thank Sylvia Stavridou, the supervisor of this thesis, who inspired me to research this complex and challenging subject and aided me with her feedback and advice to produce a result I am proud of.

I would also like to thank each and every one of the faculty members for enriching this innovative program with their expertise and perspectives. It is this variety of points of view that really made for an intriguing experience.

Of course, this whole adventure would not be the same without my classmates and friends. Evi, Kelly, Matina, Vangelis and everyone else, the time we spent together made this fulfilling and wishing to go back and relive it once more.

To all my friends that shared the moments of joy and frustration, I am thankful. Angelos, Christina, Giorgos, Lia, Panos, you experienced the worst of it but helped me push through, thank you.

Finally, I'd like to express my gratitude to my parents and brother; your unwavering support through the ups and downs of this journey was invaluable and I'm forever grateful.

"Spiral Out, Keep Going" - Maynard James Keenan

Table of Contents

DESIGNING AN EFFECTIVE COPYRIGHT ENFORCEMENT STRATEGY FOR ONLINE CONTENT-SHARING SERVICE PROVIDERS IN LIGHT OF THE DIRECTIVE (EU) 2019/790 ALGORITHMIC ENFORCEMENT, EFFECTIVE PREVENTIVE MEASURES FOR OCSSPS AND BALANCE BETWEEN COPYRIGHT AND FUNDAMENTAL RIGHTS	1
Περίληψη	1
Abstract	3
Acknowledgments	4
Table of Contents	5
List of Abbreviations	8
CHAPTER 1	9
1. Introduction	9
1.1 Problem Statement	9
1.1.1 The evolution of the internet in everyday life and media consumption	9
1.1.2 Internet Service Providers at the epicenter	10
1.2 Aim and Scope of the study	12
1.3 Research questions	13
CHAPTER 2	15
2. Methodology and Key Concepts	15
2.1 Key Concepts	15
2.1.1 Definitions	15
2.1.1.1 Layers approach	17
2.1.2 Focusing on Online Service Providers	17
2.1.2.1 Meaning and context of liability for OCSSPs	18
2.1.2.2 Why are OCCSPs being targeted for the actions of their users?	19
2.1.2.3 Limits and exemptions from intermediary liability – Safe harbors	20
2.1.2.4 OCSSPs and human rights	21
2.2 Basic Legislation	21
2.2.1 EU Legal Framework	22

2.2.1.1 The contentious art. 17 of the DSM directive	24
2.2.2 The U.S. regime and the DMCA	25
2.2.3 Relevant Case Law	26
2.3 Literature Review and Contribution	27
CHAPTER 3	29
3. Main Discussion	29
3.1 Current situation with OCSSPs	29
3.1.2 Copyright infringement	30
3.2 Solutions for the detection and blocking of copyrighted content	31
3.2.1 Algorithmic enforcement as the foundation of detection and moderation of content	31
3.2.1.1 ContentID	34
3.2.1.2 Audible Magic	36
3.2.1.3 Other Automated Content Detection Systems	36
3.2.2 Case Specific Measures	37
3.2.2.1 Notice and takedown	37
3.2.2.2 Blocking Injunctions	39
3.2.2.3 Website Blocking	40
3.2.2.4 Removal	41
3.2.2.5 Search Engine Removal – De-indexing	42
3.2.2.6 Bad Actor listings	43
3.2.2.7 Traffic Shaping – Data Caps - Disconnection	44
3.3 Issues with the prevalent prevention measures	46
3.3.1 General Monitoring	46
3.3.2 Overenforcement	47
3.3.3 Mistakes in copyright enforcement	49
3.3.4 Loss aversion	50
3.3.5 Private authors’ and small rightholders’ cul-de-sac	51
3.3.6 Power imbalance between sender and user – imbalanced incentives for OCSSPs	52
3.3.7 Competition – Proportionality	53
3.3.8 Transparency and Accountability	55

3.4 Proportionality – Balancing of competing rights	56
CHAPTER 4	59
4. Recommendations – Designing a strategy	59
4.1 Improving Algorithmic Enforcement	59
4.1.1 A balanced combination of automation and human review	60
4.1.2 Empowering users from the upload stage rather than relying solely on complaint and redress mechanisms	61
4.2 Battling overenforcement	62
4.2.1 Data-driven approach to identify clusters of bad notices	63
4.3 Competition issues	63
4.4 Improving the complaint and redress mechanism by incentives	65
4.5 Non-commercial User-generated Content	66
CHAPTER 5	67
5. Conclusion	67
5.1 Synopsis	67
5.2 Thesis Limitations and recommendations for future research	69
Bibliography	70

List of Abbreviations

CJEU: Court of Justice of the European Union

DMCA: Digital Millenium Copyright Act

DSM Directive: Directive (EU) 2019/790 Of the European Parliament and Of the Council

EU: European Union

ISP: Internet Service Provider

OECD: Organization for Economic Co-operation and Development

OCSSP: Online Content-Sharing Service Provider

U.S.: United States

CHAPTER 1

1. Introduction

The first chapter offers a brief introduction to the subject of this thesis by making an overview of the influence which the evolution of the internet has had in media consumption and everyday life, all the way to the challenges it currently poses in the effort to create a fair intellectual property landscape. Next follows a description of the aim and scope of the present study and a brief illustration of the research questions, concluding with a condensed outline of the study.

1.1 Problem Statement

1.1.1 The evolution of the internet in everyday life and media consumption

The interplay of creation and consumption of content has never been easier than today, in the era of digital revolution. Traditional means of enjoying creative works increasingly give way to digital consumption. This raises an important question; as digital consumption becomes the norm, is the current copyright regime up to the task of providing a level playing field for rightholders, users and the service providers that act as intermediaries and facilitate media consumption? To understand the complexity of the issue, we need to look into the history.

The extent to which technology has penetrated human life over the past few decades makes it easy to forget how quickly the use of the internet and digital devices has risen to prominence. The velocity of technological progress and its application to every human activity is unprecedented. It is hard to recall daily life without being online at all times, let alone a household with no internet access; yet domestic internet connection has been widespread for only about two decades and solely in developed countries, not to mention social media, smart devices and cloud computing that have been a feature for less than a decade for the majority of the population. The internet has become a ubiquitous entity in both our professional and personal lives. Yet the pace of this evolution far surpasses the ability of policymakers to adapt. (Mostert & Lambert, 2019)

The Internet itself has evolved in unpredictable ways often irrespective of its original purpose or the vision of its pioneers. From an innovation with a narrow scope of applications, used by a limited number of individuals with relevant expertise, it developed into a professional tool, an entertainment outlet and it is today a de facto public space, a platform where governmental functions take place with increasing levels of integration. The Internet is not a mere tool anymore, but rather an ecosystem where personal and business life occurs, functionally impossible to distinguish from the physical world.

Consequently, it is reasonable for people and governments to lament the uncertainty of the rules that apply to such an integral part of their lives – or even the lack thereof. It is not, however, an unpredictable outcome, given the velocity that breakthroughs and novel applications become widely available. The landscape changes seemingly overnight. Policymakers are not used to such an unstable environment.

Internet has also given birth to a borderless and instant-access global marketplace, a stage where the behemoths of global trade compete for popularity and dominance. It is impossible to write the 21st century's history so far by observing only peoples' apparent behavior. A lot is decided and shaped from the competition of these companies and the algorithms developed to support their pursuit of a larger market share.

1.1.2 Internet Service Providers at the epicenter

In that vein, public and governmental focus often shifts to the actors that facilitate this ecosystem; a wide array of companies that build and maintain the structure of the internet, innovate and deliver services to the public in an uncoordinated yet interconnected manner. These actors are referred to as online service providers / internet service providers due to their function and commonly referred to in the relevant literature as (online) *intermediaries* in discussing their role and liability in legal terms. Online intermediaries orchestrate commercial, social and political life in a global scale and they can influence the dissemination of ideas as gatekeepers and curators of online content. The “Cambridge Analytica”¹ case is a notorious example that highlighted how a social network can shape public opinion and influence world politics; able to cause an outsized impact in subtle ways that an individual might never notice. A subset of Internet Service Providers, termed Online Content-Sharing Service Providers (OCSSPs) by the EU Digital Single Market Directive, are dominating entertainment today, and are especially significant for this study.

Rather than lamenting this development, we must rather examine the characteristics, actions and objectives of the actors that foster this progress in order to discover pragmatic regulatory solutions that respond to the increasing velocity and complexity of media consumption online. Since all types of human interaction takes place online, crime and illegal activity are now exception, in some cases perpetrated by individuals unaware of their illegal activity. From internet fraud, phishing, identity theft and copyright infringement on a small or commercial scale to terrorist activities, cybercrime can take many forms. The focus of this thesis will be on copyright infringement in online content-sharing platforms.

¹<https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>

In this globalized and chaotic setting, intellectual property rules have to evolve in order to serve their purpose. A copyright holder status is not limited to them being acknowledged as the exclusive rightful owner of a work; instead copyright legislation must offer them the necessary tools to control the ownership and dissemination of their creative work, including avenues to get remunerated for it, ultimately fostering creativity. Intellectual property is protected the same way physical property is, according to the European Charter of Fundamental Rights, art 17(2).² As the ways that consumers can find and enjoy content evolve, copyright protection must evolve along the same track and seek a compromise between its inherent goal of fostering creation and limiting unlawful dissemination, ensuring that creators are fairly compensated for their effort. This underlying compromise will serve as the fundamental principle for analyzing the different schemes and methods of preventing the access to infringing content herein, taking always into account its compliance or conflict with other fundamental rights.

At the core of the issues described above lie the online service providers, or intermediaries. They play an integral role in the publication, dissemination and general availability of copyrighted content. Their role spans from the provision of the means for those activities, to the active facilitation of access via their algorithms and their own efforts for business growth. A central function of providers today is the collection of user data in order to serve those users content tailor made for their interests, playing an active role in the dissemination of content. At the same time, they enable both the exercise of the rightsholders' exclusive copyrights as defined by the relevant laws as well as the medium that bad actors use for copyright infringing activity. Ideally facilitating the former and inhibiting the latter.

It is important to highlight the intricate role of the intermediaries in this context. Intermediaries are of course subject to regulation; they have to adhere to the laws and regulations that outline the frame within which they operate. They also have to cooperate with authorities and be actively involved in the process of identifying and investigating illegal activity. At the same time, they are de facto regulators themselves. This has been described as the “shift in perception of ISPs from being mere conduits to active gatekeepers of content uploaded and shared by users”. (Frosio & Mendis, 2020) They provide an online service to their customers, regulated by certain conditions, namely those that are described in their “privacy policy” and “terms and conditions” sections that govern their relationship with their users or customers. According to Riordan they are “points of control”. (Riordan, 2013). The third element illustrating their sui generis role is that they are for-profit businesses at their core, so they have

² <https://fra.europa.eu/en/eu-charter/article/17-right-property>

to balance all these conflicting obligations to offer a lawful yet attractive product mix.

In the same vein, the relevant legislation has to take into account that conflict of interest. To what level is it going to restrict their freedom to conduct business (as an extension of the freedom of expression) in the balancing act between different types of conflicting rights and values to be protected. Simply put, there can hardly be regulation of the end users' behavior without taking into account and cooperating with intermediaries of all kinds.

1.2 Aim and Scope of the study

Despite different regulatory approaches for intellectual property in the U.S. and the EU, media consumption online is a global phenomenon, a de facto global market. The most recent legislative attempt to regulate it as such is the directive (EU) 2019/790 of the European Parliament and of the Council, aptly titled "Directive on Copyright in the Digital Single Market". The title confirms the reality of the borderless nature of intellectual property today, but its content includes both converging and diverging mandates. Being the most recent and fiercely debated development in the field, the directive and the academic discussion around it will serve as the guidepost for the present study's examination of how ISPs can administer content and the balancing of rights in that process. Moreover, given that EU member states have yet to implement the directive into their national law, there is still fine tuning to be made.

As such, in light of the DSM directive coming into force, in the present thesis I am attempting to examine the dissemination of copyright infringing material over the internet, focusing on platforms hosting user generated content or Online Content-Sharing Service Providers³. The purpose of this study is to examine the landscape, the preventive measures taken and especially the algorithmic enforcement that surfaces as the most potent and prevalent measure, using current market-based solutions as a benchmark, taking into account the interplay and balancing of rights between rightholders, users and platforms. It will be evident that one-off measures are not sufficient and that a complete strategy is needed. While I will discuss case-specific measures, in my view the goal has to be the optimization of detection and the empowerment of both the user and the rightholder in the process of copyright enforcement from the initial stages. This is the only way that the goal of a "digital single market" can be realistic while fundamental human rights are respected.

Consequently, I am going to focus on the subset of Internet Service Providers that are included in the definition of the directive and cases of copyright infringement rather than the totality of unlawful activities performed using online content service providers. In a more granular level, the ways

³As referenced in the directive

intermediaries can prevent the publication, storage and access to this type of material in a financially sustainable way, while also examining the drawbacks and limitations of current copyright enforcement practices and their impact on fundamental human rights.

Concluding this study, I will attempt to provide recommendations on current practices, solutions and insight on how the refinement of technological measures and the ideas generated in the debate around the final text of the directive can create a path for a fairer intellectual property landscape online.

The overall objective of this study is to conduct a literature review of the matters in question, discover the approaches suggested currently in the literature and provide ideas based on the theory's current body of work.

1.3 Research questions

By the word effective in the title I am trying to encompass distinct elements. An effective protection encompasses the copyright holders' rights, ISPs right to conduct business with reasonable financial burden, while at the same time creators' and consumers' fundamental rights of expression and access to information by not obstructing lawful creation and consumption.

For the present study I will begin by reviewing some key concepts and definitions and describing the role and liability of online service providers in today's copyright landscape and briefly review the European and global legal framework, as well as instructive case law on those matters. I will attempt to provide a quick synopsis of the relevant literature before going into detail on the ideas expressed in the academic discourse these past few years, and locate this study within this discourse.

In the main discussion and recommendations sections, I attempt to unfold the literature's findings and provide insight on four questions, bearing in mind that they are inextricably interwoven and the analysis of each one permeates the others.

First of all, what is the copyright situation for OCSSPs currently, in light of the DSM directive coming into force, and how the new regime proposed influences their choices? Are the new provisions on safe harbors having a trickle-down effect on users and the public?

Based on that I am going to examine the solutions OCSSPs employ in order to manage content on their platforms. Central in that analysis is the role of algorithmic enforcement that has become prevalent today and is in need of further analysis as it is being promoted by the DSM directive. At the same time I am touching upon the other measures ISPs have in their disposal to administer access to copyrighted content?

After outlining the OCSSPs and the tools they use to combat copyright infringement, follows the question of whether or not there are issues with the

current prevention measures. I will attempt to analyze the challenges posed by the aforementioned measures, and especially the matters of potential censorship, overenforcement and proportionality, regarding competition but more importantly in the balancing of copyright measures against fundamental human rights.

Finally, the question arising from the discussion is: Is the copyright enforcement system broken and the wishes of the EU parliament and the council for a Digital Single Market overly optimistic? Are the safeguards to fundamental rights empty letter? My view is that this is not the case, and given that the stakeholder dialogue will specify the implementation of the directive in member states, I will attempt to provide recommendations on feasible improvements based on algorithmic enforcement application so far.

CHAPTER 2

2. Methodology and Key Concepts

The present thesis aims to examine the current solutions for OCSSPs to monitor and restrict access to content on their websites and platforms and discuss the limitations and potential of the prevalent measures taken today within the context of the DSM Directive, as well as the latest views of the literature and the courts, especially the CJEU on the matter. In order to do that I proceeded based on the one hand on a literature review of the recent academic discourse, legislation and case law, and on the other hand on examining cases of currently available market-based solutions.

2.1 Key Concepts

The present thesis is addressed to individuals with a legal background, familiar with fundamental concepts of Internet Law. However, as it is focused on copyright and especially copyright in a digital context, I considered it useful to outline some necessary concepts regarding intellectual property and Internet Service providers, as well as the relevant legislation and case law. This brief analysis aims to define certain technical terms and provide a structure to the discussion about ISP liability in a global setting that will instruct the analysis of legal and technical measures later on, as well as the conversation about the balancing of rights and the feasibility of the recommendations from a financial and competition perspective.

2.1.1 Definitions

The public's access to the internet is facilitated by a wide range of services, provided by companies that can generally be called "intermediaries" or "Online/Internet Service Providers" as stated above. These intermediaries are online service providers and can be directly related to the end customer or not. They constitute a vast network of interrelated services that shape the internet as we know it today. Note that while "online service providers", "internet service providers" and "intermediaries" are not interchangeable terms, their differences are not yet crucial in the scope of this study. The broad definition given by the Organization for Economic Co-operation and Development (OECD), the intergovernmental economic organization centered around economic progress and world trade that is interested in policies on these matters is a solid starting point. (OECD, 2011)

"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."

Further, OECD breaks down an instructive list of six categories of ISPs, while also distinguishing between intermediaries publishing their own content or dealing their own products and the ones that deal with third party content and products – “pure” intermediaries.

1. Access providers
2. Hosts and registrars
3. Search engines and portals
4. E-commerce platforms
5. Payment Systems
6. Participatory Networking platforms (“Social Media” in simple terms)

From a copyright perspective, the most important subset of ISPs is those that host or index user-uploaded third-party material and user-generated content – the difference being that the latter category refers to content created by the user. The DSM directive defines those as Online Content-Sharing Service Providers (OCSSPs). It is them that fall under the scope of the crucial Article 17 of the DSM directive, and that are threatened to become directly liable for the actions of their users.

Referencing the directive verbatim, we can surmise the elements of those OCSSPs:

‘online content-sharing service provider means 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. Providers of services, such as not-for-profit online encyclopedias, not-for-profit educational and scientific repositories, open source software-developing and-sharing platforms, providers of electronic communications services 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.⁴

Recital 62 of the same directive explains that the definition of an online content-sharing service provider “should target only online services that play an important role on the online content market by competing with other online content services”. However, as Schwemer (2020) notes, this additional specification is unclear, as the meaning and the assessment of that “important role” is contestable.

It is obvious, but it bears repeating and is expressly stated in the directive, that commercial level piracy and platforms created to circulate pirated

⁴DSM Directive, Art. 2(6)

content fall outside the scope of any liability exceptions. Verbatim from recital 62 of the copyright directive, “in order to ensure a high level of copyright protection, the liability exemption mechanism provided for in this Directive should not apply to service providers the main purpose of which is to engage in or to facilitate copyright piracy.”⁵

2.1.1.1 Layers approach

Another approach of systematizing the different categories and functions of intermediaries is the “layers approach” (Riordan, 2013) that draws the line between the application, network and physical elements. It should be born in mind though, that as vertical integration happens in the industry, a lot of times the lines are blurred between those layers. Thus, the following figure is more instructive to understand the architecture of the internet and online service providers rather than an accurate depiction of the structure of the market today.

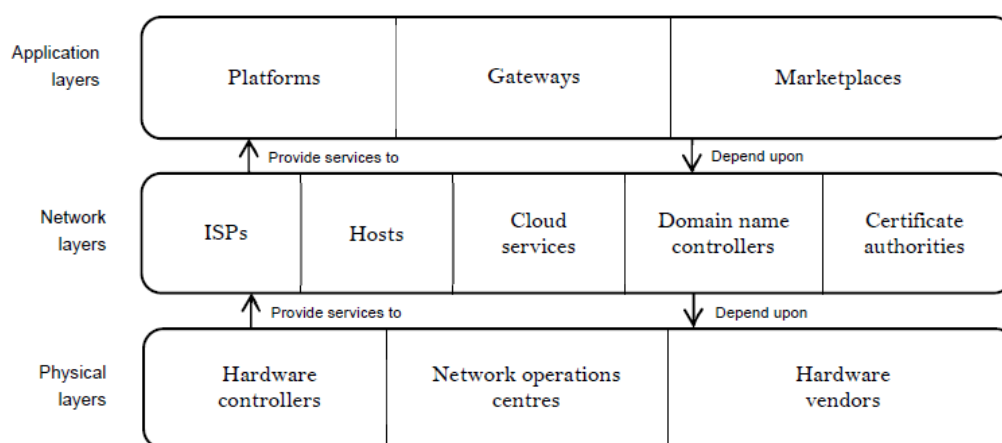


Figure 1 - Layers Approach (Riordan 2020)

It is clear that the scope of this study reflected through the DSM directive refers to the Network and Application layers. It is those categories of online service providers that engage in decision-making and are asked to take measures by the law. It is possible, however, that physical layer services may be included in the enforcement stage.

2.1.2 Focusing on Online Service Providers

The network of ISPs, from social media platforms to hosting and internet access providers, inevitably involves various jurisdictions as there is no geographical limitation in regards to where a company or the physical equipment used to ultimately serve a website or a service are based. This makes international rules a necessity and the alignment of the various policy approaches a constant challenge. The lines dictating which jurisdiction should be used are blurred, a situation that impedes the formation of a single market.

⁵DSM Directive, recital 62, pg. 108

The creation of a digital single market is the explicit goal of the Directive EU 2019/790. It is harder to foster an environment of security for both businesses and users without clarity about the rules that apply. Do companies and users act based on the wider scope of protection or do they use the lowest common denominator, minimizing their risk and being cautious about innovation?

It must be noted that innovation in this particular example is driven by competition on an international level. Thus, competition has to be protected and promoted by competition law. Regulatory inconsistencies and uncertainty create an unstable environment for competition that can be exploited and favor firms with access to more market-favorable legislations and mainly the already dominant Big Tech companies.

Further complexity is added by the question of when are the intermediaries liable. Riordan (2013) argues that by design this framework uses intermediaries in order to create, transmit and store information. Internet users depend upon a growing number of parties to access online content and acquire services in which case the intermediaries that supply this content and services deal with substantial quantities of information that is created, edited and uploaded by others.

As Castets-Renard (2020) notes, “intermediaries today do much more than passively distribute user content and facilitate user interactions. They now have near-total control of users’ online experience and content moderation”. Obviously, they stray from the “mere-conduit” role envisioned for the safe-harbor exceptions that will be mentioned in the following chapter.

2.1.2.1 Meaning and context of liability for OCSSPs

The term “liability” in the context of ISPs does not necessarily indicate the obligation for monetary remuneration for a wrongdoing. In most cases intermediary liability entails non-monetary remedies (Riordan, 2013), especially in cases when intermediaries are not the primary wrongdoer.

Similarly, intermediary liability forms the basis of their obligation to assist in investigation by sharing information and of course spearhead the attempt to prevent further spreading of unlawful material by obstructing the access to it. More detailed discussion over the specific measures follows in chapter 3.

This information wouldn’t be published without their facilitation. Especially when we focus on online content-sharing platforms, they influence how the material is presented and to whom, assuming an active role in the dissemination of content. ISPs today are not singularly focused neutral conduits, as would the “safe harbor” rules dictate but, more often than not, have transformed to integrated, wide-spanning networks that influence business and personal lives, shape political opinion (i.e. the infamous Cambridge Analytica scandal) and can be at the same time the victim, gatekeeper, facilitator and investigator of illegal activity.

“Secondary liability” is called the liability of a person or entity for the actions of another party and occurs when someone induces, facilitates or is in some form responsible for unlawful actions of another party. ISPs’ secondary liability is discussed herein because they bring together or facilitate transactions between third parties over the internet. (Sartor, 2017) Concurrent to that, is their role as a de facto public space, available to an indeterminable number of people, for whom they provide the medium for communication, transmission of information and economic activity. In an attempt to prevent possible stifling of innovation, policymakers have implemented exemptions and limits to the liability of intermediaries for content posted by their users, chief among which are the “safe harbor” rules introduced in the U.S. by the Digital Millennium Copyright Act (DMCA) and adopted at the European level by the e-Commerce directive⁶.

That was the case until the introduction of the DSM which diverges from the “safe harbor” principle that grants immunity to those service providers that are not aware of a particular infringement and act expeditiously to remove the content if they are notified of such an instance. In light of ar. 17 of the Digital Single market directive, online content-sharing providers will be responsible for copyright infringement unless the use of works on their platforms is authorized or if they have made ‘best efforts’ to obtain an authorization and prevent the availability of unlicensed works” (Schwemer & Schovsbo, 2020). As such, art. 17 introduces the threat of direct liability for OCSSPs for the wrongdoing of their users, *unless* they meet certain criteria.⁷ It represents the gradual move from intermediary liability to intermediary responsibility. (Kuczerawy, 2019)

2.1.2.2 Why are OCCSPs being targeted for the actions of their users?

In terms of copyright infringement online, initially victims sought enforcement against the primary wrongdoers. However, internet users’ relative anonymity and the multitude of services necessary for the performance of any action made investigation impractical in terms of scale and intrusive with regard to privacy. Thus, when copyright enforcement against primary infringers began to fail, claimants had to turn to the points that facilitated the hosting, dissemination and exchange of copyrighted material, i.e. online service providers. (Riordan, 2013) Ultimately, the question was the need for a modernization of liability rules for the digital age and the role of ISPs in copyright enforcement.

Intermediaries are – as evidenced by the terminology – in the midst of any illegal activity happening online. They are in a unique position where they facilitate such activity and consequently at the closest place to identify and

⁶ More detailed reference under section 2.1.2.3

⁷ More details on this paradigm shift under section 3.2.1 about the implementation of algorithmic enforcement called for by the DSM directive

prevent it (Angelopoulos, 2014) as evidenced also by Recital 59 of the Copyright Directive (Directive 2001/29/EC) which states that “In many cases such intermediaries are best placed to bring such infringing activities to an end”. They are both regulators and subjects of regulation, performing such processes using their employees or implementing relevant software solutions.

Leveraging ISPs’ unique position to identify and prevent unlawful activity does not only alleviate the cost and complexity rightholders would face in discovering and targeting primary wrongdoers; at the same time it makes them a potential normative force. They can influence a large number of users that are using their services, an audience difficult to reach individually by any authority, and strategically achieve a normative effect that can spread throughout their communities. However, the need not to overburden OCSSPs is expressly stated in the DSM directive under Art. 17, which also states the prohibition of member states to impose a general monitoring obligation.

2.1.2.3 Limits and exemptions from intermediary liability – Safe harbors

Starting with the eCommerce Directive (2000/31/EC), the EU orders certain limitations and exemptions from secondary liability for Internet intermediaries. Broadly speaking, intermediaries that provide mere conduit, caching and hosting services were exempted from secondary liability as long as they are demonstrably unaware of hosting illegal content. They are also obliged to terminate or prevent illegal activities if ordered by the competent authorities.⁸ The DSM directive recognizes the evolution of ISPs’ services and adds a tripartite obligation that established platforms have to adhere to in order to enjoy this exemption in the context of copyright infringement.⁹

This constitutes a divergence from the safe harbor dogma that has been in place for over twenty years by the DMCA in the US and the eCommerce directive in Europe.

While the letter of the law provides a framework that no one would oppose, it bears reminding that it is also inevitably reductive. Modern online service providers rarely fall neatly within these regulatory “boxes”. Intermediaries today are multi-faceted operations that integrate a variety of functions and services, and often are highly profitable multinational corporations having sophisticated tools and great power in the disposal. Usually both them and their users are one step ahead of the lawmaking process.

It is important to understand why these safe harbor exceptions were placed in the first place. Arguments about the role of immunity in helping digital and technological growth seem less convincing today than in the early days of the internet as a widely available commodity. The situation has changed vastly

⁸ eCommerce Directive (2000/31/EC),

⁹ Art. 7 DSM Directive (Directive EU 2019/790)

in the past two decades (Mann & Belzley, 2005). The internet is not on the verge of ascension, but rather a mainstay in all aspects of our professional and personal lives. This view is also supported by Sartor (2017) who notes, however, that the financial sustainability of smaller or non-profit and no-advertising intermediaries still has to be taken into account. The view supported with the DMCA in the U.S. – highlighted in the *Viacom v. YouTube* case - that even if an ISP has a general awareness of copyright infringing activity¹⁰ they are still immune to liability via the safe harbor rules is outdated in today's environment. (Samuelson, 2020)

2.1.2.4 OCSSPs and human rights

Another element that complicates the picture is that online service providers play a crucial role in enabling individuals and companies to exercise their freedom of expression. At the same time, they have to guard themselves against illegal activities performed using their services and the subsequent penalties they might face.

There is a chain relationship, that online service providers have to adhere to the law, but at the same time they have to provide a regulatory and technical framework for their users to act within legal limitations, and implement ways to check and remove any infringing material or behavior. However, intermediaries are not policymakers and their attempt to compromise these conflicting obligations often leads to extreme solutions – either that of too much leeway for illegal activity or an environment so strict that it becomes restrictive for free speech.

Evidently, in their role as regulators, intermediaries have to take into account that restrictions need to be proportionate to the desired result and neutral to the expressed opinion. Policymakers as well must proceed with the utmost care as censorship or limiting the freedom of expression of any kind is a state or interstate affair not a commercial process. Thus, there is danger in letting OCSSPs freely choose their policies and tools to combat copyright infringement, as matters of proportionality arise. Issues of accountability arise when private institutions become de facto policymakers. (Perel (Filmar) & Elkin-Koren, 2016)

2.2 Basic Legislation

The fundamental premise of the present study is the legal framework arising from the recent legislative progress regarding Copyright and the Digital Single Market in the European Union. Broadly speaking, I will try to examine the subject of preventive ways of restricting the access to copyright infringing content by online intermediaries in light of the European legislation and the resulting balancing of rights, taking into account the inevitable global scope of

¹⁰ *Viacom Int'l, Inc. v. YouTube, Inc.* - 676 F.3d 19 (2d Cir. 2012)

the matter. The main reference texts are going to be European legislation and CJEU rulings.

Ancillary to those, and depending on the issue at hand, I have used the legislative and judicial application of the EU member states (taking into account that such applications so far helped shape the text of the latest directive), as well as the situation in the US, where a lot of key players are based.

2.2.1 EU Legal Framework

The main text illuminating the analysis of the present study is 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 (henceforth the “DSM Directive”) that came into force in 6 June 2019, aiming to bring the 2001 Information Society Directive up to speed with the latest developments. The DSM directive sought to amend Directives 96/9/EC (also known as database directive) and 2001/29/EC (Copyright directive). It also touches upon the E-commerce directive (Directive 2000/31/EC) and the IP enforcement directive (Directive 2004/48/EC). The EU parliament has set a target implementation date for the member-states to be within two years after the directive came into force. As such there is still an ongoing debate and the stakeholder dialogue prescribed in art. 17 paragraph 10, as no member state has - as of yet - incorporated the requirements of the directive in their national legal copyright systems. The directive leaves the specific application of several matters at the hands of national policymakers.

The subject matter of the directive had already produced a heated debate over several controversial issues, spurring a conversation between corporations, policymakers and the public even before the finalization of its text, reflected in several open letters from artist’s organizations, academics¹¹ and various stakeholders to the European Parliament, namely from the Association of European Research Libraries (LIBER)¹², the European Composer and Songwriter Alliance¹³, the Association for Progressive Communication¹⁴, and intellectual property research centers¹⁵ among others, either for, or, more frequently against the initially proposed text. Especially in the latter case, the general public was mobilized to take part and be vocal in the discussion at an

¹¹ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3054967

¹² <https://libereurope.eu/blog/2019/01/29/copyright-reform-liber-signs-open-letter-calling-for-deletion-of-articles-11-and-13/>

¹³ <https://composeralliance.org/ecsa-open-letter-in-support-of-the-copyright-directive-2/>

¹⁴ <https://www.apc.org/en/pubs/open-letter-european-commission-article-17-eu-directive-copyright-digital-single-market>

¹⁵ https://www.create.ac.uk/blog/2018/04/26/eu_copyright_directive_is_failing/

almost unprecedented level. The online petition against (then) article 13 has been signed by more than 5 million people.¹⁶

The debate mainly centered around two provisions; article 11 of the original draft, commonly referred to as the “link tax” provision which is the article 15 of the final text and more significantly for the present study article 13 (Article 17 in the final text) which lays down the use of copyright protected content by online content-sharing service providers.

The Commission’s objective was to promote licensing of EU copyrighted works by large ISPs that dominate the market and profit disproportionately from hosting user generated content and reduce infringements by users by encouraging the use of automated content recognition tools. (Bridy, *The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform*, 2019)

Publishers and media groups have mostly been in favor of the directive, while online platforms, tech companies and the average user stood in the opposite side of the argument. By the nature of the subject matter touching upon fundamental human rights such as freedom of expression and privacy, human rights organizations have also been active pushing against the aforementioned articles. The voices against the directive also state that that OCSSP liability in these cases comes in conflict with the prohibition of general monitoring, as it would necessitate the use of automatic upload filters to take care of such a magnitude of content.

In the past, an ISP had no duty to monitor their sites for infringing material, even if they had general knowledge of users uploading copyrighted content there (Samuelson, 2020). The DSM directive’s stricter rules are a response to the changing situation, given the enormous volume of copyrighted works available in online service providers’ sites. Based on the infamous “value gap” theory which spotlights that a few Big Tech companies enjoy large profits by exploiting “safe harbor” rules, the directive now imposes strict liability on online content-sharing sites for user infringements and obliges them to use “best efforts to ensure the unavailability of specific works.”¹⁷ By creating an obvious liability risk for online content sharing platforms, the DSM directive sought to push such platforms towards seeking licensing (Samuelson, 2020) for the material that they knowingly or unknowingly host. This turned OCSSPs to filtering technologies, as will be further inspected in the main discussion. However, as Frosio (2017) incisively points this situation “de facto imposes a general monitoring obligation, as in order to filter unwanted content, all content must be monitored”.

¹⁶ <https://www.change.org/p/european-parliament-stop-the-censorship-machinery-save-the-internet>

¹⁷DSM Directive, Art. 17.

2.2.1.1 The contentious art. 17 of the DSM directive

Article 17 of the directive¹⁸ has been at the epicenter of criticism and plays a major role in the development of the copyright landscape for online content-sharing service providers. Its title reads: “Use of protected content by online content-sharing service providers” and it introduces direct liability for an OCSSP when it “gives the public access to copyright-protected works or other protected subject matter uploaded by its users.”¹⁹ In the same paragraph the directive promotes the obtainment of licensing agreements for communicating such works to the public. It also diverges in paragraph 3 from the hosting liability exceptions of the Directive 2000/31/EC²⁰, based on which services that host user generated content were not liable provided they had no knowledge of the illegal activity or acted expeditiously to remove any illegal content.

The DSM directive outlines the criteria for service providers’ exemption from liability. Service providers must demonstrably 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).²¹

The practical meaning of “high industry standards of professional diligence” and “best efforts” remains to be clarified. It is important, however, to note the inclusion of a “staydown” part in point (c) as well as the obligation of the rightholder to provide a substantiated notice, to avoid erroneous or automated notices with minimal degree of plausibility.

In articles 5 and 6, the DSM directive outlines the proportionality elements and limitations of service provider obligations based on their time in the market or size.

While until now it seems that Ar. 17 places a heavy burden on service providers and threatens the public’s access to information and creativity, it does address these issues in paragraph 7 which expressly states the constant

¹⁸ Article 13 in the fierce debates before the finalization of the directive’s text

¹⁹ DSM Directive, Art. 17 (1)

²⁰ Directive 2000/31/EC, Art. 14(1)

²¹ DSM Directive Art, 17(4)

availability of non-infringing material as a policy objective and prohibits the blocking of content that falls under the exceptions for criticism, review, parody, pastiche etc. This reflection on limitations and exceptions is to be understood as “a significant theoretical strengthening of user rights.” (Schwemer, 2020)

The highly debatable paragraph 8 says that the application of the Article shall not lead to any general monitoring obligation, a mandate that has been a matter of contention about its feasibility and whether or not it is contradictory in letter and spirit with the rest of the article.

In paragraph 9, the directive calls for the member states to ensure “effective and expeditious complaint and redress mechanisms available to users of the services” and specifies some conditions, failing or leaving it up to the members states to address the issue of the pace and the fleeting financial value of a lot of the material published. It also fails to recognize the issue of erroneous notifications and require sanctions. It is a crucial element in the balancing of users’ freedom of expression. Finally, in the last paragraph, it calls for a stakeholder dialogue to clarify and optimize the application and the practices of article 17.

The DSM directive and especially Article 17 will serve as the lens through which I will try to unfold the options for OCSSPs to design a fair and viable holistic content administration strategy.

2.2.2 The U.S. regime and the DMCA

The main relevant legal text in the US is the Digital Millennium Copyright Act (DMCA) that came into force in 1998 and, among others things, introduced the so-called safe harbor rules²² – later adopted by the EU and other countries. (Samuelson, 2020) Those rules exempt Internet intermediaries from copyright infringement liability provided they follow certain conditions, principally that they do not have knowledge of the fact that the user has published copyright infringing material on their platform and that when they do, either after a relevant notification from the rightholder or not, they proceed to expeditiously remove or block access to the relevant material. (Trapman, 2016).

Samuelson (2020) has studied the longtime convergence of the US and EU copyright systems, despite their main difference of principle – the US system’s primary principle is according to her the protection of the interests of the public, whereas the EU system construes exclusive rights broadly and principally protects the interests of the authors. It was only recently, using the “value gap” theory that EU diverged in practical terms, by pushing for stricter ISP liability rules.

It is up to debate whether the DSM directive and especially the commands of article 17 foster the creation of a digital single market as the

²² Online Copyright Infringement Liability Limitation Act (OCILLA)

Commission hopes, or rather widens the gap between the U.S. and the EU, the major forces in media creation and consumption. (Samuelson, 2020)

2.2.3 Relevant Case Law

Given the fluidity of copyright landscape and the technological developments that constantly change the scenery, courts and especially the CJEU are frequently called upon to specify the practical implementation of the directives' orders, clarify terms as well as solve theoretical inconsistencies.

An important case before the CJEU was *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH* which stated that

“an Internet service provider that allows users to access copyrighted material on its website is considered an intermediary under the Directive and that no contractual relationship between the intermediary and those whose copyright the intermediary is violating need exist”²³

And particularized matters of blocking injunctions, namely that

“an injunction in this case would not infringe upon the fundamental right to conduct business because the injunction in the case at bar would allow UPC to decide upon the measure to put in place to protect against this type of copyright infringement. The injunction would also allow UPC to avoid liability by showing that it has taken all the necessary precautions [...] the issuance of an injunction would not infringe on the rights to intellectual property, because this right is not absolutely protected and must be balanced against the public interest”

taking into account the Charter of Fundamental Rights of the European Union.

Significant on the matter of the compatibility of content filtering with the prohibition of general monitoring is the *SABAM vs Netlog NV* case before the CJEU²⁴. The decision underlines the relative nature of intellectual property rights and states that “Imposing a filtering system that would require the monitoring of all information for an indefinite period of time and to prevent future infringements would contradict the right to conduct a business, since such monitoring would be complicated and prohibitively expensive”. (Columbia University, 2012)

In terms of what constitutes a communication to the public by an ISP we refer to the 2017 *Stichting Brein v Ziggo* case.²⁵

Instructive for the reinforced position of copyright exceptions and limitations as users' rights is 2019 *Spiegel Online GmbH v Volker Beck* before

²³ C-314/12 - *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*

²⁴Case C-360/10 [2012]

²⁵ Case C-610/15

the CJEU²⁶ while *Productores de Música de España (Promusicae) v Telefónica de España SAU*²⁷ refers to the balancing of copyright and data protection as does *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*.²⁸

Also instructive was Poland's challenge before the CJEU²⁹ against the ar.17 of the DSM directive. Poland argued that the phrasing of article 17 implies an imposition of upload filters by OCSSPs that violates free speech and the freedom of information found in the Article 11 the European Charter of Fundamental Rights.

Another important input in the discussion is produced by the *Lenz* judgement³⁰, this time in the matter of the notice and takedown system and the balancing of power between platforms and users. It sets a standard to establish the validity of notices – an important aspect given the failings of the complaint and redress mechanisms at the moment – and requires rightholders to consider “fair use” and thus to form what might be called a procedurally ‘informed’ subjective good faith belief on fair use before sending a takedown notification. It is an important opinion towards the development of a fair and effective system that uses both automated tools and the human input in marginal cases that are frequent in copyright enforcement. (Leistner, 2020)

2.3 Literature Review and Contribution

The notion that the current copyright practice and mechanisms are not always well suited to serve the multitude of ways a work can be viewed, accessed or disseminated is not novel. Dornis (2018) has recently examined the ways uniformity in conventional copyright leads both to over- and under-protection in certain circumstance.

A lot of researchers and practitioners worldwide have been dealing with the issue of copyright enforcement for ISPs recently. Regardless of their point of start, that being a critique on the DSM directive, the debate before it, comparative approaches between the U.S. and EU systems, the rights of the users or the rightholders or a financially viable from a market point of view, usually the discussion converges over the same issues. The impact (Abecassis & Gann, 2018) (Commission, 2016) (Samuelson, 2020), effectiveness (Frosio & Mendis, 2020) and limitations (Castets-Renard, 2020) (Engstrom & Feamster, 2017) of content filtering, the relevance of safe harbor provisions (Agrapidis, 2017), the threat towards human rights (Gray, 2017) (Kuczerawy,

²⁶ Case C-516/17

²⁷ Case C-275/06

²⁸ Case C-70/10.

²⁹ Case C-401/19

³⁰ *Lenz v. Universal Music Corp.*, 801 F.3d 1126 (9th Cir. 2015)

2019) and the need for a harmonized market are points that have been studied extensively in the past few years. For that reason, I attempt to draw arguments from different scopes and try to combine fragments to a commercially viable and human rights sensible solutions.

Matthias Leistner offers a more levelheaded view in light of the debate around the DSM directive, focusing on the potential of algorithmic enforcement and stating that the article does not necessarily mandate a general monitoring obligation, but instead calls for an effective and proportional dynamic combination of algorithmic tools and human intervention. (Leistner, 2020)

In 2018 João Pedro Quintais published an important study titled “Global Online Piracy Study Legal Background Report”. In it, he identifies examples of enforcement measures that aiming to end or prevent infringement by third party users of their services. Such measures include but are not limited to (Quintais, 2018):

Elkin-Koren’s research is especially relevant regarding the transparency and accountability of OCSSPs use of algorithmic enforcement, especially the 2016 study with Perel (Filmar) titled: Accountability in Algorithmic Copyright Enforcement.

Overenforcement is widely studies and documented in databases such as the Lumen database and Stanford Law School’s center for Internet and Society for which D. Keller maintains a solid list of important studies over time.

The Oxford Handbook of Online Intermediary liability contains a treasure trove of academic discourse and research on the subject, gathering the work of seminal scholars including but not limited to Angelopoulos, Bridy, Erickson, Frosio, Kretschmer, Rosati, and Senftleben, and has been widely used for the ideas of the present study.

This is the passionate and comprehensive academic research on which I hope to contribute with the present study.

CHAPTER 3

3. Main Discussion

3.1 Current situation with OCSSPs

As evident by the discussion above, the DSM directive has forced Online Content-Sharing Service Providers to implement feasible measures of managing the content posted by their users that respect the balancing of copyright and fundamental rights, do not resort into general monitoring that borders on censorship, while avoiding being liable under art. 17 and remaining competitive in a ruthless market. It is a hard balance to achieve.

Additionally, it has to be noted that targeting users individually can generate bad publicity and political response, while also being costly. (Danaher, Hersh, Smith, & Telang, 2019)

Mitigating the risk of dissemination and exposure to illegal material by taking proactive measures in turn increases the risk of fundamental rights violations. (Castets-Renard, 2020)

A strict monitoring of user generated content using algorithmic solutions is shown to lead to high levels of blocking or demonetization of non-infringing content, or content that is covered by fair-use exceptions. This has to be weighed against the ineffectiveness of the users' available methods of response. According to Urban, Karaganis and Schofield's research (2017), the counter notification rates in the U.S. are consistently low and an imbalance of incentives even under the EU rules puts users at a disadvantage. This is notably true in instances of content with a "very dynamic attention curve" for which the appeal to the complaint and redress mechanism would come too late to matter. (Leistner, 2020) This dynamic attention curve refers to material that is intensely attractive for a short period of time (i.e. live events, commentary on recent news, new releases of audiovisual media) and for which the attention drops precipitously as time goes by, making the current cumbersome complaint and redress mechanism an ineffective option to rectify false decisions.

To elaborate on the incentive imbalance mentioned above, for an online content service provider, an unwarranted takedown would not pose a significant risk for damage claims. At the same time, failure to comply with a copyright infringement notification results in direct liability and damages claims. (Leistner, 2020). Given these facts, the most sensible way for an OCSSP to function is to allow the risk of overenforcement, as the main obligation after an erroneous decision to remove content would be to reinstate the content without further consequences except in extreme cases. (Leistner, 2020)

By adopting a cautious approach and not safeguarding user rights enough, ISPs have evolved into "politically unaccountable technology oligarchs

who exercise state-like censorship powers.” (Langvardt, 2017) This is a situation that the dialogue over the DSM directive is hoping to improve.

3.1.2 Copyright infringement

There is no question that large scale copyright infringement happens over the internet, especially using peer-to-peer networks or user generated content platforms and social media. Copyright owners assert that almost one quarter of global internet traffic,³¹ 80 per cent of YouTube videos,³² and 97 per cent of BitTorrent transmissions infringe their copyrights. (Riordan, 2013).

Despite the fact that no one argues that copyright infringement does happen in a large scale online, it is harder to prove that it really represents the loss of income rightholders claim. A download doesn't necessarily mean a view of the content, much less can it be equated with a lost sale that would otherwise bring revenue to the copyright owner. This way of thinking presupposes a zero-sum logic and it allows copyright holders to inflate their loss in its simplicity. (Riordan, 2013) Hard as it is to prove such claims, it is equally problematic to prove otherwise, as it is problematic to collect hard evidence for supposed behavior. Empirical evidence is inconclusive on the matter of the amount of loss suffered by copyright infringing activities, especially if the discussion focuses on parts of it being used in part of user generated content and not outright copies. A study about the income streams of music artists in different stages of their career (Garcia, 2020) uncovers that copyright is mostly important in the very early stages or when an artist is well into their stardom. For mid-level, mid-career artists, that form the most populated subset, copyright is a secondary income stream and it can be argued that the bigger exposure resulting from the – sometimes illegal – dissemination of their music can actually aid their main touring and merchandising earnings. This is not to diminish the importance of copyright, but rather to illustrate that the arguments of producing labels or large firms representing rightholders should not be taken at face value.

As mentioned above, the DSM directive pushes for widespread licensing. Even in this case, however, there is still an issue for small-scale creators or creators that make transformative uses of content. With the prevalence of algorithmic detection and monetization of content (as for example in the case of YouTube), monetization profit still goes to large conglomerates, as automatic detection and decision making cannot read through content and context as will be further examined below. Individual authors or small-scale rightholders remain at a disadvantage. (Leistner, 2020) From the platforms'

³¹ David Price, 'Technical Report: An Estimate of Infringing Use of the Internet – Summary' (January 2011) EnvisionalLtd <http://documents.envisional.com/docs/Envisional-Internet_Usage_Report-Summary.pdf>

³² Viacom International Inc v YouTube Inc, Plaintiffs' Memorandum, 8 (Case No 1:07-cv-02103, SDNY, 2012).

perspective, it is almost impossible to seek licenses, especially in a suitable format for the content to be detected, by private authors.

3.2 Solutions for the detection and blocking of copyrighted content

Regardless of the issues algorithmic enforcement/automated content detection software poses, at the same time they are being used by the largest OCSSPs today and their usage appears inevitable given the volume of judgements that has to be undertaken by each individual provider. Inevitability is not the only reason the discussion herein (and the business and academic discussion in general) centers around algorithmic enforcement. Its potential, especially taking into account the evolution of machine learning, is the one solution that if pushed in the right direction can catch up to the ever-increasing volume and complexity of content moderation and copyright enforcement. That one-way road is not only recognized by the market, but also by the discussion around the DSM directive³³. Software such as ContentID and Audible Magic is already used by the most important service providers.

Algorithmic enforcement is the only one measure that can provide a foundation for a comprehensive copyright strategy. Specific ways of removing content and their application depending on the circumstance are mostly case specific measures and their level of effectiveness comes one step later in the process. Blocking injunctions, the notice and takedown systems, de-indexing and more, are proven tools in a copyright enforcement toolbox, far from obsolete, and will be analyzed, they do not offer however the potential of a holistic solution that is represented by algorithmic solutions, aligned with fundamental rights interests and fair use exceptions.

As Mostert and Lambert (2019) argue in their study of IP measures in the digital environment:

“Filtering and monitoring for illegal copyright content especially by Big Tech players such as YouTube, Facebook and Instagram have become almost standard. Such filtering and monitoring by tracing and matching digital fingerprinting of unique identifying hashes of digital copyright files have in effect become the new norm in the industry.” (pg. 14)

3.2.1 Algorithmic enforcement as the foundation of detection and moderation of content

Content filtering is a controversial solution that has drawn the ire of the online community that claims such a solution is going to significantly alter the nature of the internet, the circulation of information and have a chilling effect on

³³ Recital 66

creativity. The solution of filtering is attractive for legislators as well as some intermediaries (especially the Big Tech companies who enjoy a competitive advantage by their mandatory use) (Spoerri, 2019) because it is a proactive measure against the dissemination of illegal content and therefore can simplify matters of liability for potential infringement. If a monitoring mechanism can catch illegal content before it is published then the service provider doesn't have to deal with the thorny issue of identifying the infringement and following the relevant legal procedures. The point remains that algorithmic copyright enforcement is a desirable tool in terms of scale, even if it is not always sensitive to the nuances of the law.

The most famous example of a filtering mechanism already in place is Google's ContentID system, which has been implemented since 2007 on some capacity on YouTube. It has been a development of heavy investment over the years drawing mixed reactions (Manara, 2018). Summed up, it offers copyright holders control and monetization options over copyrighted content uploaded on YouTube. (Gray, 2017). Researchers have argued that despite its ostensible goal to promote creativity, ContentID has the opposite result and gives copyright holders the opportunity to disproportionately benefit out of other creators' work – an issue already mentioned above. (Boroughf, 2015) The way content ID works is instructive of the way most filtering solutions are implemented and offers insight on the advantages and drawbacks of algorithmic enforcement.

Content ID works by “comparing uploaded YouTube videos against reference files provided by content owners.” (Gallo, 2011). When Content ID finds a match, it implements a policy, which consists of “if-then” statements that determine whether to implement one of three pre-defined policies: track, monetize, or block.³⁴ ContentID is not entirely automatic, and YouTube does offer a dispute and appeal process. It has been argued that content ID actually increases transaction costs. (Boroughf, 2015)

One of the main technological reasons in favor of such solutions is the rapid progress in machine learning. The hope is that the larger the scale and the longer the time period such filters are used, the more accurate their results will become, especially if it comes in the form of supervised learning, in order to help with marginal cases. The simple recognition of a copyright protected content by quantitative similarity is already feasible on a high level. The issues will be examined below in section 3.3.

The question is how extensive such monitoring solutions can be. European legislation explicitly orders that states must not implement the directive in such a way that a general monitoring obligation will be imposed for OCSSPs. Such obligation would obliterate competition as it would be very hard

³⁴ <https://support.google.com/youtube/answer/2797370?hl=en>

for all but the richest and already well-established companies to afford – especially considering YouTube/Google has an already sophisticated proprietary software with an extensive database that puts them in a dominant market position.

On the other hand, there is a comment to be made about reversing the paradigm. While copyright rules seek to eliminate copyright infringing content, upload filters treat everything as potentially infringing material and check their similarity ex-ante, not taking into account possible exceptions. The paradigm shift from “everything is allowed, except what is forbidden by the law” to “everything is forbidden, except what is allowed by the algorithm” is extremely problematic as it reverses the burden of proof. It reduces decades of nuanced discussion, conflicts and amendment regarding permitted and forbidden uses to a simple binary judgement by an automated, self-evolving system. Moreover, the constant pleas for transparency³⁵ are silenced behind business secrets and an opaque automated system dictates the legality of creative output – not to mention impacting users’ access to information

This is a step too far on giving service providers a normative role. It cancels decades of nuanced discussion of permitted uses, exceptions and carving out a sensible copyright system especially in an age where content creation has been spread out to a large number of people. This development did not happen by discussion and weighing opposing opinions, but merely from the development of a technological solution to a very specific problem. The various issues that arise from this conundrum, such as overenforcement, mistakes etc. will be discussed further.

Two more major concerns arise from the extensive use of automated systems like content ID. The first is connected with the lack of the human element. Leaving the entire decision on an algorithm in a sense erases the process and evolution that has given birth the fair use exceptions, while at the same time transferring the initiative and power from courts and authorities to corporations. (Geddes, 2020) The other concern is sometimes labeled “technofeudalism” and is connected to the primary assumption that any dissemination of copyrighted content as part of user-generated content that includes it has to be compensated for, and this arising not from the users, who are not asked if they want their works to return profit for every use. (Geddes, 2020) This might seem like a counterfactual, but not all creation relies upon making profit.

Moreover, it presents a matter of principle. Google has been involved into making and enforcing a copyright rule by implementing large scale automated algorithmic enforcement. As Joanne Gray (2017) states, “Google

³⁵Explicitly stated for online content service providers and their copyright decision making in recital 68 of the DSM directive

has created an elaborate private copyright regulation which [...] raises serious questions of accountability and private power in global copyright governance”.

Filtering as a solution suffers from another major disadvantage. Most filtering solutions are commercial products, subject to the predictable competition and trade secrets. This presents a twofold issue. First, the goal of developing such technological solutions is not accuracy according to legal nuance, but minimizing costs and increasing efficiency, to provide the most commercially attractive solution. Secondly, even if legal accuracy was high among the developers’ priorities, the function cannot be very transparent. The specific way these solutions operate are walled off behind commercial secrecy and can be unpredictable. This conflict of interest and cloudiness highlights the social issues that arise with filtering as the main solution against copyright infringement. Regulation then becomes ultimately a process left not to policymakers or rightsholders but third parties creating solutions under uncertain – and difficult to measure – implementation.

3.2.1.1 ContentID

The most prevalent automated filtering system today is none other than ContentID, developed by YouTube/Google and is the ideal test case for algorithmic enforcement. YouTube itself has been rather transparent if unpredictable about its methods – relative to other market solutions at least - and deals with an enormous amount of user uploads. On the other hand, creators reliant on YouTube monetization scheme as well as rightholders who feel infringed have been vocal about ContentID and Youtube’s monetization methods either via posting their views on YouTube or on other media. Even before the process of filtering uploads with ContentID, YouTube issues public guidelines for uploaders on how to ensure the adhere to copyright rules and successfully pass the ContentID’s requirements.

Google has made an enormous investment on its proprietary content detection software, reportedly investing more than \$100 million in building, developing and staffing the solution until 2018 and has paid more than \$3 billion to rightholders who have monetized use of their content in other videos through Content ID. (Manara, 2018) However, it is a system that is mostly limited to corporate use, by being available to rightholders that fulfill certain criteria.³⁶

Its function is in short as follows: rightholders provide a list of samples (ID files) which are then compared with material uploaded by YouTube users and determines their similarity. Apart from a mere identity check, the algorithm is designed to be able to detect similar files and also measure the length of the similar sequences in a certain uploaded file. (Leistner, 2020) At the same time, “it operates on the presumption that rightholders have exclusive rights to a work

³⁶<https://support.google.com/youtube/answer/2797370?hl=en>

and so copying or sharing for any purpose requires their permission” (Gray, 2017).

With content ID, blocking access is but one of the possible courses of action, though most rightsholders choose the monetization of their content used in other videos.³⁷ This happens as follows, summarized by Leistner (2020):

“...what Content ID can essentially do is a mere quantified identity and similarity check. As for blocking or monetization purposes, protected subject matter will be identified and monetization will be typically assigned to the registering rightholder if 90% of an uploaded video are at least 90% similar with an existing ID file (so-called 90:90-rule). (pg.52)

It is obvious as such, that the issue with the current implementation of the system is its inability to provide a qualitative judgement, which is important when fair use or some other copyright exception might be applied to a specific upload.

Another issue highlighted by Leistner (2020) is that of the lack of representation of users/user organizations and small rightsholders at the negotiation of ContentID’s basic parameters. Those are decided between large, “institutional” rightholders and Google/YouTube. Thus, only one side of the complex relationship that is in play during the copyright enforcement process can have an influence and it is the side that benefits from a very strict enforcement in the first place. Predictably then, the results of algorithmic enforcement in this case are biased towards the rightholder rather than the end user or smaller creator, even in cases of permitted or transformative uses of copyrighted material. ContentID will direct monetization towards the registered rightholder, unable to understand the nuances of the copyright exception rules, and the creator will often not be compensated at all for his creative output, if their efforts are not blocked altogether.³⁸

DeLisa (2016) suggests that Google has effectively created a mandatory licensing system under which ContentID affirms copyright infringement prior to it actually happening. Furthermore, as Gray (2017) formulates it, irrespective of the precise legal form, Google has established a copyright enforcement regime in which “infringement is assumed, permission is mandatory and licenses are preemptive.” – the issue of the reversal of the burden of proof discussed above.

Despite its shortcomings though, ContentID remains the benchmark of algorithmic copyright enforcement for online service providers, a testament to the lack of actual high-level alternatives.

³⁷Id.

³⁸More on possible proactive or revenue-sharing solutions to this issue later.

3.2.1.2 Audible Magic

Audible Magic is the most popular automated content recognition tool outside of YouTube, currently used by the largest social media and entertainment enterprises in the world, such as Facebook, Twitch, Universal Studios and Disney to name a few. As the company describes itself in its website, Audible Magic functions as a “trusted intermediary between rightholders (including labels, studios, distributors, publishers and collectives) and social media platforms (including Facebook, Soundcloud, Dailymotion and Twitch)”.³⁹ Despite being available for anyone, its pricing actually makes it an option for large companies only (Spoerri, 2019). In a nutshell, the software is using fingerprinting technology to “match audio and video content uploaded by users against a database of fingerprints submitted by content owners.” (Abecassis & Gann, 2018)

Audible magic offers recognition of audio and video content posted on online content service providers websites and platforms and helps with the licensing, monetization and royalties payment deriving from user generated content. It also promises detection even in cases of changed content by infringers to evade filters.

Audible Magic also promotes itself as a solution for online platforms to respond to the Art. 17 mandates.⁴⁰ However, it is matter of debate if its cost and position as one of the few if not the only available solutions won't perpetuate the dominance of Big Tech companies. (Spoerri, 2019)

However, Audible Magic suffers from similar contextual limitations as the ones discussed above for ContentID. Furthermore, especially in the case of music, it has reportedly been inconsistent in cases of mashups, remixes and other forms of edited copyrighted material. (Agrapidis, 2017)

3.2.1.3 Other Automated Content Detection Systems

For the sake of completeness some more options will be mentioned, noting that limited solutions already exist in the market. (Abecassis & Gann, 2018)

First of all, some OCSSPs opt to follow Google's example and create their proprietary software to detect infringing content and monitor what is uploaded on them. For example, the EU-based online audio distribution and music sharing platform Soundcloud, while also using Audible Magic, has at the same time invested more than €5 million and a part of its personnel to the development and maintenance of their own proprietary software. (Engstrom & Feamster, 2017)

³⁹ <https://www.audiblemagic.com/>

⁴⁰ <https://www.audiblemagic.com/article-17/>

Signature is another video detection software that uses fingerprinting technology, offering the option to block or monetize content, which has been developed by the Institut National de l' Audiovisuel (INA).

Gracenote is another content recognition tool using fingerprinting technology that is used for audio files, while LTU tech is a company that provides image recognition technologies which, however, only offers content recognition rather than tools to manage the content, it is consequently not suitable to cover the mandates of the DSM directive. (Abecassis & Gann, 2018)

Vobile offers content recognition technology to rightholders, creators and platforms alike. They focus on the protection and monetization of intellectual property online, going one step further to provide marketing services as well. It is the main software that is placed at the intersection of all the parties involved. Their solution is also based on a fingerprinting technology to detect both audio and video files. Additionally, *Vobile* advertises the automatic submission of takedown notices while tracking compliance and keeping archives of its activity.⁴¹

Other automatic content recognition systems such as *ArcSoft* for images and video or *Mufin* for audio identification are not used for decision-making purposes and are positioned in the entertainment market as software towards users. The fact that most companies that develop this type of automatic systems don't position themselves in the copyright enforcement market speaks both of the high barrier of entry posed by the dominant positions of Google and Audible Magic, but also of the difficulty of and impact of flaws in accuracy.

3.2.2 Case Specific Measures

As mentioned above, while algorithmic enforcement is both becoming the industry standard and also represents the future of copyright enforcement, it is especially useful in the detection stage and there are still measures and injunctions for specific files, websites or users, that are and will continue to be used in conjunction with algorithmic solutions.

3.2.2.1 Notice and takedown

"Notice and takedown" is an administrative and technical procedure, first developed as part of the DMCA in the US, that requires intermediaries to remove infringing content online, upon notice by copyright holders. It remains the quintessential method of dealing with copyright infringement online. (Mostert & Lambert, 2019) It is part of the safe harbor rules for regulating an online service provider's liability, that provide immunity if the provider acts expeditiously to remove illegal content, provided they receive information 'reasonably sufficient [...] to locate the material' from an authorized notifying agent. (Erickson & Kretschmer, 2020). The system was similarly adopted by

⁴¹ Data from vobilegroup.com

the EU Directive on Electronic Commerce (2000/31/EC) and quickly became the global standard.

Its success in copyright enforcement lies in its simplicity, and it mostly worked fine until the enormous scale of content made it impractical to deal with in a case by case basis – and especially for small rightholders, it was too cumbersome to actively seek out material that violated their copyright.

“Notice and takedown’s” issues will be briefly mentioned here, before being further examined in the next section. The prevalent issue is the exponential growth in uploaded content and subsequently the rise in costs and complexity for OCSSPs to comply. (Strzelecki, 2018) The second issue is that of the accuracy of the notices, a discussion informed by the biased incentive structure discussed above, issue that is amplified by the increase in volume. (Erickson & Kretschmer, 2020). The Lumen database⁴² is an invaluable resource to the investigation of these first two issues. Also mentioned in Urban, Karaganis, & Schofield’s (2017) study among others is that more than half of the takedown notices are generated by a single entity. Inexpensive requests with minimal prerequisites that can be sent out in bulk will inevitably be sent that way, in the expense of precision. (Seng, 2015)

Even in the case of implementing automated content recognition systems, the notice and takedown system remains central in copyright enforcement, and works in synergy with those systems. The model mostly works and it rather needs improvements than a complete overhaul. (Erickson & Kretschmer, 2020) This view is also acknowledged by the European Court of Human Rights in the *Delfi vs Estonia* case⁴³.

Urban, Karaganis and Schofield (2017) conducted primary research with OCSSPs and rightholders, discovering that they view the notice and takedown system as a foundational element in dealing with copyright infringement, regardless of the specific way each one implements it, concluding that it is “woven into the fabric” of their operation.

Conversely, notice and staydown systems that go a step further and employ filtering technologies for all communications (Romero Moreno, 2019), such as the regime effectively proposed by the DSM directive, have been found to violate EU law by the CJEU (*SABAM vs Netlog*), failing to strike a balance between the competing rights.

⁴² The Lumen database “collects and analyzes legal complaints and requests for removal of online materials” as self-described

⁴³*Delfi v Estonia* App n. 64569/09 (ECtHR, June 16th 2015)

3.2.2.2 Blocking Injunctions

Blocking orders are injunctions to “restrain an Internet service provider (ISP) or other intermediary from allowing its services to be used to infringe copyright.” (Mostert & Lambert, 2019)

As discussed above, online service providers, especially platforms hosting user-generated content are now faced with primary liability for the actions of their users, and the immunity they once enjoyed (or still enjoy outside the EU) is harder to achieve. However, they do not necessarily have to be found liable to be asked to restrict access to content. Often that restriction takes the form of blocking injunctions; simply put blocking the access of the public to the infringing material.

A major disadvantage of the different forms of blocking access to infringing content is that the subject material remains online and further infringement is not altogether avoided. Compared to the outright removal of the subject infringing material, all blocking access solutions can, and probably will, be circumvented in time, especially by commercial level infringers. Using mirror sites is a common practice to re-enable access to copyright infringing material that has been blocked. This elicits questions about the measure’s efficacy and subsequently its proportionality. Proportionality is examined in respect not only regarding the damage or hindrance to a user’s rights, but also regarding the chances of success of the action taken, as well as it’s efficacy.

At the same time, this exact characteristic is what makes blocking a viable solution in the rightsholders’ and intermediaries’ toolbox. Its temporary nature and easy reversal make it an only mildly intrusive measure that can easily be reversed in case it’s wrongly taken. Blocking can also be limited geographically and with regard to time, and can be imposed even in cases that the courts have no jurisdiction to order the removal of the content. Blocking can be utilized as an effective temporary measure until there is a final ruling regarding the disputed infringement. (Riordan, 2013)

The prevalence of blocking injunction in the EU can be traced back to the eCommerce Directive, that offered the option of blocking injunctions in cases that ISPs enjoyed immunity for monetary remedies. The increasing volume of copyright infringing activities exploiting this immunity dictated that blocking injunctions was a flexible and convenient copyright enforcement tool. (Angelopoulos, 2014)

In any case it is not the ultimate, last resort measure. Blocking can be used to minimize the spread or accessibility to the copyrighted material, which in some cases can be crucial – for example in time sensitive cases of content with a dynamic attention curve, such as live events. Making the access to such content inconvenient enough can push the user to seek a lawful channel to view the content in question.

Blocking can take the following forms:

1. IP Address blocking
2. DNS blocking
3. URL filtering
4. Deep packet inspection
5. Hybrid filtering models,

and can be granular in their implementation in terms of time and territoriality, which given the speed and the uncertainty around most cases is an asset. (Riordan, 2013)

Blocking illegal content is used in the context of the notice and takedown process that can order the blocking or removal of copyright-infringing content. One of the issues with such procedures the danger of overenforcement and the blocking of material that is not in fact infringing. According to a study undertaken by the University of California, Berkeley around 30% of requests of this category are made in error. (Urban, Karaganis, & Schofield, 2017)

3.2.2.3 Website Blocking

Website blocking is among the supply-side measures to combat access to illegal content. This form of blocking access involves ISPs blocking access to websites that “facilitate illegal consumption of content by not resolving domain requests to those sites.” (Danaher, Hersh, Smith, & Telang, 2019) It most commonly involves ISPs disabling access to certain websites which carry copyright infringing material. The latest development is dynamic blocking to combat the extensive use of mirror sites to circumvent injunctions. This measure is very frequent in the EU, as outlined in Article 8(3) of the InfoSoc directive.⁴⁴ (Mostert & Lambert, 2019)

While it has the advantages of flexible timing and territoriality, it is easily circumventable and not greatly effective at preventing the undesirable outcome. Users can find links on similar websites that have not been blocked. The blocked websites can easily be mirrored and accessed through alternative domains, rendering the measure ineffectual and finally, users can employ VPN servers to bypass the localized limitations. (Danaher, Hersh, Smith, & Telang, 2019)

However, there is an example of a large-scale blocking of access that shows - given the limitations of such studies due to variables – that decreased traffic to other pirate websites as enforcement is visible and chilling but an uptick in legal services as well. (Danaher, Hersh, Smith, & Telang, 2019)

The same researchers (2019) suggested that “the fixed cost involved with switching to a new piracy sites (which involves both search and learning

⁴⁴ Directive 2001/29/EC of the European Parliament

costs) could be higher and affect more individuals when more sites are blocked, thus some individuals might choose to substitute legal consumption for piracy.” When more sites are involved, the chilling effect on the interest for the pirated content is bigger. Larger scale movement sends a stronger signal, and when multiple outlets are blocked, users can expect action, rather than an individual site being inaccessible.

It has also to be noted that the website blocking case law is also an interesting case study from the perspective of the European harmonization. (Husovec & Van Dongen, 2017)

However, restricting access to a website in its entirety threatens to impede access to any legal content that is hosted at the same web address. (Angelopoulos, 2014), therefore coming into conflict with users’ fundamental rights and extending the injunction further than its desired aim. Such restrictions are expressly prohibited in art. 17 of the DSM directive, pointing to the fact that website blocking has to be implemented cautiously in the battle against piracy.

3.2.2.4 Removal

The outright removal of infringing material at the source is one of the most straightforward measures against copyright infringement, certainly more effective than blocking the access to particular websites or webpages. Often illegal material is stored at a central location (e.g. a cyberlocker) and accessed from multiple routes.

A famous example of effective removal of material at the source has been the shutdown of the “Megaupload” cyberlocker, which has been shown to decrease overall piracy numbers. Removal at the source is of course more effective than blocking access to particular websites. That particular example of effective removal at the source presented outsized benefits in overall piracy numbers as “many of the linking sites are negatively affected as well if they pointed to content on the host site.” (Danaher, Hersh, Smith, & Telang, 2019). However, shutting down entire sites is not a viable solution as they may have more than one use and not host exclusively infringing content. At the same time, it’s bound to create a backlash and be difficult to achieve from a legal perspective. Such websites and services are often off-shore companies using their base as a shield for illegal activity.

Even in cases when the removal is targeted to specific material rather than a whole website or its mirrors, it remains more intrusive than blocking injunctions. It removes the relevant material permanently and a high degree of evidence is needed to impact the fundamental freedoms in such a severe manner, namely the freedom of expression and the freedom to conduct business, protected by the European charter of human rights.

From an economy perspective, there is the issue that a side-effect of the strict removal of content draws even more attention to it as user’s seek what

was previously available, drawing higher levels of attention to it. While the same file or website might seize infringement, others quickly appear to offer the same content to a ripe audience in what has been described as the “whack-a-mole” problem.

Often the removal of a file or a website at the source will be a difficult option. If the infringing file is hosted at another location or website and fetched to or linked, then another service provider will have to be implicated in the enforcement, and potentially more users.

3.2.2.5 Search Engine Removal – De-indexing

De-indexing is another viable but complementary preventive measure combating the access to copyright infringing content; an important tool in the toolbox. Especially in cases where the infringing material is hosted at a safe haven (e.g. offshore) making it hard or impractical to remove at the source, de-indexing can limit the access to it. De-prioritizing content from search engine results is especially effective in cases of media with a steep attention curve. In these cases users have limited time to look for alternatives by browsing through pages upon pages of results or seeking alternatives in message boards. At the same time, it impedes the infringer from setting up and distributing the material through alternative channels.

As researched by Strzelecki (2018) search engines receive frequent requests to remove content from their search results for a violation of the law. Copyright owners are not an exception and are a main source of such requests according to the study. Those requests stem from courts, companies, non-government organizations and private entities. In the same vein, platforms that host user-generated content and social media have their own search functions and receive similar notices, manipulating the results either after an order or after assessing the validity of a claim. Most Big Tech companies employ copyright teams that are tasked with processing such requests. (Strzelecki, 2018)

Search engines (e.g. Google, Bing, etc.) cannot only remove a website or a webpage from their results; they have an array of ways to manipulate the presentation of those results to their users. They often use their algorithms to de-prioritize certain results, they can change their auto-filling mechanisms to not suggest often searched copyright infringing material and websites (Bridy, 2016) and can also remove pictures and graphics from search results.

Search engines and OCSSPs operate in a similar manner in this context. In short, a valid request to remove based on copyright laws will trigger the outright removal of a file or a URL from the search results, or its concealment further down the results. (Strzelecki, 2018)

Search engine removal and de-indexing are not as strict of a measure as the blocking of content or a website, nor as intrusive as is algorithmic enforcement. It can similarly be limited geographically or in terms of timing.

However, despite those characteristics that make it a milder measure against individual users or business, they raise questions regarding their impact on the structure of the internet and the delivery of information. Researchers and online commentators have voiced their concerns about their interference with network neutrality. Influencing how and when certain material or websites are presented in search engines in essence creates an environment where certain websites and subsequently information do not go through the usual cycle of the system in order to be presented, thus modifying the flow of information. Riordan argues that it might be better to outright remove or block infringing material rather than de-index and risk unsettling the system that tries to ensure users' freedom to share and consume information, and probably create unfair advantages in the competitive environment of web search services. (Riordan, 2013)

Even from a technical perspective, frequently manipulating and making exceptions in an algorithm can have adverse effects on its intended function, especially given the scale of copyright infringements.

De-prioritisation of certain results is a milder alternative to their outright removal. It does, however, suffer from the same drawbacks, maybe even worse so in terms of net neutrality, while being rather ineffective in cases users seek a certain piece of copyrighted material. (Riordan, 2013)

It is also notable that there exists a Voluntary Code of Practice where representatives of creative industries participate along with the largest search engines (e.g. Google, Bing) whose objective is to “determine the effectiveness of search engines' voluntary measures to fight online piracy and to encourage industry collaboration.” (Mostert & Lambert, 2019)

3.2.2.6 Bad Actor listings

Much of the copyright infringement online is driven by commercial level “pirates” who are numerous in volume and prolific in output. In most cases, those people or enterprises do not refrain after an injunction is issued against them but are repeat offenders, motivated by financial gain. As such, a “follow-the-money” approach is utilized to curtail their activity.

This approach takes the form of Bad Actor listings that identify and track illegal activity, composing “red lists”, “green lists” or “watch lists” of websites or individuals to “monitor and fight cash flows and traffic” to those places. Such lists are reported successes and are being circulated in a confidential manner among law enforcement and authorities to keep track of illegal activity. (Mostert & Lambert, 2019)

Commercial-level pirates do not only propagate their activity through their own website and platforms, but use OCSSPs infrastructure either to communicate infringing material or to direct traffic to their channels. The enormous volume of pirates in the cyberspace and their identification and tracking are central issues in copyright (and criminal) enforcement. Measures

like the above help monitor cash flows and traffic among the numerous channels they use. (Mostert & Lambert, 2019)

Examples of such listings is Denmark's "collaboration list" which during 2020, will become part of "an international database under the UN's World Intellectual Property Organization (WIPO), where authorities from each country upload and update the national lists in a joint database that will then represent a global, accumulated sum of illegal websites that can be used by authorized users in each country"⁴⁵ and Operation Creative's Infringing Website List (IWL) of the City of London Police Cyber Crimes Unit (PIPCU) whose aim is to disrupt and prevent websites from providing unauthorized access to copyrighted content. The aim of the IWL is that "advertisers, agencies and other intermediaries can voluntarily decide to cease the placement of advertising on illegal content websites by using the data contained in the IWL" (Mostert & Lambert, 2019) a practice that has proven disruptive to these websites business models.⁴⁶

3.2.2.7 Traffic Shaping – Data Caps - Disconnection

Traffic Shaping (also known as connection or packet shaping) is a widely used bandwidth management technique that entails prioritizing (and delaying) certain types of network packets. It is principally used by internet service providers to serve their different distinct traffic profiles, comply to contractual agreements or a legal order, ensure security, help in cases of network congestion or sometimes restrain resource usage from peer-to-peer services.

Traffic shaping is not reserved only as a defense measure for ISPs; it is rather a useful tool in their regular operation. It can also be a useful mechanism to curb unlawful activity. Limiting the resources allocated and thus the speed a user can access and save illegal content. Limiting a subscriber's speed of access will not solve the problem of infringement itself, but it can limit the extent of the infringement.

Data caps are limits imposed by ISPs to the amount of data a client can use – usually in a monthly basis ⁴⁷, curbing maximum speeds, charging extra fees or disconnecting the client after that limit is reached.

The main concern given in these cases arise with regard to network neutrality. Network neutrality is the principle dictating that Internet Service Providers (ISPs) must treat data running through their physical and digital infrastructure equally, regardless of their content, application, device or end-

⁴⁵From Denmark's Rights Alliance website, an organization that focus on combating piracy online - <https://rettighedsalliancen.com/collaborations-and-initiatives/>

⁴⁶ http://news.cityoflondon.police.uk/r/1184/pipcu_disrupts__719_million_worth_of_ip_crime

⁴⁷<https://www.publicknowledge.org/issues/data-caps/#:~:text=Internet%20data%20caps%20are%20monthly,and%20even%20disconnecting%20a%20subscriber>

user. Such data might be transmitted either between end-users, or between end-users and content providers or online services. This principle of non-discrimination – which is legally enforced in most developed countries and in the EU level – includes concepts like “best efforts” (dictating that ISPs make best efforts to transmit the data regardless of its type and origin) and “application-agnosticism” (where the data arises or heads to) and has long been considered a crucial factor for innovation.

By limiting the speed and consequently the facility of accessing certain websites or content internet-access service providers are impacting the competition among companies by effectively promoting some and hindering others.

The harshest preventive action is clearly the outright disconnection of a user or a business from the internet, with obvious effectiveness in curtailing copyright infringement. In this case, an internet access service provider is ordered to suspend internet access from a client for illegal activity. The process might start by an infringement on an online content sharing service platform, but usually needs a court order or a violation of the ISP’s terms to be imposed. However, in terms of copyright infringement, outright disconnection of a user will almost always be a disproportionate punishment. Internet access has arguably become a human right; an extension to the freedom of expression and opinion.⁴⁸ In this context disconnecting a user from the internet is akin to a form of digital incarceration, and it is hard to argue for such a measure given the relative nature of intellectual property rights. (Riordan, 2013)

Those measures can be imposed and be part of the OCSSPs toolbox only in collaboration with ISPs that provide internet connection as part of the battle against piracy, and always in cooperation with the authorities as they are not measures that target the material, but the users themselves. OCSSPs cannot impose these measures but are part of the copyright enforcement processes in the detection stage and should their attempts to curtail infringing activity fail they will be called upon to participate in the escalation of measures.

⁴⁸ <https://www.diplomacy.edu/blog/%E2%80%98un-declares-internet-access-human-right%E2%80%99-%E2%80%93-did-it-really>

3.3 Issues with the prevalent prevention measures

On a fundamental level and as defined by the DSM directive, preventing the access to or removing infringing material by OCSSPs must not result in an obligation to perform general monitoring or censorship of content posted on their platforms by their users. Treating everything as suspicious material and creating a bottleneck filter for content by creating an environment of indiscriminate monitoring environment comes into conflict with users' fundamental rights such as the freedom of expression or privacy, and severely impacts the fabric of the internet. Other severe measures, such as restricting or outright banning a user's access to the internet access impacts fundamental rights such as the subject's freedom of expression and are in most cases unacceptable.

Bearing in mind that intellectual property rights are by no means absolute (Merges, 2018) - a critical consideration when discussing matters of proportionality - the statement that EU member states shall not impose a general monitoring obligation is not merely the letter of the law, but has to be treated as a global general principle, instructive as policymakers and ISPs are trying to carve out a copyright strategy. At the same time, the solution should not stray too far in the opposite direction. This protection of fundamental rights should not devolve into a vulnerability exploited by commercial level infringers with the sole purpose to profit from distributing illegal copies of copyrighted works. Intellectual property enjoys protection as a fundamental right as well according to the EU charter.⁴⁹ What is protected is creators and individuals whose fundamental rights are at stake in this discussion.

Another set of issues that will be discussed in the following section arises from the power imbalances and the biased incentives created by the proposed evolution of copyright rules, spanning from the danger of overenforcement and risk aversion to the threat towards private authors and small rightholders.

3.3.1 General Monitoring

As mentioned above, the DSM directive explicitly declares that the obligations established therein should not lead to Member States imposing a general monitoring obligation.⁵⁰⁵¹ This prohibition had been already articulated by the CJEU in its SABAM v. Netlog NV decision⁵² which ruled that a general filtering technology mandate is incompatible with the E-Commerce Directive's no general monitoring rule (Samuelson, 2020), an evolution of which is the

⁴⁹EU Charter of Fundamental Rights, Art. 17(2)

⁵⁰Recital 66 directive (EU) 2019/790

⁵¹Article 17(8) directive (EU) 2019/790

⁵²Case C-360/10

clarification of Art. 17(8) that “the application of this Article shall not lead to any general monitoring obligation.”

It is hard to see how the threat of direct liability for OCSSPs combined with their extensive automatic content recognition systems will not create an environment that is practically equivalent of general monitoring.

However, as mentioned above, by creating an obvious liability risk for OCSSPs, the DSM directive sought to push such platforms towards seeking licensing (Samuelson, 2020) for the material that they knowingly or unknowingly host. Consequently, OCSSPs were forced to consider the implementation of automated content recognition technologies, as they were unable to cope with the sheer volume of content uploaded in their platforms. As Frosio (2017) comments, however, this “de facto imposes a general monitoring obligation, as in order to filter unwanted content, all content must be monitored”.

Monitoring technologies cannot take into account contextual factors and consequently decide not to provide a judgement on certain instances. A truly independent and automated system logically implies general monitoring, unless its user only implements it in a certain set of cases. However, the convenience of filtering is exactly the relief of that sorting burden.

3.3.2 Overenforcement

As already discussed, overenforcement poses a threat to fundamental rights and the core function of the internet as well as the erosion of copyright exceptions that protect users’ freedom of expression. The way things stand, senders of copyright notices that request the blocking or takedown of material have little external pressure to be accurate or pursue a systematic approach. (Urban, Karaganis, & Schofield, 2017) This is predictable. A request that is superfluous or sent in bad faith does not evoke serious adverse effects for the sender, and often there are no safeguards against such practices. Service providers tend to follow a safe approach. Consequently, if there is no cost in making general and superfluous notices, there is little reason for rightholders not to send bulk notices without care or consideration for content and context.

It would be beneficial for all sides if there was a universal blueprint on the correct reporting of infringing content, and sanctions for incomplete or bad faith requests. (Erickson & Kretschmer, 2020) This could take the form of a time limit until the next request to avoid notifiers that flood the system and repeat the same application, or stricter criteria for the request to be processed. Establishing a base level of mandatory information and verification, not only in word but in practice, across legislations and platforms is crucial in the making of a more sustainable electronic copyright ecosystem – one that improves over time as it integrates more data. This does not only benefit publishers, content creators, private authors and the public, but rightholders as well. Intermediaries will be able to commit to requests with more confidence and the compounding

of accurate data overtime will contribute to make any filtering mechanism more precise, and thus both combat overenforcement and appropriately monetize media consumption. All sides benefit from transparency and good faith.

The lack of such guarantees has infamously led YouTube's claiming system to be exploited as an extortion mechanism.⁵³ The case of the user "VengefulFlame"⁵⁴ is instructive of the dangers of giving too much leeway to (sometimes self-proclaimed) copyright holders. Google's support message boards are fraught with instances of YouTube creators being hit by fake copyright claims and extorted by scammers abusing the "three copyright strikes and you are out" system YouTube utilizes.

Google has itself acknowledged that Content ID may be used to unilaterally overstate or incorrectly declare ownership. (Gray, 2017)

There are various reasons why this overenforcement or overprotection of powerful rightsholders is happening, exploiting the "false positives" issues and the insufficient consideration of the exceptions.

First of all, copyright law is characterized by a high degree of fragmentation and uncertainty. While the EU Directive on Copyright in the Digital Single Market seeks to harmonize law and enforcement and alleviate some of that burden, it remains to be seen how it will actually be implemented by the member states.

The inevitability of automated enforcement dictates their implementation by OCSSPs. As discussed above, however, such systems are prone to overenforcement as they are not context-dependent and cannot get into an assessment of copyright exceptions. This lack of nuance and the quick adoption of such systems in order for the platforms to ensure compliance has already created an environment where overenforcement is the norm.

In the same vein, enforcement is presented with the issue of the same work containing copyright protected and non-protected elements. How does an OCSSP deal with this "partial" infringement. The way things stand today, whole works are being labelled as copyright infringing and taken down or demonetized for very small parts or legal uses of copyrighted material. The assessment of the contribution to the final work, the value added or adherence to a legal exception is absent by the current scheme. This

Another element of the overenforcement issues, is that algorithmic enforcement systems make decisions automatically, even in cases that are not relevant. (Castets-Renard, 2020)

⁵³<https://www.techdirt.com/articles/20190205/10064941534/youtubes-contentid-system-is-being-repurposed-blackmailers-due-to-failings.shtml>

⁵⁴ <https://www.tubefilter.com/2019/02/07/youtube-content-id-copyright-infringement-scam/>

3.3.3 Mistakes in copyright enforcement

The main issue with automated or algorithmic enforcement is the well discussed phenomenon of “false positives”. False positives are instances when content is considered as copyright infringing and labelled as such or removed erroneously. This can be attributed to various factors. The filtering system might disregard the fair use exceptions posited by the law or the length and importance of the copyrighted material in the new work. It might misidentify the publisher and block content from the original copyright holder. It might disregard the possibility of the publisher having the original copyright holder’s permission. It might mistake similarity with identity. (Gray, 2017)

Mistakes also happen in cases of human-sent notices. To improve the quality of such notices, platforms need to encourage senders to compile accurate, detailed notices in order to be processed. A solution is to ask senders to locate the infringing material, indicating search results, threads, comments, URLs, timestamps in audiovisual media and so on, while stating the reason for claiming infringement. This is already practiced by some OCSSPs. A complete request of this nature can provide the automated system with the necessary information to process it and in marginal cases assign it to human review. In the case of YouTube, for example, the “relevant and necessary” information also includes the specific portion of the reported video as a requirement for a valid notice. (Romero Moreno, 2020)

Apart from the prohibition of general monitoring and similar to the false positives is the fact that there is a subjective element in cases of user generated content, really in anything that isn’t just a copy of a copyrighted work being illegally published online. The issues against filtering don’t have to do with the recognition of copyright material, but rather with the human element of its publication; first of all, it is difficult to check and evaluate who is the person posting the material, and if he is rightfully doing so. Secondly, despite the material being copyrighted, posting it might not be an act of infringement, based on the exceptions discussed above.

This brings to the forefront the issue of false positives in the process of automated content filtering. As discussed already, it is not yet possible for algorithmic enforcement to distinguish between permitted and non-permitted uses of copyrighted content, nor of course argue and reason for marginal cases. In that event, it instantaneously blocks an upload, removes said content, or in some cases offers the uploader the option to edit out or mute the identified as copyright infringing part⁵⁵. The latter is no permanent solution, as it does not answer the issue of blocking perfectly legal content and alters the work created.

⁵⁵ <https://support.google.com/youtube/answer/2902117?hl=en>

It needs to be noted, however, that overall it appears that accuracy has improved with the utilization of automated systems – at least in the detection stage, as well as by providing a structured, optimized way of notice. (Erickson & Kretschmer, 2020) The main concern is overenforcement by choice or by default rather than a sticky problem of mistakes. Human notices and the potential exploitation “robo-notices” (Karaganis & Urban, 2015) which are sent by enforcement agencies acting on behalf but not always in accordance with rightholders and which can “introduce and amplify errors affecting significant quantities of works.” (Erickson & Kretschmer, 2020)

Whatever the case is, however, for the time being content recognition mechanisms are equipped to do just that, identify the content of a file by matching it to an existing sample from a database. (Spoerri, 2019) They cannot go further and determine whether or not a specific upload constitutes copyright infringement. Thus, their actual functions as of today must not be overestimated based on optimistic predictions about the future.

Finally, it is a matter of contention what an acceptable margin of error is. Audible Magic boasts that its software is accurate in about 99% of the cases. However, the acceptable false positive ratio for i.e. e-mail providers misidentifying an email message as spam is 0.1% and anything higher than that is deemed unacceptable due to the possible implications on the users’ freedom of expression. (Engstrom & Feamster, 2017) In reassessing the 99% claim under the lens of the millions of uploads OCSSPs deal with daily, a rate of error of one out of a hundred compounds to an enormous number of violations of the freedom of expression of their users – not to mention the freedom of information of the public. The impression of accuracy is false, according to Spoerri (2019).

3.3.4 Loss aversion

Loss aversion is a term borrowed by the field of behavioral economics in the analysis of decision making. In short it describes the way one feels the pain of loss twice as intensively than the equivalent pleasure of gain and the impact this emotion has in their decision making, leading them to try to avoid loss in any way possible. (Kahneman & Tversky, 1979) There has already been a discussion herein about the non-existent disincentive for a (fake or legitimate) rightholder to request a takedown and the incentive of an OCSSP to simply takedown the material instead of performing a more granular analysis, given their liability in case an infringing case remains online after it has been brought to their knowledge.

Given the low degree of uniformity and integration in copyright law and enforcement, there have been and in the foreseeable future will be a lot of flawed or inaccurate notices. Issues like a lack of signature, specificity, statement of good faith and accuracy are solvable and OCSSPs take measures

to reject such obvious defects. They are however, reportedly limited on how to proceed with more substantial matters. (Gray, 2017). Senders should be notified to correct them with the penalty of rejection.

However, a mistake in the request does not change the status of the work as legal or illegal, and it's harder for ISPs to claim ignorance. As things stand, intermediaries face a far greater risk if they reject a claim, thus in some case they default to accepting requests. (Urban, Karaganis, & Schofield, 2017) Sometimes they accept close to 100% of requests by taking down the relevant material, effectively taking copyright claims at face value. (Gray, 2017)

This conservatism is exactly what is feared. Regardless of the letter of the law, the risk imbalance can lead to a general censorship of what is posted online, despite the intentions of the policymakers. This “lack of disincentives or remedies for erroneous notices” (Riordan, 2013) is certainly alarming and encourages online service providers’ risk aversion.

3.3.5 Private authors’ and small rightholders’ cul-de-sac

Private authors and small rightholders find themselves in unfavorable position in the current environment as well as in the regime proposed by the DSM directive. The prioritization of licensing by the directive is not compatible with these categories of rightholders, as licensing is usually complex and charged with large transaction costs. (Leistner, 2020) In case of automated enforcement, such as ContentID, there is also a gap. Oftentimes the creations of such smaller scale authors, i.e. YouTubers rely on adaptations, critique or transformative uses of copyrighted material. Algorithmic systems tend to reallocate monetization of such material to the original rightholder, regardless of possible exceptions to copyright. (Leistner, 2020)

The issue is accentuated by the lack of options for those types of creators, that will be discussed in the following paragraph. In combination, those issues form an unfavorable environment for new creators to generate original or derivative work.

While the rise of OCSSPs empowers individuals to create, it does not offer the same facility to protect or profit from their works that is afforded to represented rightholders. As such there is an asymmetry. Large rightholders can protect and monetize their content posted in OCSSPs and often monetize it when a smaller creator has used it without infringing copyright, while an individual creator does not have the same opportunity. It is becoming almost imperative for the creator to join an established agency. However, this hinders the positive development of decentralizing creation.

Generally, the difficulty for private authors and small rightholders to license or register their creative work is an issue for OCSSPs as well. That kind of content is still copyright protected, and such platforms lack an obvious way to license it. As such they remain vulnerable to liability in case of a potential

infringement of the works of the numerous small rightholders whose work is not a part of filtering databases and not identifiable by the OCSSPs. (Abecassis & Gann, 2018)

3.3.6 Power imbalance between sender and user – imbalanced incentives for OCSSPs

According to Gray's study (2017) - among others - counter notices for takedown requests are few and far between. In her study, OSPs interviewed expressed their concern in encouraging users to assert their rights because of the power imbalance between notice senders and users – even in cases of clearly invalid notices. Urban, Karaganis & Schofield (2017) mention the high costs of a defendants' right to sue in case they want to contest or seek damages for wrongful copyright notices. As we mentioned above, users lack the incentive to use complaint and redress mechanisms, both due to them being slow and because OCSSPs tend to default in the side of the sender of a notice, creating a biased playing field.

The same issue is examined by Leistner's (2020) work about the DSM directive's art. 17 in comparison with the U.S. landscape. Leistner argues that the present legal situation presents biased incentives to OCSSPs, as non-compliance with a copyright notice makes them liable and at the same time an unjustified takedown will probably result only in an obligation to reinstate the material in question. As he specifically points "over-compliance will in most cases at best merely result in a duty to unblock the content". (pg.45)

This is clearly in contrast with the explicit intention of the directive for OCSSPs to provide "an effective and expeditious complaint and redress mechanism"⁵⁶ to their users. While the directive mentions those mechanisms and the provision of out of court settlement options, it doesn't order monetary remedies compared to the DMCA. (Urban, Karaganis, & Schofield, 2017) This situation is especially problematic, as they also note in their study that almost one third of automated notifications are invalid.

It is important to point out that usually the two sides come from a very different place in the first place. Usually senders are agencies or large corporate rightholders that have a vast amount of human and monetary resources, while users are usually up and coming creators or small rightholders that lack both the time and money to enter a legal battle. Institutional rightholders would almost always win this war of attrition, discouraging smaller players from contesting claims. This is exactly the reason why those imbalanced incentives widen the disparity and make little sense from the perspective of creating a fair market.

⁵⁶ Directive (EU) 2019/790, Art. 17(9)

3.3.7 Competition – Proportionality

Another concern that has been a point of debate leading to the final text of the DSM directive is the matter of the way the proposed measures will impact the market and more specifically the competition among ISPs. This especially touches upon art. 17 and the de facto obligation to use automated detection systems (Frosio, 2017) in order to enjoy immunity from liability under the commands of the directive.

Algorithmic solutions are expensive, cutting-edge commercial products that target a very specific niche in the market, with a few global conglomerates dominating the sector and their pricing follows suit. (Abecassis & Gann, 2018) Such powerful companies also possess the human and technological resources to develop solutions on their own. Conversely, service providers that are start-ups or SMEs usually lack the monetary or technological resources to get their hands on the same filtering solutions, not to mention develop their own. This arguably presents an uncompromising barrier to entry into the OCSSP platform market and poses competition law issues. (Mostert & Lambert, 2019)

Notably, the DSM directive provides safeguards for exactly this type of companies, at least in theory. Specifically, art. 17(6) reads:

[...] 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/EC (20), 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. (pg.120)

This is however a very narrow and specific scope that very few online service providers might actually benefit from (Samuelson, 2020) and such protection might actually be irrelevant due to the start-up businesses' "grow or bust" mentality. (Abecassis & Gann, 2018) Taking into account that the way that funding from investors and hedge funds is the main driver of a start-up company's growth, this is especially damaging as a relevant survey (Le Merle, Le Merle, & Engstrom, 2014) states that most investors would be

“uncomfortable investing in businesses that would be required by the law to run a technological filter on user uploaded content”.

While firms who can and have developed their own filtering technologies can enjoy economies of scale (Spoerri, 2019), smaller companies face the imposition of the DSM directive as a barrier. This is evidenced as well by the open letter to the EU parliament members from 240 (with many more following after the initial publication) EU Businesses against the copyright directive, in which they state that “most companies are neither equipped nor capable of implementing the automatic content filtering mechanisms”.⁵⁷

ContentID on the other hand might be considered the benchmark, but it is a proprietary software available only for its developer, Google/YouTube. It has been argued however that ContentID’s power lies in its comprehensive database which allows it to be so efficient in detecting uses of copyrighted material – and as such Google is in a dominant position, in which case “a compulsory access to the system on reasonable terms could be granted on the basis of European competition law.” (Leistner, 2020) However, such a plea will definitely face difficulties and pushback from the market leaders in algorithmic enforcement, and a fragmented sum of particular databases that would be costly and cumbersome for OCSSPs to check against, is a more likely outcome. (Abecassis & Gann, 2018) At the same time, as member states are given flexibility on how they will implement the directive in their domestic law, creating a central European database might not be possible due to differences in defining copyrighted material in national legislations.

The directive has not completely ignored the potential of an overly burdensome duty to OCSSPs, as evidenced by the proportionality principle incited in art. 17(5) and more specifically based on the factors of the type and audience of the subject matter uploaded, as well as the “availability of suitable and effective means and their cost”. This principle protects, at least theoretically, OCSSPs from being obliged to implement unfeasible measures but might come in conflict with the rest of the regulations of the same article. As such, the definition of what those measures are and what the high industry standards are in a market dominated by certain platforms and very few filtering alternatives has to be a focus of the stakeholder dialogue before the adoption of the directive by the national laws. The commission will have to offer guidance on matters of best efforts and available cost-efficient solutions in the market, pursuant to the standards outlined in the directive, in order to at least provide a framework for all but the industry leading firms such as Google. (Leistner, 2020)

⁵⁷ <https://nextcloud.com/blog/130-eu-businesses-sign-open-letter-against-copyright-directive-art-11-13/>

3.3.8 Transparency and Accountability

Given the increasingly valuable role OCSSPs play in our lives already discussed herein, from the access to information, to their role as entertainment and creative outlets and their processing of personal data, OCSSPs are a factor in the protection of fundamental rights. In that role, there is a need to assess the balancing of rights in their legislation and actions and a call for transparency in their operation and the plans they implement to comply with their legal obligations. Granting “decision-making power to commercial players that dominate the market” (Elkin-Koren, 1998) generates an obvious need for accountability for their de facto role in governance, a demand that is central in democratic systems. (Gray, 2017)

At the same time, the DSM directive in art. 19 specifies the transparency obligation towards all kinds of rightholders on a regular basis and taking into account the specificities of each sector regarding licensed material. The directive offers more detail in several recitals where the requirement for transparency in OCSSPs part is analyzed in more detail. Such a call for transparency is also informed by the Impact Assessment (Commission, 2016) in which rightholders testified that the way notice and staydown systems function remains opaque to them.

This requirement is especially significant in conjunction with the art. 17’s requirements for technological solutions, as such technologies are usually opaque by design, complex technical measures that are practically unknowable by the public, and also veiled behind trade secrets. (Gray, 2017)

Interestingly, the directive fails to mention users and the public as beneficiaries of this right to transparency and information, despite them being also subject to the process of copyright enforcement and with their data being analyzed in the process no less. As Romero-Moreno (2020) concludes, the accessibility principle under art. 8(2) and 10(2) of the ECHR is not met as users are not afforded the ways to understand how such filtering measures influence their electronic communications. Transparency towards users (in the form of user organizations) is only mandated in art 17(10) of the DSM directive about the stakeholder dialogue, rather than continuously as the process of copyright enforcement progresses and decision are made. This contradiction of limiting transparency duties to rightholders rather than authorities and users is also pointed out by Leistner (2020).

Gray (2017) has also underlined the issue of accountability in an environment of “private regulation” posing critical issues for public rights by the use of algorithmic solutions in copyright enforcement – as private entities are not accountable to the public.

Accountability means that decision makers justify their choices and “exert power in a fair an effective manner”. (Perel (Filmar) & Elkin-Koren, 2016).

The aforementioned privatization of governmental functions and the fog between private and public makes the matter of accountability especially significant, as Perel and Elkin-Koren (2017) characteristically comment, summarizing the accountability of ISPs regarding their automated content recognition systems:

“proper accountability mechanisms are vital for policymakers, legislators, courts and the general public to check algorithmic enforcement. Yet algorithmic enforcement largely remains a black box. It is unknown what decisions are made, how they are made, and what specific data and principles shape them.” (pg. 184)

To conclude, UN special rapporteur David Kaye underlined that “developers such as Audible Magic should make all filtering criteria fully auditable”. (UNHRC 2018, as cited in Romero Moreno 2020)

3.4 Proportionality – Balancing of competing rights

Throughout this analysis of the issues a consistent pattern comes to the surface. The options OCSSPs use to monitor copyrighted content and prevent access to infringing material, especially given what the Art. 17 of the DSM directive indicates, interfere with fundamental human rights protected by the European Charter of Human Rights (ECHR) as well as specific directives and regulations (e.g. the GDPR). The freedom of expression, the freedom to access information, the right to privacy, the freedom to conduct business and the right to a fair trial are especially relevant here and have to be balanced against the protection of intellectual property, also recognized in the same text, that dictates ISPs obligations. Relying solely on the letter of the law and the current technological capabilities threaten to brush this invaluable balancing aside. Both the academic literature and the European courts have been involved with the clarification of this balancing of rights. The user-freedom-related revisions to Article 17 reflect the Commission’s acceptance that the *new strict liability rules pose a much greater risk to fundamental rights than it previously acknowledged*. (Samuelson, 2020)

In recitals 84 and 85, the DSM directive states that it should be interpreted and applied in accordance with the rights and principles of the ECHR and that any processing of personal should respect fundamental rights, including “the right to respect for private and family life and the right to protection of personal data set out in Articles 7 and 8 of the Charter” and in compliance with the General Data Protection Regulation⁵⁸.

According to the ECHR any interference with art. 8 (right to private and family life and correspondence) and art. 10 (freedom of expression) must be a. in accordance with the law; b. pursue one or more of the legitimate aims in their

⁵⁸ Regulation (EU) 2016/679

respective second paragraphs (notably for the protection of rights and freedoms of others); and c. be necessary and proportionate. The three criteria have to be met cumulatively for the interference not to violate the relevant rights. (Romero Moreno, 2019)

Frosio (2017) notes that the implementation of automated content filtering technologies is favoring property rights disproportionately against other categories of human rights, and for that their use is inappropriate. We have already commented herein that copyright is not absolute and gives way to rights and freedoms of greater significance.

The DSM directive recognizes this precarious balancing of rights in the recital 70, with respect to article 17(7) stating that “it is particularly important for the purposes of striking a balance between fundamental rights laid down in the Charter of Fundamental Rights of the European Union, in particular the freedom of expression and the freedom of the arts, and the right of property, including intellectual property”. The commission’s inciting of the charter of fundamental rights leaves no question marks.

Another point of emphasis in the balancing should be the compliance of measures against copyright with the right to privacy and data protection principles, taking into account both the charter and the GDPR.

It is important to note that even before the DSM directive coming into force, the European Commission, in its impact assessment on the modernization of the EU copyright rules has highlighted the risk of false positives, especially in the case of transformative uses. (Commission, 2016). Along with the general shift from reactive to proactive copyright enforcement implied by the DSM (Schwemer, 2020), content moderation balances precariously between fairness and censorship. The concern about a correct balancing of rightsholder protection and freedom of expression is further highlighted by Poland’s action⁵⁹ challenging upload filters before the CJEU stating that *“the obligations on the [OCCSPs] foreseen in the contested provisions will necessarily have as a result the introduction of preventive control mechanisms which, view of the applicant, undermine the essence of the right to freedom of expression and information and which do not comply with the requirement that limitations imposed on that right be proportionate.”*

As the ECHR mentions on article 52 “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.” As such, any preventive

⁵⁹ Case C-401/19, Republic of Poland v European Parliament and Council of the European Union (2019/C 270/24), OJ C 270/22;

measures must be proportional to the goal they are trying to achieve. Any limitation or burden imposed on intermediaries, and consequently their customers and/or internet users is also a limitation of their rights.

Commenting on the matter of a measure's effectiveness when assessing its proportionality, it is argued about blocking measures by Husovec & Van Dongen (2017) based on several decisions of national courts and citing the CJEU's *Telekabel Wien* case that the mere fact that a technical measure is circumventable does not portend that it is disproportionate in the sense mentioned above. The argument that such a blocking measure was disproportionate due to its limited effectiveness is not convincing. Additionally, that the measures taken by an ISP need to be taken as whole in the assessment of their proportionality and effectiveness, as an individual measure might be necessary but not sufficient to achieve the desired outcome. (Husovec & Van Dongen, 2017). As Castets-Renard (2020) puts it, "without tools and data access to oversee removal decisions, pursuing safeguards to protect fundamental rights is a utopian goal."

As noted by Leistner (2020), the rationale behind article 17(7) of the DSM directive in general necessitates a solution that considers and actively takes into account the user's freedom to use the legal exceptions "from the very first steps onwards throughout the entire enforcement process". As such relying only on a – still inefficient - complaint and redress mechanism is not a sufficient safeguard for the users' fundamental rights.

As far as users' personal data are concerned, the implementation of automated content recognition systems represents a threat to the users' rights. This is recognized by CJEU in the *SABAM vs Netlog* case which has deemed such measures against fundamental rights. The rationale behind it that the function of such systems involves the identification, analysis and processing of information of profiles created on the platforms by their users. Since the individuals are identifiable based on these data, and especially if the software is proceeding to automated decision making, the rights of the users are being impinged.

To exemplify further, the GDPR forbids decision making based solely on automated means in article 22(1)) and profiling in article 4(4). Article 17(9) of the DSM directive states that its implementation shall not lead to "any identification of individual users nor to the processing of personal data" except in accordance with the ePrivacy directive and the GDPR. (Romero Moreno, 2020) In case such systems, as Audible Magic can, collect personal data and can identify repeat offenders in order to better deal with violations fall under the scope of these provisions. The compatibility of the DSM directive's mandates with the GDPR rests on whether or not this data processing passes the three-part test of the ECHR. (Engeler, 2019)

CHAPTER 4

4. Recommendations – Designing a strategy

4.1 Improving Algorithmic Enforcement

It is unfortunately hard to imagine, much less describe and implement, a legal framework that will stay ahead of commercial level infringers. The avenues and alternatives are simply too many, the technology ever-advancing, making the discovery and exploitation of loopholes a near certainty. This might sound grim and deterministic. However, saying that unlawful players will always find ways to circumvent technical and legal measures is based on real examples. Commercial scale infringers don't seem to go away despite global efforts.

The realistic goal for copyright enforcement and the DSM directive within the scope of this study is the outline of an integrated solution that can facilitate the access to lawful material and the accuracy of copyright notices or algorithmic solutions, in a way that both improves the financial viability for OCSSPs and respects users' and rightholders' rights in a balanced manner. Deliberate and involuntary copyright infringement still occurs, and the DSM directive's strategy against it is the promotion of licensing and the implementation of automated content recognition technologies.

In my opinion, rightholders (either individually or as part of large publishers) should focus on commercial level infringers ("follow the money" approach) and target the stifling of their profit from illegal activity. Trying to combat each case of infringement individually on such platforms is a costly and futile endeavor. This is acknowledged by the DSM directive as well, which excludes from the definition of online content-sharing service providers "services that have a main purpose other than that of enabling users to upload and share a large amount of copyright-protected content with the purpose of obtaining profit from that activity." (recital 62). However, infringement happens and enforcement is pursued through legal channels. In this case the objective is not to impede users enjoying their rights and freedoms accessing lawful content, obstruct (sometimes marginal) cases of exceptions⁶⁰, or punish those who might infringe copyright sporadically by accident. What should be the target are online service providers that systematically perform infringing actions and profit by it. In most cases this is where the demonstrable damage comes from for rightholders. As such monitoring has to be content and context depended.

That is why preventive actions such as filtering can only help up to a point. As examined above, algorithmic solutions are currently not capable of providing qualitative and contextual judgement. It has to be conceded that a

⁶⁰Art. 17(7) DSM Directive

human review is necessary and that not every case that is matched by the algorithm shall be automatically blocked, as this would conflict with users' rights. (Abecassis & Gann, 2018) In order for the algorithmic enforcement to be both effective and proportionate and in order for it to serve rather than compete against human review, there has to be a shift in rightholders' expectations, especially the large entertainment companies that represent large number of rightholders.

The "one view – one sale" logic is dated, not only outpaced by the new forms of media consumption, but evidenced by the benefits those companies and rightholders, especially the established ones, enjoy by the circulation of their material – even when it is illegal. It has really opened up a global market without any extra cost of promotion⁶¹. Benefits in terms of promotion and reach would be interesting to be studied further and obtain accurate data on. The "value gap" theory that lies on the epicenter of these developments has a narrow scope and is not empirically proven. (Frosio, 2017) To support this, I have used the Luo & Mortimer (2019) continued experiment to examine infringement as a driver of demand, and how it can be weaponized as a marketing tool – though this example refers primarily copyright infringement of images and its effects on attracting licensing. It is however notable that they report mitigation of search and transaction costs, rather than an overall damage.

4.1.1 A balanced combination of automation and human review

The need for a balanced synergy between automated decision-making systems and human moderators has been widespread in the literature (Castets-Renard, 2020). So far in this study we have seen the limitations of automated systems, as well as their potential.

As Castets-Renard (2020) puts it, algorithmic enforcement is especially useful but at the same time especially problematic in terms of copyright enforcement. Automated systems cannot interpret neither the content nor the context of the cases they make decisions on. However, especially in copyright related decisions, both the content and the context are crucial, either in the

⁶¹ It bears noting, however, that the literature is not conclusive on that matter and a lot depends on the industry. Danaher, Hersh, Smith, & Telang (2019) and Smith & Telang (2012) support the view that piracy outright harms media sales, based on a number of empirical studies. Nonetheless, the same researchers (2012)(2019) have found in previous studies that legitimate paid and illegitimate free versions of the same works appeal to different customer segments and also note that other empirical studies found no correlation between pirated content and loss of sales (Smith & Telang, *Competing with Free: The Impact of Movie Broadcasts on DVD Sales and Internet Piracy*, 2008). Much less when the issue is not commercial-level piracy, but rather the usage of a part of a copyrighted work in a new creation or a marginal case of exception. The conflicting results of the same researchers are indicative of the difficulty to quantify the loss of sales in the digital environment, as well as any benefits to the popularity that can be capitalized over time.

matter of fair use and exceptions, or regarding the identity and specificities of the infringer.

Matthias Leistner (2020) offers a more levelheaded view in light of the debate around the DSM directive, focusing on the potential of algorithmic enforcement and stating that the article does not necessarily mandate a general monitoring obligation, but instead calls for an effective and proportional dynamic combination of algorithmic tools and human intervention.

In my opinion the idea introduced by Leistner is appropriate. In the basis of its application lies the synergy between human logic and technology. Specifically, “trusted” users should have the opportunity to flag content as covered by a legal exception and delay the takedown process if their claim proves plausible “under a quantitative algorithmic check”. This process seeks to improve both the issue of the, often crucial, time period that lawful material is erroneously taken down and hurting both the uploader and the public’s freedoms and also gives the opportunity to any uploader aware of using a copyright exception, to help themselves enjoy the protection granted to them by the law. Leistner (2020) envisages this process to be combined with a new category of trusted rightholders to develop into “a dynamic, self-regulating system of process oriented complementary coupling of algorithmic tools and human agents.” (p. 77)

In time, the combination of algorithms and humans will enable both to make better informed decisions, as machine learning algorithms will not only rely on self-generated data, but will also use the human input in marginal cases to at least perform more accurate probability checks. The balance between automated decision making and human review needs to be monitored constantly according to the former’s results and the latest technological developments.

4.1.2 Empowering users from the upload stage rather than relying solely on complaint and redress mechanisms

The improvement of the complaint and redress mechanisms, both in terms of availability and in terms of speed is important and has been a point of emphasis in the academic literature as well as the DSM directive. The same holds true for effective alternative dispute resolution methods. However, the author of this study, in accordance with Leistner’s (2020) recommendations, believes in the power of empowering the individual users from the very first step of the copyright enforcement process, namely from the upload stage itself. This can be implemented in the interfaces of OCSSPs where the user can indicate the compliance of the uploaded material with copyright legislation. Of course, this presupposes platforms giving correct information about the law and the exceptions in an easy-to-understand and relevant manner, e.g. by notifying the

user during the upload stage and referring them to the relevant legal texts, or showing examples from uploaded material.

The technological readiness for algorithmic systems to assess the plausibility of such claims is in question, but it is reasonable to expect a high success rate in cases that a quantitative check can inform about the probability of such claims. (Leistner, 2020) The data derived information and statistics from such checks can help the subsequent human review in marginal cases. The added benefit of emancipating the user from the upload stage and of course the “dialogue” with the rightholder in case of dispute, is the possible formation of a better-informed digital society, one who can minimize the involuntary mistakes in the process and raise the baseline of expected knowledge around copyright tools.

As far as private authors or smaller rightholders are concerned, and based on the current reality that they are less likely to have their works licensed much less provide them in an appropriate form to be included in the reference database for algorithmic enforcement (Abecassis & Gann, 2018), a potential solution could be to afford them the tools institutional rightholders are afforded to manage their work and to provide the means for them to register and license their content – at least pending review and with preset terms - at the point of upload, eliminating the costs associated.

To sum up, the pursuit of a more active role for the users uploading content in OCSSP’s platforms would be a beneficial solution for all parties. In order for that empowerment to be realistic, it is important for OCSSPs to be able and willing to provide relevant information regarding the copyright status of the involved works, actionable information based on the copyright legislation regarding the rules and exceptions that apply in an easy to understand form and implement the tools and processes for the users to act based on those. While commercial infringers will not be stopped, the volume of accidental or negligent infringements is bound to be minimized, mitigating some of the burden for OCSSPs and allowing them to provide a better, safer service to their users while safeguarding their rights and those of the public more effectively.

Along with the possibility of a centralized database discussed below, campaigning from human rights groups, artists’ organizations to provide relevant information to the consumer and the small-scale creator at the point of upload or viewing, in an easy to digest form that could be implemented by OCSSPs would be of great help towards minimizing involuntary infringement and consequently reducing the providers’ incentive to over-enforce.

4.2 Battling overenforcement

Most of the issues discussed herein inevitably converge to the pressing issue of overenforcement. The limitations of technology, the legal incentives, the financial choices, the ascension of algorithmic solutions and lack of

education from users and creators all dictate a stricter monitoring and a tendency to block rather than allow in instances of doubt. Almost all the matters discussed above are either a cause of overenforcement or a trickle-down effect.

The analysis of recommendations has to take as a guiding principle the protection of users' fundamental rights and interests, not only because freedom of expression and the right to privacy are rights of a higher order, but also because they are the ones threatened the most by the current status quo. At the same time curbing overenforcement has to be financially viable for all OCSSPs and not only the Big Tech companies. Through that lens, it is useful to refer to the Lenz decision discussed above⁶². According to my view and Leistner's (2020) analysis, the use of automated tools is necessary. Even if they cannot make judgment on marginal cases regarding fair use and exceptions, and are guided by the OCSSPs interests with a tendency to over-block, they are currently capable of performing "ex ante plausibility checks", that can be informative to OCSSPs and rightholders. The latter will have to "cross-check whether fair use is overwhelmingly likely in a given case before sending out infringement notifications". The final goal is to establish a "minimum standard for infringement notifications". This is clearly a step in the right direction, that is also feasible for OCSSPs, as a demand for their filtering systems to perform comprehensive checks and judgements about borderline cases or ensure human review for every case would be undoubtedly overbearing and in conflict with DSM directive's art. 17.

4.2.1 Data-driven approach to identify clusters of bad notices

Another field of improvement that can help with overenforcement is the analysis of the most consistent predictors of bad claims. Examining low quality notices can help with strategizing against them, deprioritizing their process and more importantly, giving spot-on guidelines to educate the relevant audience. Encoding basic statutory requirements for claims will help first-time or one-off senders of notices to know what is expected of them and help them formulate their claims in a more precise way.

An analysis of predictive factors of claims that lead to overenforcement or for the identification of frequent copyright infringers will inevitably involve processing of personal data. In order for it to be lawful it should use only the minimum and necessary amount and be proven to produce positive results in the total number of infringements or erroneous notices in order for it to be lawful.

4.3 Competition issues

Regarding the issue of protecting competition and ensuring a fair market where new entrants can compete without being practically denied access due

⁶²Lenz v. Universal Music Corp., 801 F.3d 1126 (9th Cir. 2015)

to the dominant position of the Big Tech companies or the excessive financial burden of their copyright obligations, it is recommended that during the stakeholder dialogue there will be a more balanced and nuanced approach to the clarification the directive's "best efforts" and "high industry standards" requirements' meanings. At the same time, the directive talks about not only the availability of technical measures to comply with the obligation of art 17(4) but also the availability of licensing solutions.

As such the council should incentivize licensing by ensuring its fair pricing for smaller businesses and aid small rightholders in their licensing processes as they may not be able to access licensing the same way or implement automatic content recognition solutions.

A step further is that the best efforts have to also be feasible. Even if smaller businesses buy or develop their automated preventive solutions, the current market-based (e.g. Audible Magic) or proprietary (ContentID) software set a very high bar, but more importantly rely on a wide database of files that they accrued overtime and will have an incentive to try and withhold from other in coordination with large rightholders to control the market. It has been argued that their power lies in large part on their available databases of copyrighted files, rather than the technology itself. (Abecassis & Gann, 2018)

A couple of solutions, that both need significant political equity and will create a backlash from the Big Tech companies are the following:

The first part is to make access to the currently available database compulsory, (Abecassis & Gann, 2018) effectively disbanding the connection of the software to the database and probably conflicting with current market leaders. The other part is the "establishment of an EU-wide centralized EU-sponsored repository in order as to allow for equal access by all potential users and for controlled updating of the data by authorized entities." (Leistner, 2020)

While these measures might seem overly restrictive for the market, they really are the opposite. Limitations have two faces; accepting that a measure restricts the current market leaders' freedom to conduct business, overlooks that those market leaders enjoy dominant positions in the market and help create insurmountable barriers to entry for new businesses. Competition law exists not to protect businesses from competition, but rather protect the notion of competition from business practices that stifle it. It is unreasonable to expect a new business to be able to both prove its financial sustainability while having to both have a system in place – threatened by costly injunctions otherwise – and make best efforts to secure licenses from a vast and fragmented entertainment landscape. Even established businesses reportedly claim they are unable to implement automated content recognition systems currently.⁶³

⁶³<https://nextcloud.com/blog/130-eu-businesses-sign-open-letter-against-copyright-directive-art-11-13/>

In any case, in order for these recommendations to be effective, an enormous database has to be constantly updated with the collaboration of rightholders. (Abecassis & Gann, 2018) An accessible centralized database consolidating the sum of efforts and expertise by OCSSPs and content recognition software providers, would make it copyright enforcement more efficient for OCSSPs and rightholders alike. At the same time, it would help with compliance with the ECHR and competition law and ultimately guard against mistakes in enforcement, benefiting the public.

4.4 Improving the complaint and redress mechanism by incentives

The need for a more effective, easier to access complaint mechanism has been a mainstay of the academic literature during the past few years. (Mostert & Lambert, 2019) The limitations of this mechanism in its current form in terms of speed and effectiveness are also well documented. (Leistner, 2020) Users need to be certain that if they follow what the law indicates their material will be uploaded and stay up until successfully contested otherwise. When an OCSSP makes the decision remove or block access to uploaded material, they should properly inform the user about the decision and its rationale, and provide them with the tools to contest the decision.

This view is also supported by the examination of art. 17(9) of the DSM directive about the platforms' prohibition to take-down content "which does not infringe copyright" or copyrighted content "covered by an exception or limitation.". This could be interpreted as a stay-up obligation from the side of the OCSSP. (Schwemer & Schovsbo, 2020)

In order for those requirements not to remain empty letter, the EU and global authorities shall consider the imbalance of incentives that is observed in copyright enforcement today, for which I have talked about in section 3.3.6.

A reconsideration of the currently biased incentives is necessary, either in the former of stricter rules against erroneous takedown notices by rightholders or against overcompliance by OCSSPs, possibly allowing users to seek damages. This has to be coupled by the requirement of a higher degree of detail in takedown notices by the totality of OCSSPs and of course not lead to overreliance on algorithmic matching by the complacency that the complaint and redress mechanism works. Optimally this would work best with the empowerment of the user/uploader, balancing the options of all the sides involved.

As Leistner (2020) comments, incentivizing rightholders to act in accordance with a higher standard when notifying or when choosing what they can do with material flagged as infringement would almost certainly entail sanctioning incomplete or done in bad faith notifications and impose the obligation to carry out a plausibility check with regard to overwhelming likelihood of fair use.

Simplified, when a marginal case is detected by the algorithm the file can be brought to the attention of the rightholder as well as the creator, who will have to claim an exception for his file to stay up if it is preliminarily deemed legal or to be reinstated in case an exception is not probable. The success or failure of a claim can slowly build a profile of users. Filtering mechanisms are solely thought of as binary mechanisms of blocking or allowing content, but rethinking the technology as a notification/sorting mechanism might lead to more sustainable solutions.

4.5 Non-commercial User-generated Content

Canada's copyright Act 1985 has been praised as a middle ground, a balanced solution with reasonable demands and exception, avoiding the extremes both sides are pushing for. An interesting addition to the copyright landscape is the provision to "permits an individual to use an existing work in the creation of a new work for non-commercial purposes, and to authorize its dissemination", titled "Non-commercial User-generated Content exception"⁶⁴ – also known as the "YouTube exception". The global landscape, however, does not seem ripe for such a forgiving solution. "One major flaw in this exception is that it conflates non-commercial use with amateur creation. The distinction between amateur non-commercial use and professional commercial use is arbitrary and cannot sustain itself in modern technological practices". (Craig, 2019)

⁶⁴ Copyright Act 1985 (n 3), s. 29.21

CHAPTER 5

5. Conclusion

5.1 Synopsis

The latest development in the ever-evolving global copyright landscape has been the Directive (EU) 2019/790 of the European Parliament and the council, an attempt to harmonize copyright rules aiming to help create a digital single market. The period before the directive came into force has been characterized by an unprecedented debate, for its potential impact on fundamental human rights and competition.

In the present thesis I attempted to discuss the current copyright landscape as the member states have yet to implement the directive into their national legislation and examine the options online content-sharing service providers have in their disposal to prevent copyright infringement on their platforms in terms of effectiveness, legality and feasibility.

The view that while the DSM directive seeks to harmonize copyright rules, at the same it puts competition and fundamental rights at a vulnerable position is found to be reasonable by the present study; it has not, however, been found to produce such a dire situation as the one that was described in the heated debated that preceded its final text. Within it there are the seeds of a more balanced copyright environment.

After reviewing key concepts and literature illuminating the discussion in the present thesis and upon assessing the current situation regarding OCSSPs and copyright rules, the focus has shifted automated content recognition mechanisms and algorithmic enforcement. Such measures initially seem to contradict the prohibition of member states to impose a general monitoring obligation. The threat is imminent, it is not however a fault of technology, but of the manner of implementation of such measures. Algorithmic enforcement is not a panacea that can liberate OCSSPs and rightholders from the burden of detecting and tackling copyright infringement. It is however an invaluable tool with great potential in managing the enormous scale of copyright infringement, integrated with the traditional notice and takedown system, human review and the emancipation of users in the process of copyright enforcement.

The other thorny issue regarding the implementation of automated systems of copyright enforcement concerns their cost and impact on competition. As SMEs and start-ups have been found in most cases not to possess the financial and human resources to implement such systems, they find themselves in a highly unfavorable position that allows Big Tech companies to dominate the market. It has been argued that the value of such systems lies in their accumulated databases rather than the technology, and the author is in

favor of the proposed solution of creating central accessible databases in order to alleviate some of that burden.

Despite the focus on algorithmic enforcement, the study has found that traditional measures of preventing access to illegal material are still important in the battle against copyright infringement. The “notice and takedown” system is still an effective foundation, and automated content recognition can aid with the stay-down mandate proposed by the DSM directive. Blocking injunctions, search engine removal, bad actor listings and traffic shaping remain effective in a case by case basis.

The directive, however, does push OCSSPs further towards overenforcement and that leaves users and the public’s rights in a vulnerable position. The mistakes in copyright enforcement, automated or otherwise, exacerbate the issue. This stems from the biased incentives for OCSSPs that logically err in the side of over-blocking to avoid monetary damages a danger that is absent in the opposite case. OCSSPs benefit from siding with large rightholders as well, as they will turn to them to negotiate and license content. As such the precarious balance of copyright against the freedom of expression, the freedom to conduct business and privacy is a real issue that will remain on the forefront. The hope is that OCSSPs will not rely solely on automated decision-making and that policymakers will provide disincentives against doing so. The synergy between algorithmic enforcement and human review is necessary. An improved, quick complaint and redress mechanism can only help so far against an overly punitive copyright enforcement regime for users and smaller creators.

On the other hand, it has been found that the promotion of licensing and filtering currently propagates the pervasive issue of Big Tech companies and large copyright holders deciding the terms and measures among themselves, leaving private authors, small-scale creators and the public underrepresented. The directive does little but propose stakeholder dialogues to ameliorate this power imbalance. Including all parties in the process of designing the copyright enforcement strategy and empowering users through actionable information and relevant options is important in order to both minimize involuntary enforcement and respecting fundamental rights.

In a nutshell, while copyright infringement online is raging still, the financial impact it has on rightholders remains uncertain and algorithmic enforcement despite its current limitation and context blindness provides a hope that it can form the basis of a safer copyright environment. For that to happen OCSSPs and software developers have to take human rights into account when designing their solutions and copyright strategies, as the ultimate goal of intellectual property is to foster creation and facilitate legitimate consumption of creations of the mind.

5.2 Thesis Limitations and recommendations for future research

While the present thesis attempted to examine the effectiveness, impact and limitations of copyright enforcement in light of the Digital Single Market directive, it nonetheless has several limitations.

First and foremost, the directive has yet to be implemented in the national legislation of the member states, thus the exact manner each country will specify the issues remains unclear. As such both the fears and hopes stemming from the directive's proposals are still based on a theoretical level.

The second significant limitation is the dearth of accurate and up to date data on the results of copyright enforcement from a financial standpoint, without a reasonable and widely accepted method of quantifying damage and the obvious incentive of rightholders to inflate their losses. While there are important studies in specific industries and over specific measures, there is no consensus in the literature about the actual damage done by copyright infringement or the effectiveness of the relevant measures and strategies in curtailing this impact. Most studies are done on a regional scale.

On the other hand, the operation of automated content recognition systems and the exact copyright strategies of the market leader OCSSPs are opaque. Companies offering content recognition software are similarly cryptic about their function. The author attempted to contact several of them to no avail. Thus, the conclusions are based on the publicly available information and inferred from secondary sources.

Consequently, the limitations of this study indicate the avenues for further research. The need for more accurate data and a method to quantify damages calls for cross-disciplinary longitudinal research of the financial effects of copyright infringement and enforcement measures.

Given the fact that the DSM directive will be implemented in the member states in the coming months, it will be interesting to study how they opted to solve the intricacies discussed above, specify the details they are called to do and the overall level of harmonization achieved in the wake of the DSM directive. Similarly, if the EU and U.S. converge on copyright strategy or further diverge fragmenting the landscape even more.

Finally, it would be beneficial to undergo more technically-oriented studies on how the desired synergy between automated recognition and human review can work, how the aforementioned plausibility checks can be performed and algorithms trained to achieve greater integration of contextual factors.

Bibliography

- Abecassis, D., & Gann, A. (2018). *The impact of a content filtering mandate on online service providers*. Analysys Mason.
- Agrapidis, P. (2017). "SoundCloud, Copyright Infringement, and the "DMCA" Safe Harbor". *Law School Student Scholarship*, 922.
- Angelopoulos, C. (2014). Are Blocking Injunctions against ISPs Allowed in Europe? Copyright Enforcement in the Post-Telekabel Legal Landscape. *Journal of Intellectual Property Law & Practice*, 812-821.
- Awan, M. (2016). The User Generated Content Exception: Moving Away from a non-commercial requirement. *Canadian Intellectual Property Review*, 32.
- Boroughf, B. (2015). The next great YouTube: improving content ID to Foster creativity, cooperation, and fair compensation. *Albany Law Journal of Science & Technology*, 25, 95-127.
- Bridy, A. (2016). Copyright's digital deputies: DMCA-Plus enforcement by Internet intermediaries. In A. Bridy, *Research Handbook On Electronic Commerce Law* (pp. 185-210). Cheltenham: Edward Elgar.
- Bridy, A. (2019, June 30). The Price of Closing the 'Value Gap': How the Music Industry Hacked EU Copyright Reform. *Vanderbilt Journal of Entertainment & Technology Law*, 22, 323-358. doi:10.2139/ssrn.3412249
- Castets-Renard, C. (2020, February 9). Algorithmic Content Moderation on Social Media in EU Law: Illusion of Perfect Enforcement. *University of Illinois Journal of Law, Technology & Policy (JLTP)*, Forthcoming. doi:10.2139/ssrn.3535107
- Commission, E. (2016). *Impact Assessment on the modernisation of EU copyright rules*. Commission Staff Working Document, European Commission, Brussels.
- Craig, C. (2019, November 1). Meanwhile, in Canada... A Surprisingly Sensible Copyright Review. *European Intellectual Property Review*. Retrieved from <https://ssrn.com/abstract=3494363>
- Danaher, B., Hersh, J., Smith, M., & Telang, R. (2019). *The effect of piracy website blocking on consumer behavior*.
- DeLisa, N. T. (2016). 'You(Tube), Me, and Content ID: Paving the Way For Compulsory Synchronization Licensing on User-Generated Content Platforms'. *Brooklyn Law Review*, 1318.
- Dornis, T. (2018). Non-Conventional Copyright: An Economic Perspective. In B. (eds.), *Non-Conventional Copyright*. Edward Elgar.

- Elkin-Koren, N. (1998). Copyrights In Cyberspace - Rights Without Laws? *Chicago-Kent Law Review*, 73(4), 1155-1201.
- Engeler, M. (2019, March 23). *Copyright Directive: Does the Best Effort Principle Comply with GDPR*. Retrieved from Telemedicus.info: <https://www.telemedicus.info/article/3402-Copyright-Directive-Does-the-best-effort-principle-comply-with-GDPR.html>
- Engstrom, E., & Feamster, N. (2017). *The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools*. Engine Organization. Retrieved from <https://www.engine.is/the-limits-of-filtering>
- Erickson, K., & Kretschmer, M. (2020). Empirical Approaches to Intermediary Liability. In G. Frosio (Ed.), *THE OXFORD HANDBOOK OF INTERMEDIARY LIABILITY ONLINE* (p. Forthcoming). Oxford University Press.
- Frosio, G. (2017, October 25). To Filter or Not to Filter? That Is the Question in EU Copyright Reform. *Cardozo Arts & Entertainment Law Journal* , 36(2), 331-368. Retrieved from <https://ssrn.com/abstract=3058680>
- Frosio, G., & Mendis, S. (2020). Monitoring and Filtering: European Reform or Global Trend? In G. Frosio (Ed.), *The Oxford Handbook of Online Intermediary Liability*. Centre for International Intellectual Property Studies. Retrieved from <https://ssrn.com/abstract=3411615>
- Gallo, L. G. (2011). The (Im) possibility of Standard Technical Measures for UGC Websites. *Columbia Journal of Law & Arts*, 34, 283-315.
- Garcia, K. (2020, June 5). Contracts & Copyright: Contemporary Musician Income Streams. *The Oxford Handbook of Music Law and Policy*(Research Paper No. 20-32), Forthcoming. doi:10.2139/ssrn.3620401
- Geddes, K. (2020). Meet Your New Overlords: How Digital Platforms Develop and Sustain Technofeudalism . *Columbia Journal of Law and the Arts*, 43.
- Gray, J. (2017). Governed by Google: Algorithmic enforcement and private copyright regulation. Sydney: Allens Hub for Technology, Law & Innovation University of New South Wales.
- Husovec, M., & Van Dongen, L. (2017). Website Blocking, Injunctions and Beyond: View on the Harmonization from the Netherlands. *Journal of Intellectual Property Law & Practice*, 12(8), 695–77.
- Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263-291. doi:10.2307/1914185
- Karaganis, J., & Urban, J. (2015, September). The Rise of the Robo Notice. *Communications of the ACM*, 58(9), 28-30. Retrieved from

<https://cacm.acm.org/magazines/2015/9/191182-the-rise-of-the-robot-notice/fulltext>

- Kuczerawy, A. (2019). From 'Notice and Take Down' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression. In G. Frosio (Ed.), *The Oxford Handbook of Intermediary Liability Online*. Oxford University Press.
- Langvardt, K. (2017). Regulating Online Content Moderation. *Georgetown Law Journal*, 106(5). Retrieved from <https://papers.ssrn.com/abstract=3024739>
- Le Merle, M., Le Merle, T., & Engstrom, E. (2014). *The Impact of Internet Regulation in early stage investment*. Fifth Era LLC. Retrieved from <https://static1.squarespace.com/static/571681753c44d835a440c8b5/t/572a35e0b6aa60fe011dec28/1462384101881/EngineFifthEraCopyrightReport.pdf>
- Leistner, M. (2020, May 21). European Copyright Licensing and Infringement Liability Under Art. 17 DSM-Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Opportunity Instead of a Local Challenge? *Zeitschrift für Geistiges Eigentum/Intellectual Property Journal (ZGE/IPJ)*, Forthcoming. doi:<https://ssrn.com/abstract=3572040>
- Mac Síthigh, D. (2019, October). The road to responsibilities: new attitudes towards Internet intermediaries. *Information & Communications Technology Law*. doi:10.1080/13600834.2020.1677369
- Manara, C. (2018, 11 7). *Protecting what we love about the internet: our efforts to stop online piracy*. Retrieved 2 4, 2020, from [blog.google.com: https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/](https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/)
- Mann, R., & Belzley, S. (2005). The promise of Internet Intermediary Liability. *William and Mary Law Review*, 274-5.
- Mazziotti, G. (2020). *A Data-Driven Approach to Copyright in the Age of Online Platforms*. European University Institute, Department of Law. Badia Fiesolana: European University Institute. doi:10.2139/ssrn.3655027
- Merges, R. P. (2018). What Kind of Rights Are Intellectual Property Rights? . In R. Dreyfuss, & J. Pila (Eds.), *Oxford Handbook of IP Law*. Oxford University Press. Retrieved from <https://ssrn.com/abstract=2959073>
- Mostert, F., & Lambert, J. (2019, July 23). *Study on IP Enforcement Measures, Especially Anti-Piracy Measures in the Digital Environment*. World Intellectual Property Organization, Advisory Committee on Enforcement. Geneva: World Intellectual Property Organization. Retrieved from <https://ssrn.com/abstract=3538676>

- OECD. (2011). The Role of Internet Intermediaries in Advancing Public Policy Objectives. *Public Policy*. Organization for Economic Cooperation and Development.
- Perel (Filmar), M., & Elkin-Koren, N. (2016, February 21). Accountability in Algorithmic Copyright Enforcement. *Stanford Technology Law Review*, 473. doi:10.2139/ssrn.2607910
- Perel (Filmar), M., & Elkin-Koren, N. (2017). BLACK BOX TINKERING: Beyond Disclosure in Algorithmic Enforcement. *Florida Law Review*, 181. doi:10.2139/ssrn.2741513
- Quintais, J. P. (2018). *Global Online Piracy Study Legal Background Report*. Amsterdam: Insitute for Information Law (IViR), Faculty of Law, University of Amsterdam.
- Riordan, J. (2013). The liability of internet intermediaries. Magdalen College, Oxford.
- Romero Moreno, F. (2019). 'Notice and staydown' and social media: amending Article 13 of the Proposed Directive on Copyright. *International Review of Law, Computers & Technology*, 33(2), 187-210. doi:10.1080/13600869.2018.1475906
- Romero Moreno, F. (2020). 'Upload filters' and human rights: implementing Article 17 of the Directive on Copyright in the Digital Single Market. *International Review of Law, Computers & Technology*, 34(2), 153-182. doi:10.1080/13600869.2020.1733760
- Samuelson, P. (2020, June 12). Pushing Back on Stricter Copyright ISP Liability Rules. *Michigan Technology Law Review*, Forthcoming. Retrieved from <https://ssrn.com/abstract=3630700>
- Samuelson, P. (2020, March 10). Regulating Technology Through Copyright Law: A Comparative Perspective. *European Intellectual Property Review*. Retrieved from Available at SSRN: <https://ssrn.com/abstract=3635094>
- Sartor, G. (2017). *Providers Liability: From the eCommerce Directive to the future*. European Parliament, Policy Department A: Economic and Scientific Policy. Brussels: Directorate General For Internal Policies.
- Schwemer, S. F. (2020, June 1). Article 17 at the Intersection of EU Copyright Law and Platform Regulation. *Nordic Intellectual Property Law Review*(3/2020). Retrieved from <https://ssrn.com/abstract=3627446>
- Schwemer, S. F., & Schovsbo, J. (2020). , What is Left of User Rights? – Algorithmic Copyright Enforcement and Free Speech in the Light of the Article 17 Regime. In P. Torremans, & 4th (Ed.), *Intellectual Property Law and Human Rights*. Wolters Kluwer.

- Seng, D. K. (2015). 'Who Watches the Watchmen?' An Empirical Analysis of Errors in DMCA Takedown Notices. doi:10.2139/ssrn.2563202
- Smith, M., & Telang, R. (2008). *Competing with Free: The Impact of Movie Broadcasts on DVD Sales and Internet Piracy* . doi:10.2139/ssrn.1028306
- Smith, M., & Telang, R. (2012). Assessing the Academic Literature Regarding the Impact of Media Piracy on Sales. doi:10.2139/ssrn.2132153
- Sobel, B. (2017). Artificial Intelligence's Fair Use Crisis. *The Columbia Journal of Law & The Arts*, 45-97.
- Spoerri, T. (2019). On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market. *Journal of Intellectual Property, Information Technology and E-Commerce Law*. Retrieved from <https://www.jipitec.eu/issues/jipitec-10-2-2019/4914>
- Strzelecki, A. (2018). Website removal from search engines due to copyright violation", Aslib. *Aslib Journal of Information Management*.
- Trapman, L. (2016, December 14). *American and European safe harbours*. Retrieved from Kluwer Copyright Blog: http://copyrightblog.kluweriplaw.com/2016/12/14/american-european-safe-harbours/?doing_wp_cron=1598537110.1808159351348876953125
- University, C. (2012). *SABAM v. Netlog NV, Case C-360/10*. Retrieved from Global Freedom of Expression, Columbia University: <https://globalfreedomofexpression.columbia.edu/cases/ecj-sabam-v-netlog-nv-case-c%E2%80%9136010/>
- Urban, J., Karaganis, J., & Schofield, B. (2017). *Notice and Takedown in everyday practice*. UC Berkley Public Law Reasearh . Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628