HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

The Intermediary Liability Conundrum: Are Safe Harbors Useful?

Wilhelm Sanmark

Helsinki 2021

Master's thesis supervised by Marcus Norrgård

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Abstract

Faculty: Faculty of Law
Degree programme: Master of Laws
Study track: Master's Programme in Law
Author: Wilhelm Sanmark
Title: The Intermediary Liability Conundrum: Are Safe Harbors Useful?
Level: Master's thesis
Month and year: April 2021
Number of pages: 73
Keywords: online intermediary, liability, digital content, service provider, notice-and-takedown, content filtering, blocking, safe harbor
Where deposited: University of Helsinki, Faculty of Law
Abstract:
Whether online intermediaries should be held responsible for user-uploaded content is one of the earliest conundrums of Internet law. Since the 1990s, the prevailing model has been to exempt online intermediaries from liability for third-party infringements as long as they conform to certain conditions. Recently, calls to expand intermediary liability has intensified both in the U.S. and the EU. Adversaries of the safe harbor regulation claim that the current laws have gone too far and favor intermediaries unfairly.

The aim of the thesis is to analyze the validity of the calls to abolish safe harbors. The intent is to do so by investigating how the safe harbors work, why they exist, how they will develop in the future, and what to consider if the procedures were to be changed. The methods chosen are doctrinal research and comparative analysis. The reason for using both methods is that it will provide a deeper understanding of why safe harbors exist and additional arguments for the analysis. I have chosen to compare the U.S. and the EU intermediary liability regimes because of the vast amount of information available, their close historical ties, and the relevance of respective markets.

The question of whether intermediary liability safe harbors should exist or not boils down to which fundamental rights the legislators want to emphasize and protect. All of the involved parties have their own set of competing interests and any decision is going to favor someone. There are three ways to go about changing how intermediary liability works. The first option is to provide intermediaries complete insulation from liability, the second option is to introduce safe harbors that are conditional or to adjust existing conditions, and the third option is to introduce strict liability to intermediaries. The first two options already exist in the U.S. and are proven to work. The procedures are not flawless, but at least they conform to fundamental rights fairly well. Introducing strict liability to intermediaries would more than likely lead to ex-ante content blocking, thus violating freedom of expression to an unjustifiable extent.

Table of Contents

List of Abbreviations

ACLU	American Civil Liberties Union
CDA	Communications Decency Act
CJEU	Court of Justice of the European Union
DMCA	Digital Millennium Copyright Act
DSA	Digital Services Act
DSMD	Directive on Copyright in the Digital Single Market
ECD	Electronic Commerce Directive
ECJ	European Court of Justice
OCILLA	Online Copyright Infringement Liability Limitation Act
WIPO	World Intellectual Property Organization

1 Introduction

1.1 Background

Whether online intermediaries should be held responsible for third-party content is one of the earliest conundrums of Internet law.[1] Two U.S cases in the early 1990s with paradoxical outcomes made it apparent that the issue needed to be addressed sooner rather than later. The prevailing model ever since, has been that online intermediaries are exempt from liability for third-party content as long as they act as passive distributors.[2] If the online intermediary is involved in creating the content, it will generally be considered a publisher and thus will not qualify for the safe harbors. The safe harbors were first introduced in the U.S. and soon after the EU followed suit.[3] However, there are a few significant differences between the U.S. and the EU safe harbor schemes which will be analyzed in this thesis.

Recently, the debate about increased intermediary liability has intensified both in the U.S. and the EU.[4] The calls to repeal existing safe harbors seems to emanate from a variety of entities with distinct incentives. The general belief among adversaries of the safe harbor regulation, is that current laws have gone too far and favor intermediaries unfairly.[5] Perhaps, the most fervent opponents of the safe harbor policies are copyright holders that argue for the existence of a "value gap".[6] The controversial concept of value gap, refers to an alleged imbalance between how much online intermediaries are making on user-uploaded content compared to the rightsholders.[7] According to the theory, rightsholders are forced to accept low royalty rates because online intermediaries can otherwise simply turn down license deals and exploit the protection provided by the safe harbors.[8]

The other key argument for increased intermediary liability is tackling "hate speech" and "fake news" (misinformation). The expression "hate speech" is ambiguous to say the least, but

[1] Edwards 2019, p. 255.
[2] Savin 2017, p. 144.
[3] Frosio 2017a, p. 24.
[4] Savin 2017, p. 144.
[5] Elkin-Koren et al. 2019, p. 9.
[6] Obergfell – Thamer 2017, p. 435.
[7] Rosati 2019, p. 200–201.
[8] Elkin-Koren et al. 2019, p. 4.

essentially, the increasingly aware Internet culture is pushing for restrictions on "public speech that expresses hate or encourages violence toward a person or group based on something such as race, religion, sex, or sexual orientation".[9] Misinformation on the Internet became a hot topic during Donald Trump's presidency due to his active use of Twitter for expressing thoughts. Especially in the U.S., the concern has been that misinformation would affect, among other things, political elections, and people's perception of vaccines and COVID-19.

Clearly, the power balance between the different parties involved has shifted dramatically since the creation of the safe harbors. The user volumes have increased exponentially, giving online intermediaries unprecedented power and influence.[10] Whereas the early legislation on online intermediary liability was intended to stimulate the growth of electronic commerce, the debate has nowadays turned upside down. The current concern is that the platforms are becoming too powerful, and governments are trying to find ways of controlling them. By 2015, the largest listed online platforms had a market capitalization of USD 3.9 trillion and the number has only grown since then.[11] Online intermediaries have an essential role in enabling the flow of information and consequently protecting, among other things, freedom of expression which is a fundamental right guaranteed by law in most of the world, including the U.S. and the EU.[12] This puts them in a unique position where they can prevent or mitigate damage inflicted by their users, which is ultimately the main reason why there are calls to increase their liability.[13]

The growing power of online platforms is not only a national concern, but also a global concern due to their transborder influence.[14] However, it also works the other way around; the online intermediaries have to abide by the laws of each jurisdiction they operate in.[15] It appears to be in the interest of all relevant parties to find a working solution to the online intermediary liability

[9] Cambridge Dictionary "hate speech" definition. Retrieved April 11, 2021, from https://dictionary.cambridge.org/us/dictionary/english/hate-speech
[10] Edwards 2019, p. 256.
[11] European Commission, Staff Working Document Online Platforms, SWD (2016) 172, p. 1.
[12] Geiger et al. 2020, p. 140; U.S. Const. amend. I; Article 10 ECHR; Article 11 EU Charter. Freedom of expression not only guarantees the right to impart information but also the right of the public to receive it. With the increased importance of the Internet as a source of information and a means to express thoughts, the freedom of expression has in the recent years evolved towards a right to internet access.
[13] Savin 2017, p. 143.
[14] Elkin-Koren et al. 2019, p. 14.
[15] Frosio 2017a, p. 17.

issue. What is indisputable is that liability of online intermediaries is currently hotly debated, and it deserves further examining.[16]

1.2 Objective and Scope

The calls to repeal the online intermediary safe harbors in the U.S. and the EU have intensified during recent years. The purpose of this thesis is to analyze the validity of such demands. This will be accomplished through a multistep process. Firstly, I will investigate how the online intermediary safe harbors work and why they exist in the U.S. and in the EU. In order to answer the question whether they should be repealed or not, I believe the most sensible approach is to first understand how the safe harbors work and why they were enacted in the first place. Secondly, I will examine why the safe harbors differ from each other. Given that they are dissimilar, there must be advantages and disadvantages to one system over another. Thus, the intent is to identify and compare those differences. In the end, I will compile and analyze the arguments for and against, isolating intermediaries from liability from a universal perspective. Additionally, I will evaluate a few key features of the safe harbor policies with the intention of distinguishing which aspects of them work and which could be improved upon. In conclusion, the objective is to provide insight concerning how the safe harbors work, why they exist, how they will develop in the future, and what to be mindful of if the procedures were to be changed.

In a study with a wide subject matter such as this, it is essential to make pragmatic delimitations. The territorial delimitation is the first dilemma. Online intermediary liability is an area of law which is harmonized within the EU, meaning that the legislation in its member states is based on Union law. The research will thus be focused on EU legislation rather than national legislation of the member states. In order to understand why the safe harbors were created in the EU, it is necessary to also examine U.S. legislation. Not only does the U.S. legislation provide answers as to why the EU adopted safe harbor regulation, it also provides a rich history of relevant case law as well as written law, which serves superbly for a comparative analysis. Furthermore, the U.S. is home to a majority of the world's largest online intermediaries rendering it an interesting and relevant market to study.

[16] Hartmann-Vareilles 2017, p. 3.

The second delimitation concerns which statutes will be examined. Both the U.S. and the EU are brimming with legislation. In order to keep the research on track, it is necessary to choose a few relevant statutes to examine. Intermediary liability touches on countless areas of law and it is unquestionably impossible to cover all of them in this thesis. I decided to start with the Electronic Commerce Directive (ECD)[17], which is historically the main piece of legislation on online intermediary liability in the EU. It was found that the comparable legislation in the U.S. is split into two separate laws, Section 230[18] and the Digital Millennium Copyright Act (DMCA)[19]. Essentially, the DMCA regulates copyright infringements and Section 230 regulates the rest, whereas in the EU, the ECD regulates all of it. By this logic, I established the three core statutes I would work with. Nonetheless, the EU is in the process of creating and implementing a substantial quantity of new legislation which cannot be completely disregarded. Above all, there has been a lot of debate about the recent Directive on Copyright in the Digital Single Market (DSMD)[20]. By the time of writing this, the directive has come into force, but it has not yet been implemented by the member states. With that in mind, I will cover what the DSMD means for European online intermediary liability, to the extent it is relevant for my research questions. There is also new legislation on the horizon that is noteworthy. The European Commission submitted a legislative proposal with the title "Digital Services Act" (DSA) to the European Parliament and the European Council on December 15, 2020.[21] The DSA will only be touched upon briefly due to how early in the process the law currently is and the uncertainty of its final form if it passes. It cannot be emphasized enough that the legislation I chose to analyze does not cover all of the intermediary liability legislation. It is simply a pragmatic delimitation that hopefully yields valuable viewpoints on the topic of online intermediary liability.

Lastly, I had to consider what kind of infringements that are best to include in the research. I decided not to delimit the research to any specific infringements, instead the focus is on online intermediary liability for all third-party infringements. The decision was ultimately relatively straightforward since the ECD plays a central role in my research, and unlike its U.S.

[17] Directive 2000/31/EC.
[18] 47 U.S. Code § 230.
[19] Pub.L. 105-304 -- October 28, 1998 -- To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.
[20] Directive 2019/790
[21] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

counterparts, the ECD does not only apply to certain specific infringements. Not to delimit online intermediary liability research to specific infringement also seems to be the standard among scholars. Such delimitation would be arbitrary, unless the research had a more specific focus, which it does not.

1.3 Research Methods and Material

In the previous chapter I explained largely the method I intend to utilize in this thesis. Nonetheless, I will further elaborate on my choice of research method. As my research methods, I will be using doctrinal research and comparative analysis. Considering the research questions, neither method would give a satisfactory result on their own. Instead, I will be analyzing each legal system separately through the doctrinal research method, and finally, in the analysis chapter, I will conduct text-by-text comparative analysis and combine it with some *de lege ferenda* arguments.

The purpose of the doctrinal research method is to give a systematic exposition of the principles, rules and concepts governing online intermediary liability and to analyze the relationship between them with a view to solving ambiguities and gaps in the existing law.[22] Especially *ratio legis* will be of interest, considering the research questions. Understanding the reasons for the law, will undoubtedly provide arguments for the analysis. The first goal is to describe the existing law, in order to lay a solid foundation of understanding.[23] The method also encompasses a search for practical solutions.[24] This will be accomplished through the use of conventional material such as articles, books, reports, case law, statutes etc. The rich use of case law, especially the older case law, can be explained by the interest in *ratio legis*. Court decisions are usually ample in reasoning and are thus a valuable asset for the research. For the analysis, I will utilize plenty of legal literature by scholars, since standing on the shoulders of giants is essential for thorough research. To add another layer of depth, I will juxtapose the safe harbor policies with each other, which will hopefully yield additional arguments for the conclusion. The comparative method can present a new perspective, allowing to critically illumine the compared legal

[22] Watkins – Burton 2017, p. 13; Smits 2015, p. 5.
[23] Smits 2015, p. 8.
[24] *Id.*at p. 10.

systems.[25] Since the research is intended to examine both the U.S. and the EU safe harbors in depth, it is reasonable to talk about comparative analysis, rather than utilizing foreign legislation for the sake of arguments.[26]

1.4 Terminology

The subject of online intermediary liability encompasses a plethora of ambiguous terminology. The most significant bewilderment pertains to the vast number of synonyms, or near synonyms, that the word "intermediary" has. Interactive computer service, information content provider, online service provider, internet service provider, online platform, user-generated content platform, information society service, online content-sharing service provider, intermediary, distributor, and publisher are only a few examples of the seemingly endless number of synonyms. Some of the words mean more or less exactly the same, some are hypernyms, and some have crucial nuance differences. The intention is to keep the text as reader-friendly as possible, meaning that I aim to be as consistent as possible with the choice of terminology. Exceptions will be made in quotations or if it is otherwise necessary.

The other problem is how to define those words.[27] The fact is, that a uniform definition of online intermediary does not exist, as there is no consensus among professionals or legislators, as to what such definition should include.[28] Each statute that attempts to define one of those synonyms, have different definitions. The use of those words is not uniform even within the U.S. or the EU. Part of the reason why there is no agreement about what exactly those words mean, is that it would have considerable legal implications. If the law dictates that publishers are liable for third-party infringements, but distributors are not, then the definition of publisher and distributor is of paramount importance. This thesis will not aim to redefine or classify the terminology.

[25] Legrand 1995, p. 13.
[26] Strömholm 1971, p. 252.
[27] *See* Bostoen 2018, p. 3.
[28] Rozenfeldova – Sokol 2019, p. 868.

2 Intermediary Liability in the U.S.

2.1 Early Development towards Intermediaries' Insulation from Liability

The early case law certainly predates the online era. However, even the safe harbor policy that we have today stems from the early cases. The focus has shifted over time from television and radio broadcasters to online intermediaries, but the legal reasoning has largely remained the same. Intermediary liability was not regulated by the EU prior to the year 2000, by which most countries in the EU had little to no legislation or case law pertaining to it. The U.S. on the other hand, has for more than a half century recognized by decisions of the U.S. Supreme Court, that intermediaries have some degree of insulation from liability.[29] None of the present-day legislation was invented overnight, instead it has been an extensive process to develop the safe harbor policy that we have today. In order to understand why safe harbor policies exist today, it is necessary to begin by looking back to a couple cases regarding a local broadcasting station and a bookstore in the 1950s in the U.S.

2.1.1 First Amendment Concerns

The 1956 U.S Senate race in North Dakota appeared to be a regular Senate race with the two top candidates being Republican Milton Young and Democrat Quentin Burdick. However, a week before the election, Arthur C. Townley, a legally qualified independent candidate, gave an inflammatory speech broadcasted by the radio and television station WDAY. Townley was a former socialist organizer that had founded the Nonpartisan League, a political party that advocated for the government to take over agricultural businesses. He was infamous throughout the state for his contentious rhetoric. After numerous unsuccessful political campaigns and business efforts Townley eventually denounced socialism and took a strong stance against communism in the 1950s, while targeting the leaders of the Farmers Union. Townley became a fervent follower of the Senator Joseph McCarthy who claimed that communists worked for the federal government.[30]

[29] Kosseff 2019, p. 10.
[30] *See* Arthur C. Townley, Encyclopedia of the Great Plains. Retrieved January 13, 2021, from http://plainshumanities.unl.edu/encyclopedia/doc/egp.pd.052; Section 2: Origins of the nonpartisan league, North Dakota Official State Website. Retrieved January 15, 2021, from https://www.ndstudies.gov/gr8/content/unit-iii-waves-

During the 1956 U.S Senate race in North Dakota, WDAY had broadcast speeches by both Young and Burdick. Townley claimed that WDAY should provide him with the same opportunity that the other candidates had been granted, to broadcast his speech. Pursuant to section 315 of the federal Communications Act of 1934, any broadcaster that allows a candidate to broadcast a message "shall afford equal opportunities to all other such candidates" for the office. The law also mandates that the broadcaster "shall have no power of censorship" regarding the things they air under the equal time requirement.[31] WDAY believed that § 315 of the Federal Communications Act of 1934 barred them from removing defamatory statements contained in speeches broadcast by legally qualified candidates for public office, thus they broadcast Townley's speech.

Townley's speech was a reply to previous speeches made by Senate candidates Young and Burdick. WDAY's managers realized that Townley's speech would be divisive, and they even warned Townley that his speech might be defamatory if he could not prove his claims to be true.[32] Townley's speech accused Young, Burdick and the Farmers Educational and Cooperative Union of America of conspiring to establish "a Communist Farmers Union Soviet." Here is an evocative quote from Townley's speech:

> "For ten years, Senator Young has used the power and prestige of the high office that he holds to serve this Farmers Union. He has not raised his voice or hand to stay the communist viper gnawing at your private ownership and liberty. On the contrary, Young says everything and does everything the Farmers Union tell him to do or say".[33]

Young went on to win reelection with more than 60 percent of the vote, while Townley received less than half a percent of the vote.[34] Despite Townley's lack of success in the election, his speech attracted some attention. Shortly after the election, the North Dakota Division of the Farmers Education and Cooperative Union of America filed a defamation lawsuit against not only Townley, but also WDAY for broadcasting the speech. The union sought $150,000 from

---

development-1861-1920/lesson-4-alliances-and-conflicts/topic-7-nonpartisan-league-and-iva/section-2-origins-nonpartisan-league; Kosseff 2019, p. 12.

[31] Farmers Educ. & Co-op. Union v. WDAY, Inc., 360 U.S. 525 (1959).

[32] Kosseff 2019, p. 12.

[33] Complaint, Farmers Educational and Cooperative Union of America, North Dakota Division v. Townley, District Court of Cass County, North Dakota (Jan. 14, 1957).

[34] 1956 North Dakota U.S. Senate Election results. Retrieved January 19, 2021, from https://clerk.house.gov/member_info/electionInfo/1956election.pdf

both Townley and WDAY, arguing that by broadcasting the speech and allowing Townley to use their facilities, WDAY was equally liable for harm to the union's reputation.[35]

Both the District Court of Cass County, North Dakota and the Supreme Court of North Dakota dismissed the claims against WDAY. Judge John C. Pollock of the District Court of Cass County argued that WDAY's participation was limited to "the mechanical preparation, taping, and recording of the script and film" because federal statute required WDAY to broadcast Townley's speech without censoring it in any way.[36] The union appealed to the Supreme Court of North Dakota, which affirmed the trial court's dismissal with comparable arguments. J. Lee Ranking, who was the U.S. solicitor general at the time, urged the U.S. Supreme Court to hear the case in order for the court to adopt the government's position regarding the federal communications law. The U.S. Supreme Court agreed to review the North Dakota court's ruling. [37]

The question that the U.S. Supreme Court had to resolve was whether the Federal Communications Act of 1934 prohibits a broadcasting station from removing defamatory statements in speeches given by legally qualified candidates for office or not. If so, does the station have federal immunity from liability for defamatory statements in the broadcast?[38]

One of the most debated topics of the oral arguments was the role and nature of broadcasters versus printed media. At one point during the oral arguments, Justice Felix Frankfurter asked Douglas A. Anello, a representative of the National Association of Broadcasters, if newspapers had to put in any ads that they were offered. "It does not sir and that brings us to my second point. Petitioner would equate us with newspapers insofar as they say that newspapers are held liable without fault, but it is one thing sir to argue liability without fault, but quite another to argue liability without control. Newspapers may print what they please, they may excise, they may edit. They have no regulatory body to whom they must account every three years, nor any Section 315 telling them what they may or may not do.", Anello replied to Judge Frankfurter.

---

[35] Complaint, Farmers Educational and Cooperative Union of America, North Dakota Division v. Townley, District Court of Cass County, North Dakota (Jan. 14, 1957); Kosseff 2019, p. 13.
[36] Demurrer, Farmers Educational and Cooperative union of America, North Dakota Division v. Townley, District Court of Cass County, North Dakota (May. 23, 1957); Farmers Educational and Cooperative Union of America, North Dakota Division v. WDAY, 89 NW 2d 102, 110 (N.D. 1958).
[37] Kosseff 2019, p. 14.
[38] Farmers Educational & Cooperative Union of America v. WDAY, Inc. (n.d.). Oyez. Retrieved January 3, 2021, from https://www.oyez.org/cases/1958/248

The defendants were keen on driving home the point of broadcasters lacking the same kind of editorial control that newspapers have.[39]

Three months after the oral argument, Justice Hugo L. Black, an adamant defender of the First Amendment delivered the opinion of the 5-4 majority. The Court held that the Federal Communications Act of 1934 prohibited any censorship of political speeches that were mandated by the federal equal time rule, effectively immunizing broadcasting stations from any lawsuits stemming from those speeches. Allowing broadcasting stations to censor the content of the speech would quite clearly undermine the purpose of the Act, as the Act mandates that "licensee[40] shall have no power of censorship over the material broadcast".[41] The Act does not explicitly grant the broadcasting station immunity, but since they are not allowed to censor the speech in any way it is not reasonable for them to be liable for defamatory statements made in the speech. Furthermore, the Federal Communications Commission, the body in charge of administering the Act, has since 1948 continuously held that licensees cannot remove allegedly libelous matter from speeches by candidates. "The legislative history of the measure, both prior to its first enactment in 1927 and subsequently, shows a deep hostility to censorship either by the Commission or by a licensee.", Justice Black concluded in the majority opinion.[42]

The dissenting Justices, led by Felix Frankfurter, argued that the Communications Act of 1934 was intended to bar only federal, and not state libel prosecutions. "If § 315 could be construed to contain implicitly, between the lines, a grant by Congress of immunity from state libel laws, the Court's result would follow. But it is not possible to find such implied grant of immunity. It is common ground that an express provision granting such immunity was excised from the bill which later became the Radio Act of 1927 and repeated attempts in later revisions of the Act to introduce similar provisions have failed.", wrote Frankfurter in the opinion.[43] Justice Frankfurter approached the case from an entirely different angle than Justice Black. Justice Black focused on the freedom of speech and reasonable treatment of the broadcaster. By contrast, Justice Frankfurter was more focused on what the congress had intended when drafting the law. Justice

[39] Farmers Educational Transcript. Retrieved January 3, 2021, from https://www.oyez.org/cases/1958/248
[40] Licensee refers to the broadcasting station in this context.
[41] Farmers Educ. & Co-op. Union v. WDAY, Inc., 360 U.S. 525 (1959) at 526.
[42] *Id.* at 528.
[43] *Id.* at 536.

Frankfurter further argued that precedent set by the Court supports the view that the state laws stand, unless federal laws explicitly intercede.[44]

The Farmers Educational & Cooperative Union of America v. WDAY, Inc. ruling marks the U.S. Supreme Court's first clear recognition of the need to protect intermediaries in addition to the speakers. The majority opinion does not explicitly mention the First Amendment, but it is an unambiguous statement that the freedom of speech needs to be protected and consequently, so do intermediaries. The ruling provides two significant clarifications for interpreting section 315 of the Communications Act of 1934. First, the ruling reflects the U.S. Supreme Court's desire to avert intermediaries from censoring content by third parties. Second, the ruling creates a strong presumption for intermediaries to be exempt from liability for third-party content since they do not have to right to censor the content. Still to this day the aforementioned logic applies, and the modern safe harbor policies are based on it.[45]

2.1.2 Knowledge is Power …and Liability

On November 19, 1956, police arrested William Rothweiler, an employee of Eleazar Smith's bookstore. In the end, prosecutors charged Eleazar Smith. Smith was a Polish immigrant in his seventies and the owner of the bookstore in Los Angeles' skid row. At the time Los Angeles had an ordinance that prohibited certain businesses from possessing obscene material. Section 21.01.1 of the Los Angeles Municipal Code stated: "It shall be unlawful for any person to have in his possession any obscene or indecent writing, book, pamphlet, picture, photograph, drawing . . . in any place of business where ice-cream, soft drinks, candy, food, school supplies, magazines, books, pamphlets, papers, pictures or postcards are sold or kept for sale."[46] Rothweiler had sold the book *Sweeter Than Life,* by Mark Tryon, to an undercover officer. *Sweeter Than Life* would by today's standards certainly not be considered obscene. However, the book depicts graphically sex, even sex between members of the same gender, which in the 1950s was widely frowned upon.[47]

[44] Conclusion, Farmers Educational & Cooperative Union of America v. WDAY, Inc. (n.d.). Oyez. Retrieved January 4, 2021, from https://www.oyez.org/cases/1958/248
[45] Kosseff 2019, p. 16–17.
[46] Smith v. California, 361 US 147, 172 n.1 (1959).
[47] Kosseff 2019, p. 19–20.

There were two main questions that needed to be answered: was *Sweeter Than Life* or any other literature sold in the bookstore considered obscene and could Smith be held liable as a passive distributor if the book were considered obscene?

Both the Los Angeles Municipal Court and the Appellate Department of the Superior Court of Los Angeles County held that Smith was guilty of violating the obscenity ordinance by selling *Sweeter Than Life.* The judges were appalled by the graphic language used in the book. "The effect on me was one of depression," said Judge Pope from Los Angeles Municipal Court after reading the book. It was evident that the judges' minds were made up about the obscenity of the book and requests to bring in expert witnesses were denied. The remaining question was then: could Smith be held liable even if he did not know about the book? Smith and his attorney Stanley Fleishman argued that Smith's bookstore had thousands of books and there was no way for Smith to know about their content. Smith did not even choose the books in his store; they were bought in bulk from publishers. Smith was sentenced to 30 days in city jail. A divided three-judge panel of the Appellate Department of the Superior Court of Los Angeles County affirmed Smith's conviction. The Court held that the city's obscenity ordinance does not require the bookseller to be aware of the obscene material in order to be held criminally liable. The dissenting judge noted that there was a similar state obscenity law, but with the key difference that it only applied to those who "willfully and lewdly" sold obscene materials. He further reasoned much like the defendant, that the vendor cannot possibly know about the content of every book sold.[48]

Smith's attorneys appealed the decision to the U.S. Supreme Court. Their key argument was that Smith lacked scienter. He had no intent nor knowledge of illegality. They further argued that if the ordinance in fact imposed a strict criminal liability, it would come into conflict with the Due Process Clause in the Fourteenth Amendment of the United States Constitution. Additionally, they argued much like in the lower courts, that *Sweeter Than Life* was not obscene. The arguments presented at the Supreme Court were diverse. Roger Arnebergh, the Los Angeles City Attorney took quite a different approach. He essentially made three distinct arguments. First of all, according to him, the city's obscenity ordinance had not stifled freedom of speech.

[48] State v. Smith, Superior Court No. CR A 3792, Trial Court No. 57898 (Cal. Ct. App. June 23, 1958).

The ordinance had existed for a long time and Los Angeles still had plenty of bookstores, said Arnebergh. Secondly, Arnebergh argued that it was unreasonable having to prove that the defendant knew about the obscenity of the book that was sold. If that was the case, then it would be easier to avoid liability by having a bigger bookstore. The more books there are, the harder it is to prove that the owner knows about the content of the books. Lastly Arnebergh pivoted to a peculiar argument. His fundamental argument was that since copyright law protects books, books are property and not speech, and shall therefore not be protected by the First Amendment.[49]

Arnebergh's last argument turned out to be a mistake. The Supreme Court decided unanimously for Smith. The Supreme Court issued five different opinions, a majority opinion, three concurring opinion and one dissenting opinion. All justices, except for Harlan, agreed that the obscenity ordinance had a chilling effect on speech and thus violated the Constitution. Justice Brennan, who delivered the majority opinion, argued that a bookseller, such as Smith could not be held criminally liable without scienter. The First Amendment fundamentalists Black and Douglas argued that restriction on speech was unconstitutional regardless of scienter. Justice Frankfurter noted that a distributor should not be exempt from liability if he insulates himself against knowledge about an illegal book. Harlan agreed that Smith's conviction should be overturned, but not because of the unconstitutionality of the ordinance. Instead, Harlan reasoned that the appellant's evidence and testimony should have been admitted. "This had the effect of depriving appellant of the opportunity to offer any proof on a constitutionally relevant issue", wrote Harlan in the dissenting opinion. Arnebergh's copyright argument was not even mentioned in the majority opinion. Unlike the lower courts, the Supreme Court was not particularly interested in discussing the obscenity of *Sweeter Than Life.* At core, it was a case about intermediary liability and freedom of expression.[50]

Despite the conflicting views among the justices, eight out of nine agreed with the majority opinion which stands to this day: under the protection of the First Amendment content distributors cannot be held liable for third-party content, unless they knew or had reason to know about

[49] Oral Argument Transcript, Smith v. California, 361 U.S. 147 (1959). Retrieved January 26, 2021, from https://www.oyez.org/cases/1959/9
[50] Smith v. California, 361 U.S. 147 (1959).

the infringing content.[51] The rule applies to more than just obscenity and bookstores. It applies to all intermediaries and covers for instance also defamation. A modern example would be a webpage that lets users post content. If the service provider does not know about, for example, defamatory content uploaded by a user, it is not liable by the rule established by Smith v. California.[52]

However, the Supreme Court did not resolve all problems concerning intermediary secondary liability. The Smith v. California rule led to an absurd situation, where intermediaries might reduce their risk of liability by insulating themselves from knowledge about illegal content. It is precisely what Justice Frankfurter tried to prevent from happening. "The Court does not hold that a bookseller who insulates himself against knowledge about an offending book is thereby free to maintain an emporium for smut."[53], Frankfurter wrote in his concurring opinion. Still, that was only Frankfurter's opinion, and it would take almost half a century to finally settle the issue.[54]

2.1.3 Illustrating the Smith Rule

The Smith v. California rule creates a strong incentive for intermediaries to take a hands-off approach regarding the content they distribute to the public.[55] The less they know, the lower the risk of liability is. Briefly examining three defamation cases, involving stores selling pornographic content, will clearly illustrate how the Smith v. California rule was later applied and what the limitation of it were.

In the early 1980s, Kenneth Osmond, a former child television star, sued EWAP, owner of the adult book and video store Le Sex Shoppe. One of the movies that the L.A.-based Le Sex Shoppe sold was titled *Supercock*. The cover of the cassette implicitly claimed that the movie starred Osmond. At the time, Osmond was a Los Angeles Police Department officer. Osmond was baffled when LAPD's internal affairs department began questioning him about the movie. When he realized what was going on, he decided to sue EWAP for libel. The case is in many ways

[51] Kosseff 2019, p. 27.
[52] *Ibid.*
[53] Smith v. California, 361 U.S. 147 (1959).
[54] Kosseff 2019, p. 28.
[55] *Id*. at p. 30.

comparable to Smith v. California. Much like Smith had done, EWAP claimed that they were merely a passive distributor and knew nothing about the content of movies they sold. EWAP was not involved in producing or publishing any films. Their involvement ended at simply buying and selling the films. The trial judge granted summary judgment in favor of EWAP and dismissed the case. Osmond appealed but the dismissal was unanimously upheld. The conclusion was clear, Smith v. California had set a precedent that was followed. However, the Court of Appeals of California held that "innocence is generally considered a defense where such defendants merely circulate another's libel unless 'they knew or should have known' of the defamatory nature of the material.".[56] The court recognized that a distributor "may avoid liability by showing there was no reason to believe it to be a libel".[57] In other words, the distributor cannot necessarily avoid liability through ignorance. The court left open the possibility that immunity from liability does not apply to those who turn the blind eye to illegal content.

A few years after the Osmond v. EWAP case, another similar lawsuit occurred. The circumstances were somewhat different, but the Smith v. California rule was similarly applied. This time the plaintiff was an American feminist and activist by the name of Andrea Dworkin. Dworkin was an outspoken critic of the victimizing effects of pornography on women, which made her an enemy of the porn industry.[58] Perhaps her most fervent adversary was Larry Flynt, the publisher of *Hustler*. In 1984, *Hustler* published several features about Dworkin. Dworkins action against *Hustler* arose from three of those features. One of them was "a cartoon that portrays two women apparently engaging in cunnilingus. One woman says to the other, 'You remind me so much of Andrea Dworkin, Edna. It's a dog-eat-dog world.'"[59] The problem for Dworkin was that by the 1980s, the views on pornography had radically changed, and it would be difficult to get courts to rule pornography unconstitutional. Dworkin's attorney Gerry Spence, a famous Wyoming trial lawyer, came up with the idea of utilizing his local popularity by forum shopping. He knew that it was most likely that the lawsuit would not stand a chance in California, where *Hustler* was based, so he tried to move the trial to Wyoming.[60] There was just one problem, Wyoming state court lacked jurisdiction. Spence solved the procedural

[56] Osmond v. EWAP, 153 Cal.App.3d 842, 847 (Cal. Ct. App. 1984).
[57] *Ibid*.
[58] Andrea Dworkin, Britannica. Retrieved January 29, 2021, from https://www.britannica.com/biography/Andrea-Dworkin
[59] Dworkin v. Hustler Magazine, Inc., 611 F. Supp. 781 (D. Wyo. 1985).
[60] Kosseff 2019, p. 31.

problem by having Dworkin also sue Park Place Market, a Jackson, Wyoming, store that sold *Hustler*. In 1985 the US District Court for the District of Wyoming ruled that "Because of the lack of evidence of scienter on the part of Park Place, the Court must find that in deciding the question of diversity it must ignore the presence of Park Place as being 'fraudulently joined.'".[61] Park Place's liability was evaluated much like in Smith v. California and Osmond v. EWAP. As the plaintiffs failed to prove scienter on the part of Park Place, the court denied the plaintiffs' motion to remand. The case was eventually transferred to a federal court in Los Angeles, where all claims were dismissed. The United States Court of Appeals for the Ninth Circuit affirmed the dismissal, concluding that the First Amendment protected Hustler features as "opinion" pieces.[62] This would not be the last lawsuit involving Flynt and Park Place Market.

On May 12, 1986, Spence filed a lawsuit against Flynt and Park Palace. This time Spence himself was the plaintiff. Due to Spence's decision to represent Dworkin, he was personally attacked by *Hustler* by being named "Asshole of the Month.", "vermin-infested turd dispenser", "parasitic scum-sucker", "shameless shithole" and so on.[63] The case was for the most parts nearly identical to Dworkin v. Hustler. Nevertheless, there was one key difference this time. Park Place could no longer claim ignorance regarding the content of *Hustler*. They were still involved in the previous lawsuit, making it evident that they knew about *Hustler's* controversial nature. As a result, Park Place was to be considered a legitimate defendant and the US District Court for the District of Wyoming granted the plaintiff's motion to remand. [64] Having the same judge come to the complete opposite conclusion in two almost identical cases, indubitably portrays how erratic the legal landscape was becoming with the emerging technologies. It started to become increasingly evident that something would have to be done regarding the legislation.

2.1.4 No Control, No Liability!

In the 1990s, computers and Internet became increasingly common in U.S. households. The Web as we know it today, was developed in the early 90s and became widely adopted in the late 90s. Prior to that, online service providers such as CompuServe were used to connect to the

[61] Dworkin v. Hustler Magazine, Inc., 611 F. Supp. 781 (D. Wyo. 1985).
[62] Dworkin v. Hustler Magazine, Inc., 867 F. 2d 1188 (9th Cir. 1989).
[63] Spence v. Flynt, 816 P.2d 771 (Wyo. 1991).
[64] Spence v. Flynt, 647 F. Supp. 1266 (D. Wyo. 1986).

Internet. CompuServe Information Service was a subscription-based "electronic library"[65] that among other things, hosted online bulletin boards and online versions of newspapers. The service allowed users to post comments on a wide range of different themed bulletin boards, and even to chat with each other. CompuServe adopted a hands-off approach regarding the content that was posted on their bulletin boards. Administration of the bulletin boards was generally outsourced to external contractors, such as Cameron Communications, Inc. ("CCI").[66] CompuServe had contracted CCI to administer *Journalism Forum,* one of CompuServe's bulletin boards. CCI had further subcontracted Don Fitzpatrick Associates of San Francisco ("DFA") to publish Rumorville USA ("Rumorville"), which was a daily newsletter that provided reports about broadcast journalism and journalists. CompuServe had no direct relationship with DFA, nor could they review Rumorville's content before it was uploaded to the Journalism Forum.[67]

In 1990, Robert Blanchard ("Blanchard") and his company Cubby Inc. ("Cubby") developed Skuttlebut, a computer database designed to publish and distribute electronically news and gossip in the television news and radio industries. Skuttlebut was intended to compete with Rumorville, despite the fact that Skuttlebut distributed their newsletters mainly by fax, as they were not yet affiliated with an online service provider.[68] On April 12, 1990, Rumorville published an article accusing Skuttlebut of stealing news items from Rumorville. Rumorville alleged that Skuttlebut had gained access to Rumorville's information "through some back door". The following day, Rumorville went on to claim that Blanchard had been fired from a previous job at WABC (New York ABC television affiliate) and that Skuttlebut was a "new start-up scam".[69]

Blanchard and Cubby filed a lawsuit against both Don Fitzpatrick (head of DFA) and CompuServe. The lawsuit claimed that the false statements constituted business disparagement of Cubby, libel of Blanchard, and unfair competition as to Skuttlebut, based largely upon the allegedly defamatory statements contained in Rumorville.[70] Cubby claimed that CompuServe was the publisher of the defamatory statements and should, pursuant to federal and state defamation law, also be held liable. It was the first suit on record that sought to hold an online service

[65] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[66] *Ibid.*
[67] *Ibid.*
[68] Kosseff 2019, p. 38.
[69] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[70] Complaint, Cubby v. CompuServe, 90 Civ. 6571 (S.D.N.Y. Oct. 5, 1990).

provider liable for a third-party content.[71] CompuServe did not even attempt to dispute the defamatory nature of the content. Instead, CompuServe argued that they were merely a passive distributor of Rumorville and had no ability to control what Rumorville published. The plaintiffs claimed that CompuServe did have editorial control over Rumorville. CompuServe could deny DFA from uploading content and even remove content if they wanted to. Therefore, CompuServe should be considered a publisher, not a distributor.

Judge Leisure did not agree with the plaintiffs' contention. In the court's opinion, he recognized that CompuServe could in fact choose whether they contracted DFA to provide content or not. However, once CompuServe decided to contract DFA to manage the forum and provide content, they no longer had control of the content that was uploaded. With these arguments, Judge Leisure concluded that CompuServe shall be considered a distributor, and not a publisher.[72] Judge Leisure's approach was pragmatic. He realized that the opposite conclusion would mean that online service providers would have immense liability, to the point where they probably could no longer function. After concluding that CompuServe was merely a distributor, it was only a matter of applying the correct legislation. The case was the first of its kind, so the court had to seek guidance from older precedents. "The requirement that a distributor must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment, made applicable to the states through the Fourteenth Amendment."[73], Judge Leisure wrote in his opinion. He backed up the argument by referring to Smith v. California. It was clear that the same standards that had been established several decades earlier, would still apply. The plaintiffs would have to prove that the defendants knew, or at least should have known about the defamatory content.

On October 29, 1991, the court granted summary judgement in favor of CompuServe. Judge Leisure wrote in his opinion: "Plaintiffs have not set forth any specific facts showing that there is a genuine issue as to whether CompuServe knew or had reason to know of Rumorville's contents." and "CompuServe, as a news distributor, may not be held liable if it neither knew nor had reason to know of the allegedly defamatory Rumorville statements".[74] The decision

[71] Kosseff 2019, p. 39.
[72] Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
[73] *Ibid*.
[74] *Ibid*.

eventually proved to be a double-edged sword. It effectively created a two-step test for online service providers to be insulated from liability for third-party content. First, the online service provider must not have any editorial control over third-party content in order to qualify as distributor, rather than a publisher. Second, the online service provider must not have any knowledge or reason to know of the infringing third-party content.[75] If either of these two conditions were not met, the online service provider could face liability. As a result, the decision removed any legal incentive for online service providers to monitor or moderate third-party content on their platforms. Another case involving Prodigy, one of CompuServe's largest competitors, would a few years later display how preposterous conditions Cubby v. CompuServe had created.

2.1.5 The Moderation Paradox

Three years after the Cubby v. CompuServe ruling, it was time to apply for the first time the two-step test that it had established. Nevertheless, this time the defendant was one of CompuServe's largest competitors— Prodigy. Prodigy had bulletin boards that worked similarly to CompuServe's. One of Prodigy's most notable bulletin boards was called Money Talk. In a sense, Money Talk was similar to modern forums, as users could post comments and communicate with each other. The bulletin board was nonetheless not yet on the World Wide Web. In October of 1994, a person with the username "David Lusby" posted multiple libelous messages on Money Talk about the securities brokerage Stratton Oakmont. Essentially, Lusby accused Stratton Oakmont of "criminal fraud".[76] To this day, it remains unknown who the person behind the username David Lusby was.

On November 7, 1994, Stratton Oakmont filed a lawsuit against Prodigy and "David Lusby", mostly focusing on libel and negligence. In accordance with the aforementioned two-step test, the court had to first determine whether Prodigy was a distributor or publisher. Prodigy were clearly not the ones writing the libelous posts, but they could be held liable if it were proven that they exercised editorial control. The plaintiffs had four key arguments for why Prodigy ought to be considered a publisher:

[75] Kosseff 2019, p. 42–43.
[76] Stratton Oakmont, Inc. v. Prodigy Services Co., 23 Media L Rep 1794 (Sup. Ct. Nassau Cnty. 1995).

1) Prodigy's Director of Marketing Programs and Communications had written multiple articles to national newspapers about how Prodigy holds themselves out as an online service that exercises editorial control over the content posted on their bulletin boards, thereby expressly differentiating themselves from their competition and expressly likening themselves to a newspaper.
2) Prodigy promulgated content guidelines in which they, inter alia, requested users to refrain from posting insulting comments and claimed that they would remove any content that violated their content guidelines.
3) Prodigy used a software screening program which automatically prescreened all bulletin board postings for offensive language.
4) Prodigy used Board Leaders whose duties included enforcement of the content guidelines. The Board Leaders had the ability to remove content as they pleased.[77]

The defendants tried to argue that they had changed the policies since and no longer exercised the alleged kind of editorial control. The plaintiff's evidence was compelling nonetheless, and the court held that Prodigy had become akin to a publisher with responsibility for defamatory postings that made it onto their site.[78] Since Prodigy failed to meet the criteria of step one in the two-step test, it did not matter whether they knew about the libelous content or not. They were already considered a publisher which brought on liability for all content on their platform.

The decision was widely criticized. The court had held that an online service provider that monitored and moderated content was akin to a traditional publisher such as a newspaper. However, that train of thought was problematic—Prodigy received 60,000 postings daily—far more content than any traditional publisher had to deal with.[79] It was virtually impossible to moderate all content that was uploaded to the bulletin boards. Any minor effort to keep the platform clean led to liability for all content, even though it could not be fully monitored. Large online service providers would effectively have to abandon moderating all together or stop providing

[77] *Ibid.*
[78] *Ibid.*
[79] CDA 230: Legislative History, Electronic Frontier Foundation. Retrieved February 9, 2021, from https://www.eff.org/issues/cda230/legislative-history

communications services in order to avoid liability. Either way, the consumers would suffer, and the technological development would be stifled.[80]

A few months after the court's decision, Prodigy apologized publicly for the libelous posts. It was enough for Stratton Oakmont to drop the lawsuit. Prodigy was naturally relieved not having to pay anything, but the court's ruling finding Prodigy to be a publisher was still on the books. Usually, a company would not be too concerned about a ruling of a state trial judge. In this case there was hardly any case law, meaning that in future cases the courts would most likely consider the Stratton Oakmont v. Prodigy decision. As the ruling had not been favorable for Prodigy, they wanted it to be changed. They requested reargument which Stratton Oakmont did not oppose. Still, the request was denied. The judge argued that there was a real need for some precedent and the fact that Stratton Oakmont had dropped the lawsuit did not change it.[81] It would not take long after this highly controversial ruling before the legislators decided to take action, the situation was unbearable.

2.2 Communications Decency Act

In 1995, the U.S. Congress was in the middle of a substantial overhaul of the outdated Communications Act of 1934. The Congress was primarily focused on telephones and cable TV.[82] However, some members of the Congress were concerned about the lack of legislation for the Internet. That year, Senators James Exon (D) and Slade Gorton (R) cosponsored a bill that was intended to address the problem of children accessing pornography and other offensive material on the Internet.[83] Meanwhile, Representatives Christopher Cox (R) and Ron Wyden (D) were working on a bill of their own. The Stratton Oakmont ruling was the straw that broke the camel's back. Incentivizing online service providers to take a hands-off approach would stifle the development of the Internet. Cox and Wyden knew something had to be done.[84] Their solution was what is today commonly known as *Section 230.* The amendment was intended to protect online service providers, such as Prodigy, from liability for third-party content. In its final bill, the U.S.

[80] Johnson 1996, 589–.
[81] Kosseff 2019, p. 54.
[82] Kosseff 2019, p. 60–61.
[83]Cosponsors: S.314 — 104th Congress (1995-1996), retrieved February 15, 2021, from https://www.congress.gov/bill/104th-congress/senate-bill/314/cosponsors; Dickinson 2010, 863–.
[84] Kosseff 2019, p. 59.

congressional conference committee decided to combine both the Exon-Gorton and Cox-Wyden bills into Title V of the Telecommunications Act of 1996, also known as Communications Decency Act of 1996.[85] The fact that the Cox-Wyden amendment became together with the Exon-Gorton amendment part of the Telecommunications Act of 1996, and consequently the CDA, was merely a coincidence. The timing of the legislative overhaul just happened to be favorable.

2.2.1 Strike Down on the CDA

The CDA faced immediate opposition. On the day that President Clinton signed the bill, the ACLU together with 19 other plaintiffs sued to prevent the CDA from being enforced. The plaintiffs argued that "the censorship provisions were unconstitutional because they would criminalize expression protected by the First Amendment and because the terms 'indecency' and 'patently offensive' are unconstitutionally overbroad and vague."[86] A federal three-judge panel ruled in favor of the plaintiffs and subsequently the government appealed to the U.S. Supreme Court. The government were no more successful in the Supreme Court than in the lower court. Justice John Paul Stevens wrote in the opinion of the court:

> "We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[87]

In other words, the Supreme Court concurred with the plaintiffs' arguments. On June 26, 1997, the Supreme Court unanimously struck down the CDA, except for Section 230.[88] All that remained of the CDA was the Cox-Wyden amendment.[89]

---

[85] Kosseff 2019, p. 72.
[86] Reno v. ACLU — Challenge to censorship provisions in the Communications Decency Act. Retrieved February 16, 2021, from https://www.aclu.org/cases/reno-v-aclu-challenge-censorship-provisions-communications-decency-act
[87] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997).
[88] *Ibid*.
[89] Kosseff 2019, p. 76.

2.2.2 The Cox-Wyden Amendment: Section 230

Section 230, or 47 U.S.C. § 230, as it is officially codified, is a rather lengthy piece of legislation. However, the most significant part boils down to subsections 230(c)(1) and (c)(2):

> **(c) Protection for "Good Samaritan" blocking and screening of offensive material**
>
> **(1) Treatment of publisher or speaker**
>
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
>
> **(2) Civil liability**
>
> No provider or user of an interactive computer service shall be held liable on account of-
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph

The most renowned part of Section 230 is the 26 words in subsection (c)(1). Section 230 (c)(1) provides immunity from liability for “providers” and “users of interactive computer service” who publish third-party content. The million-dollar question then is: what is an interactive computer service? Unfortunately, it is exceedingly difficult to give a thorough and accurate answer because the answer keeps changing. It is an ongoing debate how Section 230 (c)(1) should be interpreted and every once in while courts marginally alter the interpretation. Section 230 (f)(2) is intended to help with the interpretation of what an interactive computer service is. It states:

> “The term ‘interactive computer service’ means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the

> Internet and such systems operated or services offered by libraries or educational institutions."[90]

The definition is somewhat outdated, but in the very least it provides a guideline. A modern example of this includes all of the major social media platforms. Section 230 provides immunity from liability for Facebook, Youtube, Amazon, Twitter and generally any other service that provides a platform for third-party content.[91] Even traditional publishers such as newspapers or blogs can gain immunity for, say a reader comment section. Newspapers and blogs are nonetheless liable for what they publish themselves since they can control that content. Section 230 provides immunity from liability only for third-party content, in this example the comment section.

Section 230 (c)(2) further provides protection from civil liability for "Good Samaritan" blocking and screening of offensive material. It seems like the statute is a direct response to the *Stratton Oakmont, Inc. v. Prodigy Services Co.* ruling as the statute perfectly fits the case. However, some scholars think that Section 230 (c)(2) might be superfluous.[92] Section 230 (c)(1) already provides immunity by stating that no provider or user of an "interactive computer service" shall be treated as a publisher, and as is known from previous case law, distributors are generally not liable for third-party content on their platforms. In other words, it seems like Section 230 (c)(2) is somewhat redundant.

There are a few exceptions to the immunity from liability that Section 230 provides. The exceptions can be found in Section 230 (e):

> (1) No effect on criminal law
>
> (2) No effect on intellectual property law
>
> (3) State law
>
> (4) No effect on communications privacy law

[90] 47 U.S.C. § 230 (f)(2).
[91] *See Force v. Facebook, Inc., 934 F.3d 53 (2nd Cir. 2019)*. Section 230 did apply to Facebook even in a case related to terrorism. *See also Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008)*. Section 230 barred a negligence claim against MySpace for failing to implement safety measures to protect minors and failure to institute policies relating to age verification.
[92] Dickinson 2010, p. 869.

(5) No effect on sex trafficking law

A significant exception for intermediaries is that Section 230 (c) has no effect on intellectual property law. It means that Section 230 does provide protection for intermediaries for, say defamatory third-party content, but interestingly not for copyright infringing third-party content. Copyright infringing third-party party content is instead regulated by the Digital Millennium Copyright Act ("DMCA"). The exceptions of criminal law and intellectual property law were made in fear of attracting too much political opposition.[93] If not, the U.S. could have ended up with a more comprehensive piece of legislation, such as the European counterpart Electronic Commerce Directive 2000.[94]

2.2.3 The Court Approves of Section 230 Protection

On April 25, 1995, six days after the Oklahoma City bombing, an anonymous user on America Online (AOL) posted a message advertising merchandise glorifying the bombing. People were instructed to call the plaintiff, Kenneth Zeran, if they were interested in buying the merchandise. Zeran had nothing to do with the post or the merchandise, yet he started receiving a barrage of angry calls. Zeran contacted America Online (AOL) to have the post removed, which they did. Shortly after the removal of the first post, a similar post appeared again. Zeran asked AOL to take it down as well, which they did, but the damage was already done. Zeran claims that in the final days of April he received abusive phone calls every two minutes. To make matters worse, a broadcaster at a radio station in Oklahoma City, read the slogans on air and encouraged listeners to call Zeran and harass him. In January of 1996, Zeran filed suit against the radio station and in April of the same year, he filed a separate action against AOL. Zeran alleged that "AOL was negligent in failing to respond adequately to the bogus notices on its bulletin board after being made aware of their malicious and fraudulent nature".[95]

Zeran sued AOL for negligence, with the notion that intermediaries are liable for distribution of content which they "knew or should have known"[96] was of a defamatory character. Zeran relied his claim on the *Cubby* holding, in which a service provider could not be held liable for

[93] Kosseff 2019, p. 66.
[94] Directive 2000/31/EC.
[95] Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997).
[96] *See* Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 141 (S.D.N.Y.1991).

distributing defamatory statements unless it knew or had reason to know of the statements. Naturally, AOL did not agree with the claim. Instead, AOL argued that the brand-new Section 230 preempted the holding of *Cubby*. Nonetheless, there was a catch—the inflammatory messages had been posted prior to the enactment of Section 230. It meant that there were two questions at issue:

1) does Section 230 apply to a lawsuit that is filed after its enactment but based on facts that occurred prior to its enactment?
2) does Section 230 preempt Zeran's state law negligence claim?[97]

Zeran contended that applying Section 230 on his case would violate the stricture against retroactive application of statutes. However, the District Court found that Congress had intended Section 230 to be applied to all suits filed after its enactment regardless of when the events that the suit arose from occurred. The District Court held that Section 230 (d)(3) "constitutes an adequately clear statement of Congress' intent to apply § 230 of the CDA to claims that are filed after the enactment of the CDA".[98]

The District Court further found that Section 230 (d)(3) is not intended to preempt state law—to the contrary, it is intended to retain state law remedies, unless the state law remedies conflict with Section 230. Yet, the Supremacy Clause[99] commands preemption of state law whenever it directly conflicts with federal law. With those arguments, the District Court held that Zeran's suit conflicted with both the express language and purposes of Section 230.[100]

In conclusion, the answer is yes to both of the questions above and consequently AOL's motion for judgement on the pleadings was granted. Zeran appealed to the Fourth Circuit, but the Fourth Circuit granted judgement in favor of AOL. The Fourth Circuit held that each of Zeran's claims were barred by Section 230 as it "creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." [101] After having lost again, Zeran petitioned to the U.S. Supreme Court, but the court declined

[97] Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997).
[98] *Ibid*.
[99] U.S. Const. art. VI, § 2.
[100] Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997).
[101] Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).

to hear his case. Still to this day, *Zeran* provides extensive protection for intermediaries against liability for third-party content.

2.2.4 Scope of Section 230 Immunity

The most challenging, yet crucial question on the subject of Section 230 is how to determine whether someone is an Information Computer Service (distributor/intermediary) or an Information Content Provider (publisher). Publishers are liable for third-party content, whereas intermediaries are immune. That is to say, the distinction makes all the difference. The problem is that frequently, it is not as clear cut as one would think. Especially in the Internet era, the amount of online service providers has skyrocketed, meaning that there is a multitude of variation between each one of them.[102] Before the enactment of Section 230, the solution was to prohibit intermediaries from all editing and monitoring of third-party content, or else they were considered publishers. Section 230 (c) now allows blocking and screening of third-party content provided it is done in good faith. That in turn created a new quandary: how much can the intermediary be involved in the content without becoming liable as a publisher?[103]

It is a question that courts across the U.S. have had to consider multiple times. *Zeran* set the tone for other courts by concluding that Section 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. The holding provided broad immunity to intermediaries and to this day it still largely stands.[104] There have been numerous cases aligning with *Zeran*, too many to cover all of them here.

However, one particularly interesting case is *Blumenthal v. Drudge*.[105] Drudge was contracted by AOL to write a column for AOL. One of the articles was defamatory and consequently Blumenthal sued both AOL for hosting the article and Drudge for publishing it. The Court found no liability for AOL, despite AOL's contractual relationship with the creator of the defamatory content and the fact that AOL had board managers that were supposed to monitor and edit such illegal content. The Court held that Section 230 was meant to provide immunity to service

[102] Goldman 2020, p. 159.
[103] Dickinson 2010, p. 871.
[104] Balasubramani 2016, p. 275; Sevanian 2014, p. 132.
[105] Blumenthal v. Drudge, 992 F. Supp 44 (D.D.C. 1998).

providers in exactly this kind of cases. The key takeaway is that Section 230 precludes courts from entertaining claims that would place service providers in a publisher's role even when the service provider has had an active role in soliciting the content.[106]

There are nonetheless some cases too that have outlined the limits of Section 230. In *Fair Housing Council of San Fernando Valley v. Roommates.com, LLC*[107], the United States Court of Appeals for the Ninth Circuit, sitting en banc, held that Section 230 did not provide immunity to an online service provider that used dropdown menus in a questionnaire. Due to the dropdown menus which offered prefilled answers, Section 230 (c)(1) "information provided by another information content provider" condition was not met. The Court held that the defendant was an information content provider. For other parts of the website, the defendant was considered an interactive computer service, thus gaining immunity from liability. It is possible for an online service provider to be both an intermediary and a publisher. It is also worth noting that even the slightest contribution to the content may bar an online service provider from Section 230 immunity.[108]

In *Barnes v. Yahoo!*[109], Barnes who was a user of Yahoo, had asked Yahoo to remove objectionable third-party content about her. Yahoo promised Barnes to remove the content but then failed to do so. The Court held that pursuant to Section 230 Yahoo had no obligation to remove third-party content. The Court consequently dismissed Barnes' tort claim. However, the Court found that Section 230 does not bar a promissory estoppel claim. The reason for it is that Yahoo's liability comes from the promise to remove the content instead of their publishing conduct. It is sort of a contractual liability, which Section 230 does not preclude.[110] Section 230 does not contain a notice-and-takedown policy, but apparently it does not preclude it either provided that the liability is not based on the intermediary's publishing conduct. This is one of the distinguishing factors of Section 230 compared to the Digital Millennium Copyright Act and the Electronic Commerce Directive.

---

[106] *Ibid*.
[107] Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008).
[108] *Ibid*.
[109] Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009).
[110] *See* Barnes v. Yahoo!, Electronic Frontier Foundation. Retrieved February 21, 2021, from https://www.eff.org/issues/cda230/cases/barnes-v-yahoo

In *Anthony v. Yahoo! Inc.*[111], Section 230 (c)(1) was not applied because Yahoo had created the fraudulent content themselves and did accordingly not meet the standards. *Gucci America, Inc. v. Hall & Associates*[112] is another case where the Court held that Section 230 was not applicable. This time it was due to the fact that Section 230 does not provide protection against trademark infringement claims. Intellectual property law is one of the few explicit exceptions listed in Section 230 (e).

It seems like it is futile to attempt forming an exact definition for the extent of Section 230's application. Numerous cases have already explored its boundaries and slightly shifted the scope of it. Since every case is unique, there will undoubtedly be more cases in the future further elucidating the application of Section 230. So far, courts have been inclined to follow *Zeran's* precedent by applying Section 230 extensively. Curiously, many scholars seem to disagree with *Zeran*, in that Congress' intent was actually not to create such a broad immunity. A common notion seems to be that the Court was right by ruling in favor of AOL, but the arguments they used created too broad of an immunity.[113]

2.3 Liability for Third-party Copyright Infringement

2.3.1 Legitimate Use of the "Betamax"

In the 1970s, Sony sold a consumer-level video tape recorder called the "Betamax". The Betamax allowed consumers to record television programs and watch them later. Universal City Studios alongside with multiple other media companies sued Sony for copyright infringement, alleging that the Betamax was used to record their copyrighted works, thus making Sony liable for copyright infringement. The California District Court had to address two fundamental questions:

1) does recording television programs for noncommercial home use constitute copyright infringement?

[111] Anthony v. Yahoo! Inc., 421 F.Supp.2d 1257 (N.D.Cal. 2006).
[112] Gucci America, Inc. v. Hall & Associates, 135 F. Supp. 2d 409 (S.D.N.Y. 2001).
[113] *See e.g.*, Patel 2002, p. 679–689; Freiwald 2001, p. 594–596; McManus 2001, p. 647–; Pantazis 1999, p. 547–550; Kane 1999, p. 488–489; Wiener 1999, p. 905–; Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1395 (2004).

2) Does Sony's sale and marketing of the Betamax to the general public constitute contributory infringement of copyrighted public broadcasts under the Copyright Act of 1976?

The District Court ruled in favor of Sony, finding that time-shifting for noncommercial purposes was indeed legitimate fair use, and that Sony's actions did not constitute contributory infringement.[114] The Ninth Circuit Court reversed the District Court's decision in part,[115] after which Sony appealed to the U.S. Supreme Court. The issue that the Supreme Court had to tackle was whether or not Sony's sale of video tape recorders to the general public violated the respondents' copyrights. In a 5-4 opinion, the Supreme Court held that the sale of the video tape recorders to the general public does not constitute contributory infringement of respondents' copyrights.[116] The Court rationalized the holding with two main arguments: most of the Betamax users used it for its intended legitimate purpose of time-shifting broadcasts, and moreover the plaintiffs failed to demonstrate that time-shifting would cause non-minimal harm to the value of their copyrighted works.[117] The "Betamax case" is still to date a significant landmark case. Especially noteworthy is the argument about Sony not being liable for contributory infringement because of the legitimate purposes and substantial non-infringing uses of the Betamax.

2.3.2 Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA)[118] was signed into law in 1998 in hopes of bringing U.S. copyright law "squarely into the digital age."[119]. The DMCA implements two 1996 World Intellectual Property Organization (WIPO) treaties and addresses a number of other significant copyright-related issues.[120] The DMCA was not created from scratch, instead it was built on case law concerning secondary liability for copyright infringement such as the *Betamax case*.[121] In the DMCA, it is Title II, the Online Copyright Infringement Liability Limitation Act

[114] Universal City Studios, Inc. v. Sony Corp. of America, 429 F. Supp. 407 (C.D. Cal. 1977).
[115] Universal City Studios, Inc et al. v. Sony Corp. of America et al., 659 F.2d 963 (9th Cir. 1982).
[116] Sony Corp. v. Universal City Studios, 464 U.S. 417 (1984).
[117] *Ibid*.
[118] Pub.L. 105-304 -- October 28, 1998 -- To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.
[119] Report of the Senate Comm. On the judiciary, S. Rep. No. 105-190, at 2 (1998); *See also* Nimmer 2000, p. 680.
[120] The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary. Retrieved February 26, 2021, from https://www.copyright.gov/legislation/dmca.pdf
[121] Dinwoodie 2017, p. 100.

(OCILLA or Section 512)[122], that regulates online service providers' secondary liability. It affords online service providers protection from liability for copyright infringement if they meet certain conditions. There are two general conditions that must always be met to be eligible for Section 512 protection:

i. online service providers must adopt and reasonably implement a policy of terminating in appropriate circumstances the accounts of users who are repeat infringers; and
ii. they must accommodate and not interfere with "standard technical measures."[123]

Additionally, the online service provider must qualify for at least one of the following categories:

i. Transitory communications;[124]
ii. System caching;[125]
iii. Storage of information on systems or networks at direction of users;[126] and
iv. Information location tools.[127]

Each of the four above-mentioned categories have a subset of conditions that have to be met in order to qualify for protection.[128] An online service provider that meets the two general conditions and the conditions of any of the four alternative provisions is granted full protection from liability for monetary damages and partial protection from injunctive relief.[129] Failure to meet the conditions does not automatically induce liability for copyright infringement to the online service provider. For that to happen, the copyright owner must prove the violation while the service provider may still avail itself of defenses such as fair use.[130] Copyright owners may also request a court to issue a subpoena to an online service provider for identification of an alleged infringer.[131]

---

[122] 17 U.S.C. § 512.
[123] *Id*. at 512(i)(1)(B). *See also* The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary. Retrieved February 26, 2021, from https://www.copyright.gov/legislation/dmca.pdf
[124] *Id*. at 512(a).
[125] *Id*. at 512(b).
[126] *Id*. at 512(c).
[127] *Id*. at 512(d).
[128] They are numerous and can be found listed at 17 U.S.C. § 512.
[129] 17 U.S.C. § 512(j).
[130] *Id*. at 512(l). *See also* The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary. Retrieved February 26, 2021, from https://www.copyright.gov/legislation/dmca.pdf
[131] 17 U.S.C. § 512(h).

Of the four provisions, DMCA 512(c) is predominantly applied to online service providers affording them insulation from liability for copyright infringements committed by their users. In order to be eligible for the protection, online service provider must meet the following conditions:

> **"(1)** In general. —A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—
>
> **(A)** **(i)** does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
>
> **(ii)** in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
>
> **(iii)** upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
>
> **(B)** does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
>
> **(C)** upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[132]

Unlike Section 230, the DMCA 512 (c)(1)(A) bars protection if the online service provider knew or should have known about the infringing content.[133] The provision emanates from case law predating the enactment of the DMCA.[134] Since the DMCA unequivocally bars strict liability

[132] *Id*. at 512(c)(1).
[133] *See* Lerner 2020, p. 353; Goldman 2020, p. 159.
[134] *See e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). Some other cases suggest that online service providers could be strictly liable for their users' infringement. *See e.g*., Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993); Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997); Goldman 2015, p. 103.

for online service providers, a form of effective system for copyright owners to protect their rights had to be instituted.[135]

The solution was a notice-and-takedown policy, which is yet another difference compared to Section 230. The simple concept of the notice-and-takedown policy is that the copyright owner notifies the online service provider of copyright infringement, after which the online service provider has to remove the flagged content or else, they become liable.[136] The notice-and-takedown procedure is brilliant in many ways, but it does not come without its problems. The system has been widely abused in different ways. According to one study, nearly a third of Google's takedown requests were invalid.[137] According to Google's Transparency Report, Google has received more than five billion takedown notices, which means that Google alone may have received nearly two billion bogus DMCA takedown notices.[138] An increasing amount of the takedown notices are automatically sent by bots, meaning that there is no human interaction. The DMCA mandates that takedown notices must be based on a "good faith belief"[139] that the content is infringing. It is difficult to see how a bot could act based on good faith belief. It seems like there is an inherent need for human interaction to do so. The bots are however not the only source of bogus takedown notices. Online service providers often prefer to play safe and remove flagged content regardless of the validity of the claim, as they do not want to risk becoming liable.[140] On the flip side of the coin, copyright owners and even scammers have discovered it and are abusing it by sending invalid takedown notices. Another typical misuse situation is where takedown notices are sent for content that fall under fair use. Moreover, copyright owners have in some cases brought action against online service providers for third-party copyright infringement without having sent a takedown notice first.[141] If successful, these kinds of lawsuits undermine the entire notice-and-takedown system.

[135] Goldman 2015, p. 103.
[136] *See e.g.*, Kuczerawy 2020, p. 528.
[137] Urban – Karaganis – Schofield 2017, p. 88.
[138] Google Transparency Report, Content delistings due to copyright. Retrieved March 1, 2021, from https://transparencyreport.google.com/copyright/overview?hl=en
[139] 17 U.S.C. § 512(c)(3)(v).
[140] Seltzer 2010, p. 174.
[141] *See e.g.*, UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011); Viacom Int'l Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir 2012); Goldman 2015, p. 104.

2.3.3 Peer-to-Peer File Sharing Services

Peer-to-peer file sharing services constitute a distinctive challenge in the context of intermediaries' secondary liability for copyright infringement. Typically, a peer-to-peer file sharing service will provide a platform that connects its users to each other. The users will then share content to each other. At first glance, these services are no different from other online intermediaries, such as the big social media platforms. Of course, there are different kinds of peer-to-peer file sharing services. Some might moderate or organize content whereas others do not. In theory, some are passive service provider though and should on the face of it, not be liable for potential third-party infringements. However, copyright law puts its own spin on it changing how some things work. There are multiple high-profile peer-to-peer file sharing service cases, but A&M Records, Inc. v. Napster, Inc. was the first major case to apply copyright laws to such a service.

Napster was an early peer-to-peer file sharing service that allowed its users to transmit a variety of files, but it was best known as a platform for sharing and downloading music for free in MP3 format. Unsurprisingly, record companies did not like it, and in 1999, a number of them filed a motion for a preliminary injunction in order to stop the file sharing. Plaintiffs alleged Napster was liable for contributory and vicarious copyright infringement for providing a platform where users could obtain copyrighted works without copyright holders' authorization. The district court granted plaintiffs the preliminary injunction and subsequently Napster appealed.[142]

Napster claimed that their users' activity fell under fair use.[143] Napster made the argument that its users merely space-shifted the content and that it should therefore be protected under *Sony Corp. of America v. Universal City Studios, Inc.* The Ninth Circuit disagreed concluding that *Sony* was not applicable because it was the end user who time-shifted the broadcast, unlike in *Napster*. In *Napster* users first space-shifted the content and then shared it with others. It is clearly not the same to copy something for personal use and to copy something for later distribution. Additionally, the Court did not buy into the idea that the content on Napster would consist of samples and copies of songs that users already owned. The Court found that Napster knew that its service was mainly used for infringing activities and that it still had failed to

[142] A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000)
[143] 17 U.S. Code § 107.

remove said content. It further found that Napster did indeed benefit from the file sharing and that it negatively impacted record sales and thus also revenue. As a result, the Ninth Circuit affirmed in part the District Court's decision. The Ninth Circuit reversed in part the District Court's decision because it found that it was the plaintiffs' burden to notify Napster of any infringing content, which Napster would then remove. Napster did not possess the technology to recognize all infringing content and the Ninth Circuit found that it did not have to do so either.[144]

MGM Studios, Inc. v. Grokster, Ltd. is a U.S. Supreme Court decision from 2005. *Grokster* is commonly described as the successor to *Napster* because of the similar factual backgrounds. The district court ruled for Grokster, reasoning that the service could be used for legitimate purposes.[145] The Ninth Circuit affirmed the decision. However, the Supreme Court found that the lower courts had misinterpreted the safe harbor established by *Sony*. The Supreme Court took issue with Grokster's active role in marketing and managing the infringing activity. Justice Souter wrote in the Supreme Court's opinion:

> "We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[146]

The other concern was the extent of the service's legitimate use. The plaintiffs were able to prove that upwards of 90 percent of the content was copyrighted. Clearly, the service had hardly any commercially significant non-infringing use. The Copyright Act did not expressly make online service providers liable for third-party infringement, but the Supreme Court argued that secondary liability doctrines should be applied. The "only practical alternative"[147] was to go against the online service provider for secondary liability. Going after individual users of the service would have been futile. Essentially with said arguments, the Supreme Court vacated the Ninth Circuit's judgement.[148]

---

[144] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).
[145] The decision was based on *Sony Corp. of America v. Universal City Studios, Inc. ("Betamax case").*
[146] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005)
[147] *Ibid*.
[148] *Ibid*.

In conclusion, online service provider's liability for third-party copyright infringements seem to be affected by at least two things:

1) does the product have commercially significant non-infringing use; and
2) is the intermediary inducing copyright infringement.

These two conditions have been considered in all of the copyright cases I covered, but interestingly they are rarely considered in the context of the Section 230. Is there are reason why the same logic could not be applied beyond copyright law? If not, would it make sense to do so? Nevertheless, the *Grokster* and *Betamax* cases remain two of the most significant cases of secondary liability jurisprudence in the U.S.[149]

[149] Lerner 2020, p. 353.

3 Intermediary Liability in the EU

3.1 Electronic Commerce Directive 2000

When the Internet started growing and e-commerce began gaining traction in the 90s, the EU and the U.S. were poles apart in terms of the legal landscape. In the late 90s, the U.S. had enacted two significant pieces of legislation on Internet law, whereas the EU still had no harmonized legislation worth mentioning.[150] The same was true for case law. Some member states in the EU did have national legislation that touched on the topic, but nothing significant enough to discuss here. The new legislation in the U.S. was at least partly a product of cases involving online service providers. The EU on the other hand, did not have prior harmonized legislation, which meant that there was no relevant case law either. In the late 90s, the EU decided that it needed to catch up with the legislation, not to fall too much behind in the development of e-commerce. On June 8, 2000, the Electronic Commerce Directive (ECD)[151] came into force.[152] The idea was to promote the growth of e-commerce by creating a coherent regulatory framework.[153] The ECD covers a wide range of topics, including advertising, spam, online contracts, online orders, enforcing existing legislation, and last but not least—liability of service providers. The directive covers essentially all types of commercial online services, including:

i. "news services (such as news websites)
ii. selling (books, financial services, travel services, etc.)
iii. advertising
iv. professional services (lawyers, doctors, estate agents)
v. entertainment services
vi. basic intermediary services (Internet access, transmission and hosting of information)
vii. free services funded by advertising, sponsorship, etc."[154]

[150] Savin 2017, p. 22.
[151] Directive 2000/31/EC.
[152] Member states had to implement the Directive before January 17, 2002. *See* Article 21(1) ECD.
[153] European Commission, A European Initiative in Electronic Commerce, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(97)157 (Brussels, 15 April 1997).
[154] ECD Document Summary. Retrieved March 8, 2021, from https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32000L0031

The list above does however not directly apply to the statutes about service provider liability. The EU regime for intermediary service provider's liability consists of Articles 12-15 of the ECD and some provisions of the Copyright Directive (2001/29/EC).[155] Articles 12-15 of the ECD contain three provisions under which service providers can be exempt from liability for third-party infringements—"Mere conduit", "Caching" and Hosting. The remaining Article is a ban on obligation to monitor content. The exemptions cover all kinds of illegal content, including copyright infringements and defamation. They also provide protection from both civil and criminal liability.[156]

This is the most significant difference compared to the U.S. system is that the U.S. system is divided in to the DMCA and the CDA, whereas the European counterpart is just one Directive. It means that the ECD must be different than at least one of the corresponding U.S. statutes. The ECD's exemptions parallel the ones of the DMCA, meaning that the CDA is somewhat unique compared to the European legislation. The reason for the Directive being so similar to the DMCA, is at least in part because it is modelled on it.[157] Just like in Section 512(c) of the DMCA, the Directive's hosting safe harbor is built around a notice-and-takedown scheme.[158]

The fact that the U.S. is a federation, and the EU is a union, also makes a difference. The ECD being a directive, means that there is national variation between the member states in regard to how the act is implemented and enforced. In the U.S. on the other hand, there is more extensive and coherent enforcement from the top level. Of the cases concerning intermediary liability that reach the Court of Justice of the European Union (CJEU), a vast majority is dealing with intellectual property law. The case law is heavily focused on hosting safe harbors under Article 14 and the prohibition on general monitoring obligation under Article 15.[159]

[155] Savin 2017, p. 153.
[156] Goldman 2020, p. 155.
[157] Savin 2017, p. 167.
[158] Goldman 2020, p. 167.
[159] Husovec et al. 2020, p. 20.

3.1.1 Mere Conduit

Article 12 of the ECD contains the exemption for mere conduits. This refers to situations where service providers act as passive intermediaries. Article 12(1) stipulates that a service provider will not be liable for third-party content on the condition that the provider:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

The conditions stipulated in Article 12(1) are effectively a more precise description of a passive service. The service provider may not create the content, have knowledge of it, nor control it. If any one of the conditions is not met, the service provider has failed to act as a mere conduit and will accordingly not be exempt from liability under Article 12.[160] Unlike Articles 13 and 14, Article 12 does not contain an explicit notice-and-takedown scheme. However, Recital 42 of the directive states that the exemptions only cover cases where the "service provider has neither knowledge of nor control over the information which is transmitted or stored". Additionally, Article 12(3) stipulates that it does not prevent courts or authorities from requiring the service provider to terminate or prevent an infringement. The conclusion seems to be that a service provider acting in good faith can be exempt from liability under Article 12 but gaining knowledge of an infringement will revoke the protection.[161]

McFadden v. Sony Music[162] is one of very few ECJ cases that have touched on the mere conduit provision. McFadden was the owner of a lightning and sound rental business and as a way to promote his business, he provided a free Wi-Fi connection. The Wi-Fi connection was not password protected, meaning anyone in the vicinity of his store could access it. In 2010, a music file on which Sony Music claimed ownership was illegally shared using the connection. About a month later, McFadden received a cease-and-desist letter from Sony Music demanding him to stop the infringing activity. McFadden asserted that he did not personally commit the alleged infringement and in return he brought an action for a negative declaration ('*negative*

[160] Savin 2017, p. 155.
[161] *Ibid*.
[162] Case C-484/14.

Feststellungsklage'). In reply to McFadden's claims, Sony Music made several counterclaims. Sony Music sought to obtain from McFadden: "first, payment of damages on the ground of his direct liability for the infringement of its rights over the phonogram, second, an injunction against the infringement of its rights on pain of a penalty and, third, reimbursement of the costs of giving formal notice and court costs.".[163] On January 16, 2014, the referring court dismissed Mc Fadden's action and upheld the counterclaims of Sony Music. McFadden appealed the decision, claiming that he is exempt from liability under the provisions of German law transposing Article 12(1) of the ECD. In the appeal, Sony Music claimed that the court should uphold the judgement at first instance or alternatively order McFadden to pay damages for allowing third parties to infringe their rights. The German Court was uncertain whether the mere conduit safe harbor was applicable or not, so they referred a number of preliminary questions to the European Court of Justice (ECJ). In essence, the referring court wanted to know if McFadden qualified as an "information society service" by providing an open Wi-Fi connection to attract potential customers and how extensive was the protection of Article 12.

The ECJ found that "information society services" typically covers services provided for remuneration[164], however, providing free Wi-Fi connection for advertising purposes was also of "economic nature"[165]. The Court made a broad interpretation and accepted that Article 12 was applicable to businesses that provided open Wi-Fi connection as a form of advertisement. Furthermore, the Court held that McFadden met the conditions of Article 12(1) and should therefore be afforded its protection. The ensuing question was, how broad was the immunity provided by Article 12? The Court held that Article 12 provides immunity from all liability. Sony Music was not entitled to claim compensation nor reimbursement for legal expenses. Article 12 did however not bar the copyright holder from seeking injunction from national authorities in order to stop the infringing activity. Lastly, the problem was determining an appropriate deterrent measure to stop the infringing activity. The measure must be effective enough to stop the infringement but targeted enough so that it does not restrict legitimate use of the Wi-Fi connection. The ECJ found that a complete ban on offering Wi-Fi would violate Articles 11 and 16 of the Charter of Fundamental Rights of the European Union. Ultimately, the ECJ settled for an injunction

[163] McFadden v. Sony Music C-484/14 para 28.
[164] Article 1(2) of Directive 98/34.
[165] McFadden v. Sony Music C-484/14 para 41.

which requires the service provider to make the Wi-Fi connection password protected. The Court noted that the password protection is only effective if the users are required to reveal their identity in order to obtain the password to the Wi-Fi connection. This kind of a scheme would interfere with the aforementioned freedoms, but only marginally.[166]

McFadden is an interesting decision which provides some guideline to the application and extent of the mere conduit safe harbor. It is also a good reminder of how challenging it can be to strike a balance between different freedoms and rights. On one side there is copyright, which is essential for a well-functioning economy, and on the other side there is the freedom of expression, information and conducting business, which are also essential for the same reasons. It seems as if McFadden could severely limit the viability of offering open Wi-Fi connection as a means of marketing.[167] This might though be one those decisions that becomes at least partly obsolete with time. Mobile Internet connections have already become so common, that the need for Wi-Fi connection has drastically decreased since 2010 when the infringement of the McFadden case took place.

Another case that touches on Article 12, although not to the same extent as *McFadden*, is Sotiris *Papasavvas v. O Fileleftheros Dimosia Etairia Ltd., Takis Kounnafi, Giorgos Sertis*.[168] *Papasavvas* is a decision that explored in more general terms the application of Articles 12-14. What makes the decision so intriguing is that it is a defamation lawsuit involving a newspaper—a prime example of an intermediary liability case, which is rare in the ECJ. In 2010, Papasavvas sued a newspaper company, its editor-in-Chief and one of its journalists for defamation because of some articles they had written. Papasavvas sought damages for harm and requested the national court to order a prohibitory injunction to stop the articles from being published. The referring court had a plethora of questions for the ECJ concerning the application of Articles 12-14. Nevertheless, the decision boils down to two fundamental questions:

1) does the definition of "information society service" in the ECD cover online information services that are funded by means of commercial advertisements rather than directly by the recipient?

[166] *Id.* at para 90-92
[167] Husovec 2017, p. 124.
[168] Case C-291/13.

2) Can a newspaper that operates a free website get protection under any of the safe harbors of Articles 12-14?

The first question is important because if the service provider cannot be considered an information society service, then all of the safe harbors are automatically off-limits. The question is practically identical to the one in *McFadden,* and so is the conclusion. The Court held that the term "information society service" should be interpreted broadly. Recital 18 in the preamble of the ECD supports the conclusion. In other words, a newspaper that is funded with advertisement money can be considered an "information society service". The second question is in fact also rather simple to answer in light of the theoretical background. A newspaper that publishes articles is a textbook example of something that does not meet the criteria for the safe harbors. A newspaper has editorial control over the content that it publishes and therefore there is no need to limit its liability. So even on a conceptual level it does not work in favor of the newspaper. For the ECJ, it was simply as easy as looking at the conditions stipulated in Article 12-14. The newspaper was clearly not just a "mere conduit" or passive in any sense, meaning that it was outside the scope of the safe harbors.[169]

In the context of the ECD and its U.S. counterparts, the decision was very much foreseeable. The decision is in line with the fundamental concept of intermediary liability and safe harbors. If anything, it is odd that the referring court would ask questions that are seemingly so obvious. Perhaps it is the lack of case law from the ECJ that uncertainty, in which case it is good to get these decisions even for seemingly simple questions.[170]

3.1.2 Caching

In computing, caching is the process of storing copies of files in a temporary storage location, so that future requests for that data are served up faster than is possible by accessing the data's primary storage location. By doing so, reuse of previously retrieved or computed data is fast and

[169] Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd., Takis Kounnafi, Giorgos Sertis C-484/14

[170] Note that a few years earlier, the European Court of Human Rights held in *Delfi AS v. Estonia 64569/09* that a news outlet was liable for defamation based on comments posted in its comments section. In *Delfi*, the plaintiff invoked Article 10 of the European Convention on Human Rights. Interestingly Papasavvas did not use the same freedom of expression argument that had succeeded in a fairly similar case a few years earlier.

efficient.[171] Caching can be performed both by the end-user and the service provider.[172] Article 13 of the ECD is the safe harbor for caching. Considering the purpose and the technology of caching, caching is perfectly in line with other exemptions from liability. Caching is simply a tool for making computing more efficient and it does not typically involve intent or active actions of any kind. Article 13 does stipulate a number of conditions for the service provider to be exempt from liability for caching. A "service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

> (a) the provider does not modify the information;
>
> (b) the provider complies with conditions on access to the information;
>
> (c) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
>
> (d) the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
>
> (e) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement."[173]

Most of the provision boils down to that the purpose of caching must be to facilitate the flow of information to the intended recipient, which is anyway the primary purpose of the technology. Article 13(1)(e) is different though—it imposes a notice-and-takedown scheme. The service provider must "expeditiously" remove or disable access to infringing content after becoming aware of it. "Obtaining actual knowledge" could happen independently or by notice from a third party. The notice-and-takedown scheme is what makes the caching safe harbor quite different

[171] Caching Overview. Retrieved March 12, 2021, from https://aws.amazon.com/caching/
[172] Savin 2017, p. 157.
[173] Article 13(1) of Directive 2000/31/EC.

from the mere conduit safe harbor. Similar to the other safe harbors of the ECD, Article 13(2) stipulates that the safe harbor does not preclude authorities from requiring the service provider to terminate or prevent an infringement.

The fact that no direct ruling on Article 13 in the context of intermediaries exist,[174] suggests that caching is rarely used for other than its intended purpose. It is also possible that caching is so technical that the infringed party does not even detect the infringement. Local temporary copies of files for faster access are certainly not as easy to find as for example a published article or other publicly available content online.

3.1.3 Hosting

Article 14 of the ECD relates to hosting, which involves, inter alia, managing websites for end-users.[175] Article 14(1) reads as follows:

> "Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:
>
> (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or
>
> (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information."[176]

According to the provision, the hosting safe harbor applies to a service provider that stores information provided by a user of the service. The provision does not further specify what kind of services are covered. Instead, it has been up to the courts to interpret the extent of Article 14's application. The CJEU has interpreted the safe harbor to cover a wide range of services such as

[174] Savin 2017, p. 158.
[175] *Id.* at p. 146.
[176] Article 14(1) Directive 2000/31/EC.

social media platforms[177] and e-commerce platforms[178]. Naturally, there are plenty of hosting services that fit the description but have not been explicitly confirmed by the CJEU to fall under Article 14. Certain examples include web hosting, online media sharing platforms, file storage and sharing, cloud computing services, social networking and discussion forums, collaborative production, online marketplaces, collaborative economy, online games, search tools, and rating and reviews.[179] A substantial amount of the world's most popular online services fit the description.

There are however two exceptions to the rule. Firstly, if the service provider knew or should have known about the infringement and fails to remove or disable access to the information, the safe harbor does not apply.[180] A typical example of it would be peer-to-peer file sharing websites where the service provider usually either knows or should know that the service is mainly used for illegal purposes. The second exception is that the safe harbor does not apply if the user of the service is acting under the "authority or the control" of the provider.[181] The entire idea of the safe harbors is to insulate service providers from liability for third-party infringements. If the user is acting under the control of the service provider, the user is effectively no longer a third party and the service provider should not be insulated from liability for its infringements.

Identical to the mere conduit and caching safe harbors, the hosting safe harbor does not preclude authorities from requiring the service provider to terminate or prevent an infringement.[182] However, one unique feature of Article 14 is that it also allows Member States to establish procedures governing the removal or disabling of access to information.

Hosting is an extensively utilized safe harbor, which means that there are multiple CJEU cases relating to it. *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*[183] is a noteworthy example of such a case, as it clarified that search engines operators do not infringe trademark rights if they allow advertisers to use a third party's trademark as a keyword. Google, the defendant in the case, operates a free search engine. The search engine works by means of an

[177] *See* SABAM v Netlog C-360/10.
[178] *See* L'Oréal v. eBay C-324/09.
[179] Hoboken et al. 2018.
[180] Article 14(1) Directive 2000/31/EC.
[181] Article 14(2) Directive 2000/31/EC.
[182] Article 14(3) Directive 2000/31/EC.
[183] Joined Cases C-236/08, C-237/08, and C-238/08.

algorithm identifying keywords and presenting the user with a list of results.[184] In addition to the natural results, Google operates an advertisement system called "AdWords", which suggests sponsored links based on the keywords used. The sponsored search results are differentiated from the natural results so the user can tell them apart.[185] AdWords is an automated process that allows advertisers to choose keywords that they want to lead to their link. Every time a user clicks the sponsored link, Google gets compensated, meaning that it is in Google's interest to make the advertisements appealing and effective.[186] As a result, Google provides some data to advertisers, such as the number of searches on its search engine featuring the selected keywords, as well as related keywords, and the corresponding number of advertisers.[187]

In 2003, Luis Vuitton ("LV"), a French luxury goods company, discovered that sponsored links leading to websites selling counterfeit LV products showed up when Google users typed in keywords containing LV's trademarks, such as "Luis Vuitton", "LV" and "Vuitton". Not only could advertisers use LV's trademarks as keywords, but Google also offered those keywords in combination with words like "imitation" and "copy".[188] LV brought proceeding against Google, inter alia, seeking a declaration that Google had infringed its trademarks.[189] Google lost both in the Tribunal de grande instance de Paris and in Cour d'appel de Paris. Google further appealed to the Cour de cassation, which then referred three questions to the CJEU for a preliminary ruling. Essentially, the questions revolved around whether Google could be enjoined from using trademarked keywords or otherwise be held liable for offering such service.[190]

The Court concluded that based on European copyright law, LV has the right to prohibit Google from using keywords identical with LV's trademark in its sponsored links.[191] The Court was more lenient towards Google concerning the liability question. The Court held that "it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control

[184] Opinion of Advocate General Poiares Maduro, Google France, 2010, para 9.
[185] *Id*. at para 10.
[186] *Id*. at para 11.
[187] *Id*. at para 12.
[188] Google v. Louis Vuitton C-236/08, para 28-29.
[189] *Id*. at para 30.
[190] *Id*. at para 41.
[191] *Id*. at para 99, 105.

of the data which it stores".[192] Additionally, the Court pointed out that Google must not be precluded Article 14 protection for the mere fact that their referencing service is subject to payment.[193]

The fact that the entry of a search term matches the keyword is also not sufficient to justify the view that Google has knowledge of, or control over the data.[194] Lastly, the Court concluded that if the service provider lacked knowledge or control over the data, it cannot be held liable for data stored at the request of a third party.[195] The decision provides broad protection for service providers. It seems to suggest that Google could only be held liable if they were explicitly notified about the specific infringement and they still failed to remove the infringing content.[196] The decision is not really controversial, but it provides a valuable guideline to how Article 14(1)(a) should be interpreted.

Only a year later, the CJEU gave another closely related decision. However, this time the dispute was between L'Oréal and eBay.[197] L'Oréal is an international personal care company that manufactures and supplies cosmetics, perfumes, and hair care products. L'Oréal holds a number of national trademarks in the United Kingdom as well as Community trademarks.[198] It operates a "closed selective distribution network", which means that authorized distributors are not allowed to further supply products to other distributors.[199] eBay on the other hand, is a multinational e-commerce corporation that facilitates sales through its website. A part of eBay's revenue comes from commissions on sales of products.[200] All users must accept eBay's user agreement in order to buy or sell on the platform. One of the terms in that agreement is a prohibition on selling counterfeit products and on infringing trademarks.[201] In certain instances, eBay assists sellers to describe and categorize their products, create their own web stores, and even advertises the product on third party websites.[202]

---

[192] *Id*. at para 114.
[193] *Id*. at para 116.
[194] *Id*. at para 117.
[195] *Id*. at para 120.
[196] Savin 2017, p. 160.
[197] L'Oréal v. eBay C-324/09, para 21.
[198] Opinion of Advocate General Jääskinen, L'Oréal, 2010, para 21.
[199] L'Oréal v. eBay C-324/09, para 22.
[200] *Id*. at para 28.
[201] *Id*. at para 30.
[202] Opinion of Advocate General Jääskinen, L'Oréal, 2010, para 27.

In 2007, L'Oréal expressed its concerns regarding the widespread sale of infringing goods on eBay's European websites and requested eBay to take action to address the concerns.[203] Not being satisfied with eBay's response, L'Oréal brought several actions against eBay in various Member States.[204] L'Oréal claimed that eBay was jointly liable for multiple infringements.[205] The British High Court of Justice was one of the courts that had been brought action before. The High Court of Justice decided to stay the proceeding and referred a plethora of questions to the CJEU for a preliminary ruling.[206] The referred questions were largely same as in *Google v. Luis Vuitton*. Essentially, the questions revolved around whether eBay could be enjoined from advertising trademarked goods without the consent of L'Oréal and whether they were protected under the hosting safe harbor of Article 14.[207]

Regarding the first question, the Court came to the exact same conclusion as in *Google France*, even referring to the decision. L'Oréal can prohibit eBay from advertising products that infringe on L'Oréal's trademarks, as long as certain conditions are met.[208] Unsurprisingly, the conclusion regarding liability was much the same as in *Google France* due to the near identical questions. The Court found that a service provider does not fall within the scope of Article 14 "where the service provider, instead of confining itself to providing that service neutrally by a merely technical and automatic processing of the data provided by its customers, plays an active role of such a kind as to give it knowledge of, or control over, those data".[209] The important question then was whether eBay played an active role or not. That is where eBay differed from Google. Google had setup an automated and passive system, whereas eBay was actively promoting its sellers in multiple ways.[210] The Court held that a service provider cannot rely on the hosting safe harbor of Article 14 of the ECD if:

> "the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers

[203] Opinion of Advocate General Jääskinen, L'Oréal, 2010, para 34.
[204] L'Oréal v. eBay C-324/09, para 33.
[205] Opinion of Advocate General Jääskinen, L'Oréal, 2010, para 34-36.
[206] L'Oréal v. eBay C-324/09, para 50.
[207] *Id*. at para 50.
[208] *Id*. at para 94, 97.
[209] *Id*. at para 113.
[210] *Id*. at para 114, 116.

but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale."[211]

The Court concluded that it was for the referring court to examine whether eBay played such a role or not.[212] Moreover, the Court held that the service provider could not rely on exemption from liability "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful and, in the event of it being so aware, failed to act expeditiously in accordance with Article 14(1)(b) of Directive 2000/31.".[213]

The decision does manage to shed some light on the interpretation of Article 14 by providing an example of what constitutes an "active" service provider. Apparently, optimizing the presentation and promoting offers implies that the service provider might have played an active role, thus becoming liable. In contrast, based on *Google France* and *L'Oréal*, it should be safe to say that making money on the service, providing general information, and setting terms of service does not mean that the service provider has played an active role.[214]

3.1.4 No Obligation to Monitor

Article 15 of the ECD is a prohibition against imposing a general obligation to monitor on online service providers. The prohibition applies to services covered by Article 12-14 when they transmit or store information.[215] Article 15(1) also stipulates that Member States shall not impose a general obligation "actively to seek facts or circumstances indicating illegal activity". The former rule means that service providers do not have an obligation to passively observe activity on their platform, whereas the latter means that the service providers do not have an obligation to actively seek infringements.[216] Essentially, service providers do not have to do anything to detect infringements on their platforms.

[211] *Id*. at para 116.
[212] *Id*. at para 117.
[213] *Id*. at para 120.
[214] Hoboken 2019, p. 33; Savin 2017, p. 161; Husovec 2017, p. 20.
[215] Article 15(1) Directive 2000/31/EC.
[216] Savin 2017, p. 162.

Pursuant to Article 15(2), the service provider does nonetheless have to cooperate with authorities. Member States may establish obligations for service providers to inform authorities of alleged illegal activities at the authorities' request. Authorities have the right to receive "information enabling the identification of recipients with whom the service providers have storage agreements."[217]

The primary rule is, that abstract non-target filtering is a violation of free speech and is therefore banned. Unsurprisingly, there are exceptions to the ban on monitoring content. Plenty of CJEU cases touch on the topic of Article 15, as the rights-holders are keen on finding ways to protects their assets. *L'Oréal*[218] is a good example of a case where the referring court asked a plethora of questions, including one about monitoring. In that case, the CJEU held that measures may be taken by a trading platform against repeated infringers.[219] *McFadden*[220] is another case that touched on the topic of monitoring. That time, the CJEU held that password-locking is an appropriate measure to stop infringing activity on an open Wi-Fi network.[221] The CJEU has both ruled for some exceptions to the general rule of Article 15 and against violations of its principles.

One of the most notable rulings relating to Article 15, is *Eva Glawischnig-Piesczek v Facebook Ireland Limited*.[222] In 2016, a Facebook[223] user shared an article on his Facebook wall, generating a thumbnail with the photograph of Ms. Glawischnig-Piesczek—an Austrian politician of The Greens parliamentary party.[224] The user also published defamatory comments about Ms. Glawischnig-Piesczek in connection to the article.[225] A few months after the Facebook post was published, Ms. Glawischnig-Piesczek requested Facebook Ireland to take it down.[226] Facebook did not comply with Ms. Glawischnig-Piesczek's request, so she decided to bring action before the Austrian Commercial Court. The Court issued an interim order to disable access to the

[217] Article 15(2) Directive 2000/31/EC.
[218] L'Oréal v. eBay C-324/09.
[219] *Id*. at para 139.
[220] McFadden v. Sony Music C-484/14.
[221] *Id*. at para 90.
[222] Case C-18/18.
[223] *See* Opinion of Advocate General Szpunar, Glawischnig-Piesczek, 2019, para 11. Facebook Ireland Limited is a subsidiary of the U.S. corporation Facebook Inc. with headquarters in Dublin, and it operates a social media platform for users outside the U.S. and Canada. Facebook is accessible at the address www.facebook.com. Facebook requires users to create a profile, after which users have access to the service where they can e.g., publish comments.
[224] Eva Glawischnig-Piesczek v. Facebook Ireland Limited C-18/18, para 11.
[225] *Id*. at para 12.
[226] *Id*. at para 13.

defamatory post. Facebook did disable access to the content, but only in Austria.[227] The decision was appealed all the way to the Supreme Court of Austria.[228] The Supreme Court decided to stay the proceedings and refer a few questions to the CJEU for a preliminary ruling.

The Supreme Court essentially asked whether Article 15(1) precluded courts from:

i. ordering online service providers to remove or block access to content that is "identical" to content which was previously declared illegal
ii. ordering online service providers to remove or block access to content that is "equivalent" to content which was previously declared illegal
iii. ruling for a worldwide injunction.[229]

The CJEU held that despite Article 15(1) prohibiting a general obligation to monitor content, it does not prohibit courts from ordering an obligation to monitor "in a specific case".[230] A good example of such a specific case is when the court has already declared content to be illegal.[231] Given that it is so effortless to reupload or share content on social media platforms, it is quite likely that the defamatory content would show up again, if the platform does not prevent it.[232] If the content is already declared illegal, it does not matter who requests the storage of said information, the service provider may be ordered to take it down regardless. This does not mean that the service provider has a general obligation to monitor content, instead it must target the infringing content.[233]

The CJEU noted that the effects of an injunction could easily be circumvented if users were allowed to post equivalent content that was only slightly altered from the original illegal post. The CJEU held that "in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives effectively, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the

[227] *Id*. at paras 14-15.
[228] *Id*. at paras 16-18.
[229] *Id*. at paras 20-21.
[230] *Id*. at para 34.
[231] *Id*. at para 35.
[232] *Id*. at para 36.
[233] *Id*. at para 37.

information whose content was declared to be illegal".[234] The Court found it to be necessary to extend the monitoring to equivalent content, in order to effectively protect a person's reputation and honor.[235] The biggest problem with extending monitoring to equivalent content, is to outline what exactly constitutes "equivalent" content. The decision mentions that "specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal"[236], can be used to identify equivalent content. The Court does not go into more detail about how the service provider should identify "equivalent" content, leaving it ambiguously up for interpretation.

Lastly, the CJEU held, referring to Article 18(1), that the ECD does not have any territorial limitation to the scope of the measures which Member States are entitled to adopt.[237] However, the Court noted that it is up to the national court to ensure that the EU rules are consistent with the international laws.[238] The CJEU merely found that the ECD itself does not restrict a global reach.

To sum up the takeaway, the CJEU ruled that courts may impose an obligation on service providers to remove identical and equivalent content to what has already been declared illegal. The Court justified its approach with the desire to provide people with effective protection against defamatory content. Any other conclusion would have made it significantly harder for the infringed party to take effective action. The only puzzling question is, how exactly the service providers should determine what content is "equivalent" to the original content. The Court did provide some guidelines, but it will surely be a topic of discussion in the future.

The CJEU has also ruled against the use of filtering mechanisms pursuant to Article 15 of the ECD. There are two such cases involving the same plaintiff—SABAM. SABAM is a Belgian collective management organization that represents authors, composers, and publishers.[239] One of its responsibilities is to authorize the use of copyright-protected works for third parties.[240]

---

[234] *Id*. at para 41.
[235] *Id*. at para 44.
[236] *Id*. at para 45.
[237] *Id*. at para 49.
[238] *Id*. at paras 51-52.
[239] About Sabam. Retrieved March 24, 2021, from https://www.sabam.be/en/about-sabam/about-sabam
[240] SABAM v. Netlog NV C-360/10, para 15; Scarlet Extended SA v. SABAM C-70/10, para 15.

Both in *SABAM v. Netlog NV*[241] and in *Scarlet Extended SA v. SABAM*[242], SABAM tried to impose filtering systems on service providers in order to protect copyrights. Netlog was an "online social networking platform" where members could create a profile, chat, play games, share videos and pictures and so on. Scarlet, on the other hand, is an Internet service provider which merely provides access to the Internet. Netlog and Scarlet did have something in common, people used their services to illegally distribute copyright-protected works such as movies and music.

In both cases, SABAM brought action against the defendants demanding them, inter alia, to "cease and desist from making available to the public musical and audio-visual works from SABAM's repertoire without the necessary authorization"[243]. The Belgian courts were uncertain about the legality of such injunctions and decided to refer the question to the CJEU. In both cases, the referred questions are almost identical word for word.

The referring courts asked, in essence, whether Directives 2000/31, 2001/29, 2004/48, 95/46 and 2002/58, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction against a hosting service provider or an ISP which requires it to install a system for filtering:

i. information which is stored on its servers by its service users;
ii. all electronic communications passing via its services, in particular those involving the use of peer-to-peer software;
iii. which applies indiscriminately to all of those users;
iv. as a preventative measure;
v. exclusively at its expense; and
vi. for an unlimited period,

which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual property rights, with a

[241] Case C-360/10.
[242] Case C-70/10.
[243] SABAM v. Netlog NV C-360/10, para 20; Scarlet Extended SA v. SABAM C-70/10, para 20: "SABAM also sought an order requiring Scarlet to bring such infringements to an end by blocking, or making it impossible for its customers to send or receive in any way, files containing a musical work using peer-to-peer software without the permission of the rightholders, on pain of a periodic penalty".

view to preventing those works from being made available to the public in breach of copyright or blocking the transfer of files the sharing of which infringes copyright ('the contested filtering system').[244]

Implementing such filtering system would require the service providers to:

i. identify within all of the electronic communications of all its customers, the files relating to peer-to-peer traffic;[245]
ii. identify the files containing works in respect of which holders of intellectual-property rights claim to hold rights;
iii. determine which of those files are being stored and made available to the public unlawfully; and
iv. block file sharing that it considers to be unlawful[246]

In order to be able to carry out all of the aforementioned measures, the service provider would effectively have to implement general monitoring, which is prohibited by Article 15(1) of the ECD.[247] Moreover, such injunction would seriously infringe the service provider's freedom to conduct business since it would have to implement complicated, costly, and permanent technological solutions at its own expense, which Article 3(1) of Directive 2004/48 prohibits.[248] Lastly, the CJEU voiced its concerns about the injunction restricting access to information. A general monitoring system would more than likely also block some legal content and infringe on the right to protection of personal data, thus violating Articles 8 and 11 of the EU Charter of Fundamental Rights.[249] In both cases, the CJEU concluded that the legal framework of the EU precluded an injunction made against a service provider which would require it to implement a general monitoring system.[250]

Courts appear to have an inclination to impose monitoring on service providers, whereas Article 15(1) of the ECD expressly forbids a general obligation to monitor.[251] Cases such as *UPC*

[244] SABAM v. Netlog NV C-360/10, para 26; Scarlet Extended SA v. SABAM C-70/10, para 29.
[245] Scarlet Extended SA v. SABAM C-70/10.
[246] SABAM v. Netlog NV C-360/10, para 36; Scarlet Extended SA v. SABAM C-70/10, para 38.
[247] SABAM v. Netlog NV C-360/10, para 38; Scarlet Extended SA v. SABAM C-70/10, para 40.
[248] SABAM v. Netlog NV C-360/10, para 46; Scarlet Extended SA v. SABAM C-70/10, para 48.
[249] SABAM v. Netlog NV C-360/10, paras 48–50; Scarlet Extended SA v. SABAM C-70/10, paras 50–52.
[250] SABAM v. Netlog NV C-360/10, para 52; Scarlet Extended SA v. SABAM C-70/10, para 54.
[251] van Eecken 2011, p. 1501–1502.

Telekabel Wien[252], *Glawischnig-Piesczek*, *McFadden*, *Google France* and *L'Oréal* have all established some kind of limitations to the "no general obligation to monitor" rule. Conversely, the two *SABAM*-cases represent a stricter interpretation of Article 15(1). However, it must be noted that SABAM demanded much more extensive monitoring systems than any of the other aforementioned plaintiffs, which ultimately, is the reason behind the denial by the CJEU. It is apparent that the CJEU attempts to walk a fine line between protecting the rights-holders and protecting the service providers along with their users. Article 15(1) does evidently not provide full immunity for service providers against the need to filter or monitor content. Instead, it prohibits authorities from imposing an extensive filtering system that would be unconscionably expensive to implement and intrusive against the users.

3.2 DSM Directive

The Directive on Copyright in the Digital Single Market (DSMD)[253] is an EU directive which came into force on June 6, 2019. Member States are supposed to implement the directive by the summer of 2021. The DSMD updates the EU's copyright legislation, which comprises of 11 directives. The directive supplements the existing legislation, rather than replacing it. The aim of the directive is to adapt certain key exceptions to copyright to the digital and the cross-border environment, improve licensing practices and ensure wider access to content, and to achieve a well-functioning marketplace for copyright.[254] Essentially, it is an effort to close the alleged "value gap" between online intermediaries and copyright holders, or in other words, an attempt to ensure that copyright holders get remunerated appropriately.[255]

Article 17 is one of the most intricate and contentious articles of the directive.[256] It is a significant step towards consolidating the transformation of online intermediaries[257] from passive neutral services to active 'gate-keepers', through legislative means.[258] The provision limits itself to

[252] UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH C-314/12.
[253] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
[254] DSMD Document Summary. Retrieved March 20, 2021, from https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32019L0790
[255] *See* Mendis et al. 2020, p. 559; Frosio 2017b, p. 567–568; Quintais 2019, p. 17.
[256] *See e.g.*, Metzger 2020, p. 1.
[257] Article 17 DSMD uses the term "online content-sharing service provider". For readability and consistence reasons I use the synonyms "online intermediary" and "online service provider", unless I am quoting.
[258] Mendis et al. 2020, p. 557.

online intermediary liability relating to copyright infringing user-generated content. It does not affect the existing intermediary liability framework related to other illegal content such as defamatory statements, hate speech, violations of privacy, etc.[259] Article 17 is an extensive provision with loads of substance, but I will attempt to break down its focal parts and analyze how it will affect online intermediary liability in the EU. What Article 17 does, is it in fact introduces a new type of safe harbor by imposing new obligations on online intermediaries.[260] Consequently, the important question is what online intermediaries must do in order to avoid liability under Article 17. The answer can be broken down into two main parts: licensing and other conditions.

The directive introduces a new obligation for online intermediaries to obtain authorization from copyright holders, for instance by concluding a licensing agreement, in order to make publicly available copyright protected works.[261] This policy also excludes the application of Article 14 ECD,[262] making online intermediaries clearly liable for user-uploaded copyright-infringing content on their platform, unless they meet the requirements of the Article 17 DSMD safe harbor.[263] There are some valid concerns with making licensing the primary way to avoid liability for online intermediaries. The practical process of concluding licensing agreements with all the rightsholders is a daunting, if not impossible task. The obvious solution is to turn to collecting societies. Though, even if the online intermediary finds a collecting society willing to enter into a licensing agreement with the umbrella effect meant in Article 17(2), it will still not solve the problem, for the collecting society landscape in Europe is highly fragmented.[264] Large online platforms will have more resources and leverage to negotiate licenses across the EU. The licensing obligation may thus bestow upon big players a competitive advantage that leads to further market concentration. The licensing obligation could lead to a decline in diversity of both content and service providers, making it a twofold risk from the perspective of both public and private interests.[265] Concluding licensing agreements with reasonable terms could also prove to be a challenge, especially for smaller actors, considering the preemptive nature of the

[259] *Id.* at p. 560–562.
[260] Husovec – Quintais 2021, p. 7.
[261] Article 17(1) and 17(2) Directive (EU) 2019/790.
[262] Article 17(3) Directive (EU) 2019/790.
[263] Garstka 2019, p. 4; Curto 2020, p. 89.
[264] Senftleben 2019, p. 4.
[265] *Id.*at p. 9.

agreement.[266] In a lot of cases, neither contracting party will have knowledge of the quantity or quality of content that will be used.

The other component of Article 17 DSMD is what happens when the online intermediary fails to obtain a licensing agreement. Under certain conditions the online intermediary can still be exempt from liability. The conditions are that the service provider has to demonstrate that it has:

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)."[267]

Additionally, Article 17(5) DSMD stipulates that, among others, the type of service and content, the audience and the size of the service, and the availability of suitable and effective means and their cost for service providers are elements that shall be taken into account when determining whether the service provider has complied with its obligations under paragraph 4.

The first thing that stands out is the number of conditions combined with equivocal word choices. Expressions such as "best efforts", "high industry standards", "relevant and necessary information", and "expeditiously", combined with most of paragraph 5, may very well cause confusion in national courts down the road and it will likely fall to the CJEU to interpret the meaning of such expressions.[268]

Perhaps the biggest concern with the new provision is Article 17(4)(b), which requires the service provider to "make best efforts" to ensure the unavailability of infringing content. Some scholars are concerned that it will culminate in a comprehensive filtering obligation,[269] even

[266] Ahmaoja 2019, p. 878.
[267] Article 17(4) Directive (EU) 2019/790.
[268] *See* Edwards 2019, p. 270.
[269] *See e.g.*, Senftleben 2019, p. 7–8.

though Article 17(8) DSMD and Article 15 ECD explicitly forbids it.[270] Despite this, it may be argued that the ISPs will still be forced to implement filtering measures mainly "to ensure the unavailability of specific works. Such obligation would also be a big concern considering fundamental rights to impart and receive information.[271] The way Article 17(4) is phrased, it is less risky for service providers to filter too much than it is to filter only clear-cut cases of infringement. At the current level of technological sophistication, algorithms are often unable to accurately identify the nuances between unauthorized and permissible use of copyright-protected content.[272] Moreover, the provision does not provide any strong incentives for service providers to be cautious of over-blocking.[273] The stricter filtering obligation signifies a change in the perception of online intermediaries from being passive players to being active gate-keepers with the duty to avert the posting of infringing content on platforms managed by them.[274]

Articles 17(6) and 17(7) contain exceptions to liability imposed by Article 17. Online intermediaries that have been available to the public in the EU for less than three years and that have an annual turnover below EUR 10 million do not need to comply with Article 17(4)(b). In other words, the monitoring obligation does not concern newer small service providers. The other exception is a special regime for fair use. The fair use exceptions are quotation, criticism, review, caricature, parody, and pastiche. Previously, these were optional exceptions,[275] but now the exceptions have become mandatory.[276] On the face of it, these mandatory exceptions are great for freedom of expression. However, this provision too runs the risk of being difficult to accurately interpret despite a valiant effort to explain the exception in Recital 70 DSMD.

The provision is also equipped with a section about redress procedure. Article 17(9) stipulates that service providers must have an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of content uploaded by them. In other words, there needs to be a counter notice system for the users of the service. The provision goes on to require that counter notices are processed without “undue delay” and decisions to disable access to or remove uploaded content

[270] *See e.g.*, Curto 2020, p. 92.
[271] Mendis et al. 2020, p. 563.
[272] *See* Frosio 2011, p. 135–141; Mendis et al. 2020, p. 563.
[273] Senftleben 2019, p. 8.
[274] Mendis et al. 2020, p. 546.
[275] Article 5(3) Directive 2001/29/EC.
[276] Husovec – Quintais 2021, p. 14.

are subject to human review. Moreover, out-of-court redress mechanisms shall be available for the settlement of disputes. If it takes a long time for users to get the decision, it is foreseeable that the complaint and redress is incapable of safeguarding freedom of expression.[277] Even a delay of a few days can make a significant difference for a content provider in the competitive online environment. Article 17(9) only regulates disputes over disabling of access to, or the removal or content. It was perhaps an oversight not to include monetization claims in the provision.[278] Monetization claims are common on platforms such as Youtube and make up a significant portion of all the copyright disputes on the platform. Why take down the content if you can claim the monetization instead?

Article 17 is part of a broader policy push in the EU towards increased responsibility of online platforms, which comes largely at the cost of increased monitoring obligations and reduced freedom for users to engage with content online.[279] Article 17 DSMD represents the withdrawal from a broad international harmony with legislation such as the DMCA. As large platforms face increasing scrutiny from lawmakers on issues unrelated to copyright, the political balance of power could shift in ways that would also embolden critics of the DMCA in the U.S.[280] Varying national legal systems already create substantial uncertainty for online intermediaries as they face different liabilities and safe harbors depending on the applicable law. The fragmentation of online intermediary liability legislation caused by the implementation of Article 17 may slow down the growth of online service providers and perhaps even negatively impact the global economy.[281] It remains to be seen whether the legislative revision of the role of online intermediaries under Article 17 as regards copyright-protected content will expand to other areas of intermediary liability such as defamation and hate speech.[282]

[277] Senftleben 2019, p. 9.
[278] Garstka 2019, p. 12.
[279] Quintais 2019, p. 17.
[280] Lerner 2020, p. 368.
[281] Curto 2020, p. 99
[282] Mendis et al. 2020, p. 565.

4 Comparative Analysis

4.1 Knowledge of Infringement

The role of intermediaries' knowledge of infringement has been a topic of debate for decades. In the landmark case *Smith v California* from 1959, the U.S. Supreme Court held that content distributors cannot be held liable for third-party content, unless they knew or had reason to know about the infringing content. The two cases involving *Hustler* in the 1980s, demonstrated well the significance of awareness. In the two nearly indistinguishable cases, the court came to two completely different conclusions about intermediary liability due to the intermediary's knowledge of infringement. The swift technological development and the rise of online service providers in the 1990s threw a wrench in the works. Some service providers decided to moderate the content on their platform, while others did not. This led to a problem with the decades old *Smith* rule. Service providers that moderated content were considered to become aware of infringing content on their platforms, thus losing the status of distributor and becoming distributors instead. *CompuServe* and *Prodigy* came to embodiments of the absurdity also sometimes referred to as the "Good Samaritan paradox". The Good Samaritan paradox disincentivizes service providers to proactively monitor the legality of the material they host because, if they do so, they may lose the benefit of the liability exemption.[283] This issue has been dealt with differently in different statutes.

The first statute to address the Good Samaritan paradox was Section 230. Section 230 tackles the issue by guaranteeing protection for all service providers regardless of their awareness. Section 230(c) is even titled "Protection for Good Samaritan blocking and screening of offensive material". In the early days on online intermediaries, the concern was that online intermediaries are not effectively allowed to moderate user-generated content. Now it has changed and there are concerns that online intermediaries do not moderate content even though there are calls for them to do so. Some argue that they reap the benefits of immunity without monitoring.[284] Actually, online intermediaries never had an obligation to moderate content before the Section 230 either. Historically speaking, the immunity was not granted to intermediaries so that they could

[283] De Streel et al.2018, p. 18.
[284] *See e.g.*, Dickinson 2010, p. 870.

monitor content, it was to guarantee freedom of expression.[285] Perhaps, it is a valid concern that the unconditional immunity of all online intermediaries might be fostering a hands-off approach because it is easier and cheaper.[286] It is also worth noting that a lot of services might want to moderate content in order to appeal to a broader audience, as was the case with Prodigy.[287]

The DMCA and the ECD contain a much different approach to knowledge of infringement.[288] Many of their safe harbor provisions include a condition that the service provider must not have actual knowledge of illegal activity nor awareness of facts or circumstances from which the illegal activity or information is apparent. It effectively means that Section 230 affords online intermediaries far greater protection from liability than what the DMCA and the ECD does.

The recently adopted Article 17 DSMD brings yet another approach to knowledge of infringement by not even mentioning it. It does not offer complete protection like Section 230 does, but it does neither explicitly rule out exemption from liability if the online intermediary had knowledge or reason to know about the infringement. As long as the online intermediary conforms to Article 17(4), it should gain protection from liability regardless of its level of awareness.

The safe harbor schemes of Section 230 and Article 17 DSMD have the advantage of not needing to deal with the problem of determining when the online intermediary has had knowledge or should have known about an infringement. On the contrary, there has been plenty of debate about the knowledge issue in cases that fall outside of the scope of Section 230 and DSMD. Perhaps the most compelling argument regarding knowledge of infringement relates to inducing illegal activity. In *L'Oréal,* the CJEU made the connection that taking an active role in facilitating, or in other words, inducing illegal activity leads to knowledge of infringement. "Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data

[285] Smith v. California, 361 US 147, 172 n.1 (1959).
[286] Sevanian 2014, p. 136–137.
[287] Goldman 2020, p. 164.
[288] Article 14(1)(a) ECD is almost word for word a copy of DMCA 512(c)(1)(a).

relating to those offers for sale.", the CJEU wrote.[289] Nevertheless, for example in the *Betamax* case, the U.S. Supreme did not make the same connection, even though both subjects were under close scrutiny. It is worth noting though that *Betamax* predates any online intermediaries, which may explain the discrepancy. Inducing illegal activity might be one possible indicator to determine whether the online intermediary, but it is certainly not the entire solution. Safe harbor schemes such as Section 230 and Article 17 DSMD have the advantage of being unambiguous as there is nothing left for interpretation regarding the online intermediary's knowledge of infringement.

4.2 Notice-and-Takedown

Notice-and-takedown is a process which allows rightsholders to request online intermediaries to remove or disable access to infringing user-generated content. It is a negligence-based approach, meaning that it is a reactive rather than a proactive obligation for intermediaries[290] As one might expect, Section 230 does not include such a scheme due to the complete immunity from liability that the law affords online intermediaries. Likewise, unsurprisingly, the DMCA and the ECD contain paragraphs on notice-and-takedown with almost the exact same phrasing.[291] However, there is one significant difference between the DMCA's and the ECD's notice-and-takedown regulation. Unlike the DMCA, the ECD does not define what constitutes a proper takedown notice.[292] In the EU, it is up to each Member State to establish more specific procedures and requirements. The distinction can therefore more likely be attributed to political reasons than any legal argument. Lastly, Article 17(4)(c) DSMD also includes a notice-and-takedown policy. The DSMD notice-and-takedown policy is sort of a hybrid of the latter two. It does not go into as much detail as section 512(c)(3) DMCA, but it offers more than the provisions in the ECD. According to Article 17(4)(c) DSMD, online intermediaries must take action "upon receiving a sufficiently substantiated notice from the rightholders". "Sufficiently substantiated notice" goes straight to the rather lengthy list of ambiguous and thus problematic expressions of the DSMD. Alas, Recital 66 DSMD which refers to the notice-and-takedown policy, does not provide any further help with the interpretation of what "sufficiently substantiated

[289] L'Oréal v. eBay C-324/09, para 116.
[290] Mendis et al. 2020, p. 546.
[291] *See e.g.*, 17 U.S.C. § 512(c)(1) and Article 14(1)(b) ECD.
[292] *See* 17 U.S.C. § 512(c)(3) and Recital 46 ECD.

notice" exactly means. Article 17(4)(c) DSMD is also unique in the sense that it obligates service providers to make "best efforts" to prevent future uploads of content that has been taken down once. It means the DSMD's notice-and-takedown scheme is in fact a notice-and-stay down scheme. In conclusion, two of the statutes include very similar notice-and-takedown policies, in fact one is actually a notice-and-stay down scheme, and Section 230 stands out by affording a uniquely broad protection for online intermediaries by not having a scheme at all.

Notice-and-takedown schemes certainly have both advantages and disadvantages. Perhaps the loudest criticism relates to the chilling effect that notice-and-takedown procedures have on free speech. It is widely recognized that notice-and-takedown policies make service providers remove content too easily in fear of liability.[293] Challenging the takedown requests may be an unappealing option due to intimidation, high legal risks, and a weak prospect of a successful redress.[294] Service providers appear to fear lawsuits from rightsholders more than they do from users, which is not surprising considering the discrepancy in power between rightsholders and users on average. Not only is content being removed or disabled too easily, but takedown notices are also sent too often without any legitimate justification. A study conducted in the U.S. reveals that up to 30% of DMCA takedown notices were legally dubious, and 57% of DMCA notices were filed against competitors.[295] This is at least partly believed to be due to the ease of the process.[296] Senders of unwarranted takedown requests could perhaps be better held accountable with stricter liability. Currently, notice senders are rarely held liable for abusive requests.[297]Another reason for the high rate of bogus notices can be attributed to the large quantity of takedown notices that are sent by automated algorithmic systems. Lots of companies, especially large companies, use automated algorithmic systems due to their low maintenance costs and high efficiency. Google has possibly the most well-known content filtering system in the world called "Content ID". Still, the convenience and low maintenance costs comes at the price of high error rate.[298] Google's Content ID has been called a "censorship machine", rightsholders are

[293] *See e.g.*, Savin 2017, p. 159; Urban – Karaganis – Schofield 2017; Garstka, Krzysztof 2019; Frosio 2016, p. 3.
[294] Fiala – Husovec 2018, p. 3.
[295] Urban – Quilter 2006, p. 621.
[296] *See e.g.*, Elkin-Koren 2017; Goldman 2020, p. 168.
[297] Kuczerawy 2020, p. 530–531.
[298] Edwards 2019, p. 272.

effectively forced to surrender control of their intellectual property to Google and content providers have very limited redress mechanisms at their disposal.[299]

Without a doubt, the amount of bogus takedown notices that are being sent is a substantial problem with notice-and-takedown schemes. The technological development is most likely only going to boost the presence of automated algorithmic systems. On the upside, algorithms will surely improve over time on recognizing infringing content correctly and thus lowering the rate of dubious takedown requests. In the meantime, legislators ought to ensure that content providers have access to effective redress mechanisms such as a well-functioning counter-notice system. A fast, balanced redress procedure can mitigate any damage done to the freedom of expression. Even if the content is found infringing in the end, the right to a fair trial demands that the uploader should be given an adequate opportunity to challenge the takedown notice.[300]

While the DMCA offers content providers the opportunity to file counter-notices and rebut unfounded takedown requests, the mechanism is utilized relatively rarely.[301] The reason for such low utilization, is that content providers have to state, under penalty of perjury, that they have a good faith belief that the material was removed or disabled as a result of a mistake or misidentification.[302] Such imbalance in risk for the rightsholder and the content provider is problematic. It is problematic that the sender of a takedown notice faces so little liability while content providers may, in fear of liability, not appeal takedown requests even when they know they are right. Pursuant to the Finnish implementation of the ECD, the takedown notice must state the reason for removal of the content and provide information on the right to appeal in a court.[303] Informing the content provider of the charges brings an element of the right to a fair hearing into the process. Curiously, also Article 17(9) DSMD provides that rightsholders "shall duly justify the reasons" for their takedown requests. Article 17(9) DSMD indicates that perhaps the less harmonized solution of the ECD was not enough to ensure the rights of content providers.

While Article 17(4)(c) DSMD is the only out of the four statutes analyzed that contains an explicit notice-and-stay down policy, it is actually not the first one to enable such a policy. CJEU's

[299] *Id.* at. p. 275.
[300] Garstka 2019, p. 10.
[301] Urban – Quilter 2006, p. 621.
[302] Kuczerawy 2020, p. 532.
[303] The Finnish Information Society Code (917/2014) (n. 13) s. 187.

landmark decision *Glawischnig-Piesczek* from 2018, introduced a notice-and-stay down mechanism in the EU, which obligates online intermediaries to block content that is identical or similar to the infringing content. The logic of a notice-and-stay down policy is however nothing new. The similar logic was applied decades earlier in *Spence v. Flynt* on the other side of the Atlantic Ocean. After Park Place had been sued once earlier for distributing defamatory content, they could no longer claim to not know about the nature of said content. The first lawsuit essentially served as a rudimentary notice-and-stay down request way ahead of its time. Evidently, it was not called by that name, but the logic was largely the same. Notice-and-stay down does not come without its problems. The policy effectively leads to a monitoring obligation for the service provider, which in itself is problematic on multiple levels.[304]

Imperfect as the notice-and-takedown and stay down mechanisms are, they embed a fundamental safeguard for freedom of information as long as they force intermediaries to actually consider the infringing nature of the content before deciding whether to take action.[305] In the end, the notice-and-takedown procedure is one of the essential mechanisms through which a balance between the interests of rightholders, online intermediaries and users is achieved.[306] That is, unless legislators decide to go for the Section 230 approach which affords online intermediaries full protection from liability for user generated content.

4.3 Content Filtering and Blocking

Content filtering and blocking is a continuation to the notice-and-stay down discussion and a partly overlapping subject. None of the safe harbor policies include an explicit general obligation to monitor content, but the legislation in the EU requires service providers to block content identical or similar to previously blocked content, as was explained in the previous chapter. Remarkably, both Article 15 ECD and Article 17(8) DSMD explicitly state that the safe harbor provisions shall not lead to any general monitoring obligation. Still, it may be argued that the notice-and-stay down procedure in fact culminates in a comprehensive filtering obligation. This corresponds with the filtering measures which are forbidden by the aforementioned provisions

[304] *See* Kuczerawy 2020 p. 538; Elliot Harmon, '"Notice-and-Stay-Down" Is Really "Filter-Everything"' (EFF, 21 January 2016). Retrieved April 2, 2021, from https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything
[305] Geiger et al. 2020, p. 145.
[306] Van Eecke 2011, p. 1479–1480.

and that the CJEU has prohibited in *Sabam v. Netlog*.[307] The functionality of the technical side of blocking certain content without screening all content is outside the scope of this research but it is worth noting. Despite proactive general monitoring not being explicitly imposed by law, online service providers have begun to voluntarily implement content filtering systems as a means of protecting themselves from lawsuits with regards to user generated content.[308] A perfect example of this is Google's previously mentioned Content ID.

There is a global trend supported by legislators, courts, rightsholders and even online service providers that inclines towards the imposition of proactive monitoring and filtering obligations on online service providers.[309] However, not everyone is in favor of the trend as it is a cause of valid concern. An ex-ante procedure based on filtering and automatic infringement-assessment systems that online service providers might deploy to monitor content, might disproportionally favor property rights against other fundamental rights, namely freedom of expression.[310] An ex-ante procedure that filters all user generated content before it is uploaded is essentially a form of censorship. To put it into perspective, such conduct would be in direct conflict with the U.S. Supreme Court's *Farmers Union v. WDAY* decision from 1959 in which the Court held that filtering content was censorship and that it would violate the First Amendment. Nevertheless, to this day, the U.S. legislation does offer intermediaries broader protection from liability. Another concern pertains to the present level of technological sophistication.

Much like the automated algorithmic systems send a lot of unjustified takedown notices, they also generate an abundance of false positives when filtering content, leading to overblocking and jeopardizing the fundamental right to freedom of expression.[311] A common reason for false positives is that an algorithmic system has difficulties recognizing when the use of copyrighted content falls under fair use.[312] Manual assessment would be desirable, especially when dealing with fair use. To require humans to assess content that falls under fair use is a tricky proposition as well. The financial burden of online service providers should not become disproportionate either.[313] A possible solution would be to let content creators label content as fair use which the

[307] Senftleben 2019, p. 7–8.
[308] Mendis 2020, p. 555.
[309] *Id*. at p. 564.
[310] *See* SABAM v Netlog C-360/10 (n. 3) para. 52.
[311] Geiger et al. 2020, p. 146; Garstka 2019, p. 6.
[312] *See* SABAM v Netlog C-360/10 (n. 3) para. 50.
[313] *See* Geiger – Izyumenko 2020, p. 578.

service provider would then manually review. The obvious flaw with such a system is that it could be easily abused by users in the hopes of bypassing the automated filter and getting infringing content published. Whatever the solution to false positives may be, the situation must improve.

The future of content filtering does not appear trouble-free. Emerging technology and trends consistently challenge the filtering procedures. For example, live streaming is currently wildly popular, and it poses new challenges to content filtering systems.[314] Everything happens in real time, so there is no way to review the content in advance. Perhaps, this is an aspect that the algorithmic systems may be able to address in the future when they become more advanced. If the problems pertaining to censorship and freedom of speech cannot be soon solved, maybe it is time to look for other alternatives. For example, a detect and notify procedure could be a better approach than detect and block from a freedom of expression point of view.[315] The Section 230 model with broader protection ought to be also considered in the EU to ensure that the fundamental rights are respected.

4.4 Liability for User-Generated Content

Doctrines of intermediary liability can be best explained by intermediaries' assumption of responsibility for primary wrongdoers.[316] The doctrines have been based on different theories ranging from moral to utilitarian approaches.[317] The intermediaries are oftentimes much easier to identify, contact, and hold accountable than the users of their services. Arguably, online service providers are also able to intervene in infringing behavior on their service making it convenient to impose liability on them instead of only the users. For rightsholders, it is usually futile trying to track down users and seek redress from them.[318]

Of the four statutes analyzed, it is only Section 230 that provides a completely unique solution to the intermediary liability question. Section 230 provides online service providers full immunity from liability for third-party infringements with a few exceptions, namely concerning

[314] Common 2019, p. 6.
[315] Garstka 2019, p. 9–10.
[316] Curto 2020, p. 88.
[317] Frosio 2017a, p. 25.
[318] Geiger et al. 2020, p. 75.

intellectual property and sex trafficking.[319] The DMCA, the ECD, and the DSMD all encompass compromises between liability and no intermediary liability for third-party infringements. Online service providers are exempt from liability only if they conform to certain conditions set by the safe harbor provisions. All three statutes have slightly different conditions, but the logic remains the same. The conditions and their intricate elements are important, but only if such conditions exist at all. As was demonstrated in the previous chapters, mechanisms such as notice-and-takedown or content filtering are only relevant if the safe harbor procedure imposes conditions, meaning that they are not even considerations in the context of Section 230. At the end of the day, the greater question encompassing all four statutes is whether the safe harbors should exist at all.

Perhaps the most prominent argument against the safe harbors is the alleged "value gap". Value gap refers to an alleged mismatch between the value that online service providers are perceived as obtaining from protected content and the revenue returned to relevant rightsholders.[320] According to the theory, rightsholders are forced to accept low royalty rates because online intermediaries can otherwise simply turn down license deals and exploit the protection provided by the safe harbors.[321] Youtube is a prime example of a service that allegedly unfairly favors the platform over the rightsholders. "When we negotiate with YouTube, they can practically name their own price. If we refuse their offer, they might choose to pay nothing at all, pointing to the so-called 'Safe Harbour' exemption. But the Safe Harbour rule is completely obsolete and out of date with our present situation", said Anders Lassen, the former CEO of the Danish collecting society KODA.[322] The statement sums up well the sentiment of a lot of rightsholders—online service providers abuse the safe harbors to implement an "act first, license later" approach, coercing rightsholders to agree to unfair terms on a take-it-or-leave-it basis.

Allegedly, the imbalance in power exists due to online service providers being immune to liability and therefore having insufficient incentives to enter into ex-ante licensing agreements with rightsholders.[323] One study suggests that the DMCA's safe harbor provisions cost the U.S. music

[319] *See* 47 U.S. Code § 230(e) for complete list of the exceptions.
[320] Rosati 2019, p. 200–201.
[321] Elkin-Koren et al. 2019, p. 9.
[322] KODA Annual Report 2017.
[323] Elkin-Koren et al. 2019, p. 31.

industry up to one billion dollars a year in lost royalties.[324] Additionally, rightsholders claim that safe harbors put an enormous burden on them to enforce their rights, forcing them to constantly monitor online content for infringements.[325] The claim is difficult to approve in light of the increasing demands on online service providers to filter user uploaded content. Sure, rightsholders must protect their rights, but it is an inherent feature of being a rightsholder and not a consequence of the safe harbor regulation. Nonetheless, there appears to be some validity to the "value gap" argument. Rightsholders are encountering new challenges pertaining to their monetization structures because the way content is consumed is changing. With the soaring popularity of paid services such as Spotify and Netflix, there is light in the end of the tunnel for rightsholders. Spotify and Netflix have been well known to spend considerable amounts of money on licensing deals with rightsholders. While the value gap arguably does exist, at least to some degree, the idea that it does exist due to safe harbors may be questioned. The value gap was not a problem in the early days of the safe harbors. Copyright protected content was still mostly being consumed offline. It is only when the consumption of such content moved to the Internet and rightsholders began making less money, that the value gap discussion started. Rightsholders need to be fairly compensated in healthy economy, it just should not be done at the expense of online service providers.

With critics claiming for example that Section 230 privileges online publishers over their offline counterparts by giving online publishers more favorable legal protection,[326] would it make sense to abolish the safe harbors and revert to how it was before them? There is little doubt that strict liability of online service providers would result in some of them withdrawing from the market or limiting the type and range of the services they provide.[327] There is a direct economic relationship between regulatory burden and development. The more exposed online service providers are to liability, the less likely they are to invest in the development of electronic commerce.[328] Abolishing safe harbors would essentially lead to mandatory filtering, which without a doubt would burden smaller platforms and new entrants to the market.[329] One way to counter the problem could be to implement something like Article 17(6) DSMD that exempts new and small

[324] *See* Beard et al. 2017.
[325] Elkin-Koren et al. 2019, p. 32.
[326] Goldman 2020, p. 162–163
[327] Savin 2017, p. 145.
[328] *Ibid*.
[329] Elkin-Koren et al. 2019, p. 48.

online service providers from liability. Regardless of the countermeasures, it is hard to imagine that a strict liability for online service providers would lead to anything else than concentration of power to the market leaders. The larger the company is, the more resources it has to conform to new regulation. The leading platforms have the resources to implement monitoring systems and procedures, whereas smaller platforms might not.[330] Abolishing the safe harbors could further encourage online service providers to generate their own content in order to obtain the rights, either by backing user-generated content or by producing it themselves.[331] For example Netflix has already undertaken this for years, assumingly to cut back on the licensing fees. This procedure would more than likely become much more beneficial and common. Again, the leading platforms would undoubtedly be able to adapt to such change much more easily than smaller platforms. What exactly the concentration of power to a few leading platforms would mean for the consumers, is hard to tell. From a competition point of view, it would more than likely be a negative change.

Where will the intermediary liability regulation go in the future? The recent regulation in the EU seems to suggest that the safe harbors will not be abolished, at least in the near future. The DSMD, which has not even been fully implemented, is largely in line with the with the ECD. The DSMD actually brings yet another safe harbor to the EU law. The new Directive neither abolishes safe harbors nor affords online service providers complete insulation from liability, it is merely a marginally updated version of the old safe harbors. The legislators in the EU have intentions of further updating the safe harbor regulation. The European Commission has drafted a proposal for the Digital Services Act.[332] At this stage, it is too early to tell if the proposal passes and what it would look like in its final form. On the face of it, it does not seem to propose any radical changes to how intermediary liability works in the EU. Much like the DSMD, it will most likely be a mere update to the existing regulation, if it passes. The changes would concern the notice-and-takedown scheme and other features of the safe harbor procedure rather than being a complete overhaul of intermediary liability. In the U.S., there is nothing as substantial on the horizon. There have been calls from various groups to revamp the legislation, but nothing

[330] *Ibid*.
[331] Dolata 2017; Elkin-Koren et al. 2019, p. 48.
[332] Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Retrieved April 18, 2021, from https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital

tangible has yet been drafted. Perhaps the legislative efforts in the EU will inspire the U.S. to also make either minor updates, or even a complete overhaul of the much-debated Section 230.

5 Conclusions

The question of whether intermediary liability safe harbors should exist or not boils down to which fundamental rights the legislators want to emphasize and protect. The involved parties can be divided into four main groups: intermediaries, users, rightsholders, and governments. Each group has their own set of interests and rights. For example, the freedom to conduct business is an integral fundamental right for intermediaries, whereas the freedom of expression is crucial for the users. Rightsholders want to be fairly remunerated, and governments have a complex responsibility of balancing economics and politics. Governments must respect the fundamental rights while making political decisions that stimulate the economy.

The reason why intermediaries were isolated from liability in the first place can be attributed largely to the freedom of speech. The U.S. Supreme Court believed that imposing liability on intermediaries for third-party content would result in censorship from intermediaries which would consequently stifle free speech. With the rapid increase of online intermediaries in the 1990s, it became apparent that the old policies needed to be adjusted. The reason being that the old policy incentivized intermediaries to adopt a hands-off approach to content moderation. The entire idea of the broad protection afforded by Section 230 is to allow intermediaries to moderate content in order to improve the user experience. Legislators wanted to incentivize intermediaries to create a safe and clean environment without illegal content. Copyright infringement was excluded from Section 230 for political reasons and instead it was included in the DMCA which was enacted in 1998. The EU followed suit and essentially copied the DMCA a couple years later. The DMCA implemented a safe harbor policy which does not unconditionally exempt intermediaries from liability. For intermediaries to be insulated from liability, they must conform with certain conditions. The same procedure can be found in the EU legislation, only with slightly different conditions.

There are three ways to go about changing how intermediary liability works. One option is to provide intermediaries complete insulation from liability, such as is done in Section 230. The second option is to introduce safe harbors that are conditional, such as the DMCA, the ECD, and the DSMD. In the case that conditional safe harbors already exist, the conditions can be adjusted. The third option is to introduce strict liability to intermediaries. Neither the U.S. nor the EU has yet tried employing this option. Since the intermediary liability conundrum involves

lots of competing rights and other interests, there is likely no solution that would satisfy everyone. The only solution that can almost certainly be ruled out is imposing strict liability on intermediaries. If intermediaries were liable for everything that was posted on their platforms, they would undoubtedly have to filter all content ex-ante. Such a solution would seriously violate the freedom of expression. The other two options are proven to work. Both have their advantages and disadvantages and at the end of the day, it is a political decision. From a legal point of view, both are possible.

This study managed to answer the question of what the purpose of safe harbors is. Therefore, there is no apparent reason to conduct further investigation on the same subject. Instead, this study indicates that future research should be focused for example on safe harbor conditions and mechanisms such as notice-and-takedown and content filtering. Investigating the existing procedures and offering solutions to their problems would be useful as there are plenty of unanswered questions pertaining to them. Investigating what implications implementing a broader protection of intermediaries would have on the EU, could similarly be fruitful.

References

Literature

Ahmaoja, M. (2019). Musiikin verkkojakelijoiden lisenssisopimukset ja Youtuben ContentID-järjestelmä DSM-direktiivissä, Lakimies 7–8/2019, 874–895.

Beard, R. et al. (2017). Safe Harbors and the Evolution of Music Retailing (March 2017). Phoenix Center Policy Bulletin No. 41.

Bostoen, F. (2018). Neutrality, fairness or freedom? Principles for platform regulation. Internet Policy Review, 7(1).

Balasubramani, V. (2016). Online intermediary immunity under section 230. Business Lawyer, 72(1), 275-286.

Common, M. F. (2019). Fear the Reaper: How content moderation rules are enforced on social media. International Review of Law, Computers & Technology, (ahead-of-print), pp. 1-27.

Curto, N. (2020). EU Directive on copyright in the digital single market and ISP liability: what's next at international level? Journal of Law, Technology & the Internet, 11, 84–.

De Streel, A. et al. (2018). Liability of online hosting platforms Should exceptionalism end? Center of regulation in Europe.

Dickinson, G. (2010). An interpretive framework for narrower immunity under section 230 of the Communications Decency Act. Harvard Journal of Law and Public Policy, 33(2), 863–.

Dinwoodie, G. (2017). Secondary Liability of Internet Service Providers (1st ed. 2017.). Springer.

Dolata, U. (2017). "Apple, Amazon, Google, Facebook, Microsoft: Market concentration competition - innovation strategies," Research Contributions to Organizational Sociology and Innovation Studies, SOI Discussion Papers 2017-01, University of Stuttgart.

van Eecken, P (2011). "Online service providers and liability: a plea for a balanced approach". Common Market Law Review. 48: 1501–1502.

Edwards, L. (2019). Law, policy, and the Internet. Hart.

Elkin-Koren, N. (2019). Is It Time to Abolish Safe Harbor? When Rhetoric Clouds Policy Goals. Stanford Law & Policy Review.

Elkin-Koren, N. (2017). Fair Use by Design, 64 UCLA L. REV. 1084-5.

Fiala, L. – Husovec, M. (2018). Using Experimental Evidence to Design Optimal Notice and Takedown Process. SSRN Electronic Journal.

Freiwald, S. (2001). Comparative institutional analysis in cyberspace: the case of intermediary liability for defamation. Harvard Journal of Law & Technology, 14(2), 569–.

Frosio, G. (2017a). Internet intermediary liability: Wilmap, theory and trends. Indian Journal of Law and Technology, 13(1), 16-38.

Frosio, G. (2017b). From horizontal to vertical: an intermediary liability earthquake in Europe. Journal of Intellectual Property Law & Practice, 12(7), 565–575.

Frosio, G. (2016). Digital piracy debunked: a short note on digital threats and intermediary liability. Internet Policy Review, 5(1).

Frosio, G. (2011). 'COMMUNIA Final Report on the Digital Public Domain', report prepared for the European Commission on behalf of the COMMUNIA Network and the NEXA Center, 99–103.

Garstka, K. (2019). Guiding the Blind Bloodhounds: How to Mitigate the Risks art. 17 of Directive 2019/970 Poses to the Freedom of Expression.

Geiger et al. (2020), Intermediary Liability and Fundamental Rights. In Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. Oxford University Press.

Geiger, C. – Izyumenko, E. (2020). Blocking Orders: Assessing Tensions with Human Rights. In Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. Oxford University Press.

Goldman, E. (2020). An Overview of the United States' Section 230 Internet Immunity. In Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. Oxford University Press.

Goldman, E. (2015). Proceeding Open Net. Harvard Berkman Center joint seminar on intermediary liability: how the DMCA's online copyright safe harbor failed. Korea University law review, 18, 103–.

Hartmann-Vareilles, F. (2017). Achievements in civil intellectual property enforcement and recent initiatives within the Digital Single Market Strategy on the regulatory environment for platforms and online intermediaries. ERA-Forum, 18(1), 1–6.

Hoboken, J. (2019), Hosting intermediary services and illegal content online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape: final report. Publications Office of the EU.

Hoboken, J. et al. (2018). "Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape". Publication Office of the European Union.

Husovec, M. – Quintais, J. (2021). How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms. GRUR International (Issue 4/2021, forthcoming).

Husovec, M et al. (2020), The e-commerce Directive as the cornerstone of the Internal Market. Study requested by the IMCO committee.

Husovec, M. (2017). Holey cap! CJEU drills (yet) another hole in the e-commerce directive's safe harbors. Journal of Intellectual Property Law & Practice, 12(2), 115–125.

Johnson, R. (1996). Defamation in cyberspace: a court takes a wrong turn on the information superhighway. Arkansas Law Review, 49(3), 589–.

Kane, M. (1999). Blumenthal v. Drudge. Berkeley Technology Law Journal, 14(1), 483–501.

Kosseff, J. (2019). The Twenty-Six Words That Created the Internet. Cornell University Press.

Kuczerawy, A. (2020). From 'Notice-and-takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression, In Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. Oxford University Press.

Legrand, P. (1995). ‘Comparative Legal Studies and Commitment to Theory’, Modern Law Review 58, 262.

Lerner, J. (2020). Secondary Copyright Infringement Liability and User-Generated Content in the United States, In Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. Oxford University Press.

McManus, B. (2001). Rethinking defamation liability for Internet service providers. Suffolk University Law Review, 35(3), 647–.

Mendis, S et al. (2020). Monitoring and Filtering: European Reform or Global Trend? In Oxford Handbook of Online Intermediary Liability. Edited by Giancarlo Frosio. Oxford University Press.

Metzger, A. et al. (2020). Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law – Comment of the European Copyright Society.

Nimmer, D. (2000). A Riff on Fair Use in the Digital Millennium Copyright Act. University of Pennsylvania Law Review, 148(3), 673–742.

Obergfell, E. – Thamer, A. (2017). (Non-)regulation of online platforms and internet intermediaries – the facts: Context and overview of the state of play. Journal of Intellectual Property Law & Practice, 12(5), 435–441.

Pantazis, A. (1999). Zeran v. America Online, Inc.: Insulating Internet service providers from defamation liability. Wake Forest Law Review, 34(2), 531–.

Patel, S. (2002). Immunizing Internet service providers from third-party Internet defamation claims: How far should courts go? Vanderbilt Law Review, 55(2), 647–.

Quintais, J. (2019). The New Copyright in the Digital Single Market Directive: A Critical Look. European Intellectual Property Review 2020(1).

Rosati, E. (2019). Copyright and the Court of Justice of the European Union (First edition). Oxford University Press.

Rozenfeldova, L. – Sokol, P. (2019). Liability Regime of Online Platforms New Approaches and Perspectives. EU and Comparative Law Issues and Challenges Series, 3, 866-887.

Savin, A. (2017). EU Internet law (2nd ed.). Edward Elgar Pub.

Seltzer, W. (2010). Free speech unmoored in copyright's safe harbor: chilling effects of the DMCA on the First Amendment. Harvard Journal of Law & Technology, 24(1), 171–.

Senftleben, M. (2019). Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market.

Sevanian, A. (2014). Section 230 of the Communications Decency Act: a "good Samaritan" law without the requirement of acting as a "good Samaritan." UCLA Entertainment Law Review, 21(1), 121–.

Smits, J. (2017). What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research. In R. van Gestel, H. Micklitz, & E. L. Rubin (Eds.), Rethinking Legal Scholarship: A Transatlantic Dialogue (pp. 207-228). Cambridge University Press.

Strömholm, S. (1971). Användning av utländskt material i juridiska monografier. SvJT 1971, 251-263.

Urban, J. et al. (2017). Notice-and-takedown in Everyday Practice (March 22, 2017). UC Berkeley Public Law Research Paper No. 2755628.

Urban, J. – Quilter, L. (2006). "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", Santa Clara Computer and High Technology Law Journal 22.

Watkins, D. – Burton, M. (2017). Research Methods in Law: Vol. Second edition. Routledge.

Wiener, D. (1999). Negligent publication of statements posted on electronic bulletin boards: is there any liability left after Zeran? Santa Clara Law Review, 39(3), 905–.

Internet sources

1956 North Dakota U.S. Senate Election results. Retrieved January 19, 2021, from https://clerk.house.gov/member_info/electionInfo/1956election.pdf

About Sabam. Retrieved March 24, 2021, from https://www.sabam.be/en/about-sabam/about-sabam

Andrea Dworkin, Britannica. Retrieved January 29, 2021, from https://www.britannica.com/biography/Andrea-Dworkin

Arthur C. Townley, Encyclopedia of the Great Plains. Retrieved January 13, 2021, from http://plainshumanities.unl.edu/encyclopedia/doc/egp.pd.052

Barnes v. Yahoo!, Electronic Frontier Foundation. Retrieved February 21, 2021, from https://www.eff.org/issues/cda230/cases/barnes-v-yahoo

Caching Overview. Retrieved March 12, 2021, from https://aws.amazon.com/caching/

Cambridge Dictionary "hate speech" definition. Retrieved April 11, 2021, from https://dictionary.cambridge.org/us/dictionary/english/hate-speech

CDA 230: Legislative History, Electronic Frontier Foundation. Retrieved February 9, 2021, from https://www.eff.org/issues/cda230/legislative-history

Cosponsors: S.314 — 104th Congress (1995-1996), retrieved February 15, 2021, from https://www.congress.gov/bill/104th-congress/senate-bill/314/cosponsors

DSMD Document Summary. Retrieved March 20, 2021, from https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32019L0790

ECD Document Summary. Retrieved March 8, 2021, from https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32000L0031

Elliot Harmon, '"Notice-and-Stay-Down" Is Really "Filter-Everything"' (EFF, 21 January 2016). Retrieved April 2, 2021, from https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything

Farmers Educational & Cooperative Union of America v. WDAY, Inc. (n.d.). Oyez. Retrieved January 3, 2021, from https://www.oyez.org/cases/1958/248

Farmers Educational Transcript. Retrieved January 3, 2021, from https://www.oyez.org/cases/1958/248

Google Transparency Report, Content delistings due to copyright. Retrieved March 1, 2021, from https://transparencyreport.google.com/copyright/overview?hl=en

KODA Annual Report 2017. Retrieved March 12, 2021, from https://www.koda.dk/media/150394/koda_annual-report-2017.pdf

Oral Argument Transcript, Smith v. California, 361 U.S. 147 (1959). Retrieved January 26, 2021, from https://www.oyez.org/cases/1959/9

Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Retrieved April 18, 2021, from https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-single-market-digital-services-digital

Reno v. ACLU — Challenge to censorship provisions in the Communications Decency Act. Retrieved February 16, 2021, from https://www.aclu.org/cases/reno-v-aclu-challenge-censorship-provisions-communications-decency-act

Section 2: Origins of the nonpartisan league, North Dakota Official State Website. Retrieved January 15, 2021, from https://www.ndstudies.gov/gr8/content/unit-iii-waves-development-1861-1920/lesson-4-alliances-and-conflicts/topic-7-nonpartisan-league-and-iva/section-2-origins-nonpartisan-league

The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary. Retrieved February 26, 2021, from https://www.copyright.gov/legislation/dmca.pdf

Table of Other Documents

Complaint, Cubby v. CompuServe, 90 Civ. 6571 (S.D.N.Y. Oct. 5, 1990)

Complaint, Farmers Educational and Cooperative Union of America, North Dakota Division v. Townley, District Court of Cass County, North Dakota (Jan. 14, 1957)

Demurrer, Farmers Educational and Cooperative union of America, North Dakota Division v. Townley, District Court of Cass County, North Dakota (May. 23, 1957)

European Commission, A European Initiative in Electronic Commerce, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(97)157 (Brussels, 15 April 1997).

European Commission, Staff Working Document Online Platforms, SWD (2016) 172, p. 1.

Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC

Report of the Senate Comm. On the judiciary, S. Rep. No. 105-190, at 2 (1998)

Opinion of Advocate General Jääskinen, L'Oréal, 2010.

Opinion of Advocate General Poiares Maduro, Google France, 2010.

Opinion of Advocate General Szpunar, Glawischnig-Piesczek, 2019.

Table of Cases

U.S.

A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000)

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001)

Anthony v. Yahoo! Inc., 421 F.Supp.2d 1257 (N.D.Cal. 2006)

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

Barrett v. Rosenthal, 114 Cal. App. 4th 1379, 1395 (2004)

Blumenthal v. Drudge, 992 F. Supp 44 (D.D.C. 1998)

Cubby. v. CompuServe, 776 F. Supp. 135 (S.D.N.Y. 1991)

Cubby v. CompuServe, 90 Civ. 6571 (S.D.N.Y. Oct. 5, 1990)

Doe v. MySpace, 528 F.3d 413 (5th Cir. 2008)

Dworkin v. Hustler Magazine, Inc., 611 F. Supp. 781 (D. Wyo. 1985)

Dworkin v. Hustler Magazine, Inc., 867 F. 2d 1188 (9th Cir. 1989)

Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157 (9th Cir. 2008)

Farmers Educational and Cooperative Union of America, North Dakota Division v. WDAY, 89 NW 2d 102, 110 (N.D. 1958)

Farmers Educ. & Co-op. Union v. WDAY, Inc., 360 U.S. 525 (1959)

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

Gucci America, Inc. v. Hall & Associates, 135 F. Supp. 2d 409 (S.D.N.Y. 2001)

MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005)

Osmond v. EWAP, 153 Cal.App.3d 842, 847 (Cal. Ct. App. 1984).

Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993)

Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997)

Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal.

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997)

Smith v. California, 361 US 147, 172 n.1 (1959)

Sony Corp. v. Universal City Studios, 464 U.S. 417 (1984)

Spence v. Flynt, 647 F. Supp. 1266 (D. Wyo. 1986)

Spence v. Flynt, 816 P.2d 771 (Wyo. 1991)

State v. Smith, Superior Court No. CR A 3792, Trial Court No. 57898 (Cal. Ct. App. June 23, 1958)

Stratton Oakmont, Inc. v. Prodigy Services Co., 23 Media L Rep 1794 (Sup. Ct. Nassau Cnty. 1995)

UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011)

Universal City Studios, Inc. v. Sony Corp. of America, 429 F. Supp. 407 (C.D. Cal. 1977)

Universal City Studios, Inc. v. Sony Corp. of America, 659 F.2d 963 (9th Cir. 1982)

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

Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997)

Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997)

EU

Delfi AS v. Estonia 64569/09

Eva Glawischnig-Piesczek v. Facebook Ireland Limited Case C-18/18

Google v. Louis Vuitton C-236/08

L'Oréal v. eBay C-324/09

McFadden v. Sony Music C-484/14

SABAM v Netlog C-360/10

Scarlet Extended SA v. SABAM C-70/10

Sotiris Papasavvas v. O Fileleftheros Dimosia Etairia Ltd., Takis Kounnafi, Giorgos Sertis C-484/14

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

Legislation

U.S.

17 U.S. Code § 107

47 U.S. Code § 230

Communications Act of 1934

Digital Millennium Copyright Act of 1998

Telecommunications Act of 1996

EU

Directive 98/34

Directive 2000/31/EC

Directive 2019/790

Information Society Code (917/2014) (Finland)