CEU CENTRAL EUROPEAN UNIVERSITY

A COMPARATIVE ANALYSIS OF THE EU AND US TRENDS IN REGULATING INTERMEDIARY SERVICE PROVIDER LIABILITY

By Radu Șomlea

LL.M SHORT THESIS
COURSE: Legal Aspects of Internet and Electronic Commerce
PROFESSOR: Dr. Caterina Sganga
Central European University
1051 Budapest, Nador utca 9.
Hungary

Abstract

As the internet evolved to a medium that encourages user creation and participation, this was met with a strong need to enforce intellectual property rights and to establish the role of internet service providers in doing so. This thesis discusses the recent regulatory trends in the field of internet service providers' liability by means of a comparative analysis between the US and EU, since they both provide extensive regulation and case law on this matter and host a big part of the providers' activity. This paper looks at how these two jurisdictions deal with intermediaries' liability, draws attention to the important differences between the two and evaluates what are the prospects in this field, giving its own suggestion. A strong emphasis will be put on the key concept of safe harbor, and how it has been applied by the courts. Finally, this thesis differs from other studies in the field by using the comparative analysis of the actual and proposed ISP liability regimes to come up with one of its own.

Acknowledgement

To begin with, I am extremely grateful to my supervisor, Assistant Professor Caterina Sganga, for being a very encouraging and supportive advisor. Her sheer energy, friendly guidance, and vast knowledge created the spark that ignited my interest for this subject, but also the fuel needed to keep improving and finish the thesis.

I would also like to thank my family, whom I hope I have not neglected too much this past year. Irrespective of this, they showed me nothing else but unconditional love and much needed support. Special thanks go out to my bigger brother, who has always pushed me to challenge and improve myself.

Table of contents

Introduction

One of the very first things I did after entering Central European University's (CEU) wonderful building for the first time was to connect to their available Guest Wi-Fi network. The connection page greeted me with a message and some terms that I had to accept before gaining access to the internet. Like most people do, I clicked on the big blue button without reading any of the text[1]. The second time this messaged appeared, I decided out of curiosity to give it a read.

As it turned out, the text I had previously skipped reading was CEU informing me that, according to the applicable legislation, it qualified as an intermediary service provider (hereinafter ISP). Moreover, the message went on to say that CEU was excluding its liability for any information transmitted through an information society service that consists of the storage of information made available by others, or the provision of access to such information. Finally, it read that CEU has no obligation to monitor any contents that are stored, transmitted, or provided access to through its network.

For myself, this raised started to raise several questions, such as why this step was deemed necessary and after a further incursion in the field of intellectual property and internet law, I decided to tackle these questions in the present thesis.

[1] For a study on how people accept terms and conditions without reading them, see Böhme R and Köpsell S, 'Trained to Accept?: A Field Experiment on Consent Dialogs', Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (ACM 2010) <http://doi.acm.org/10.1145/1753326.1753689> accessed 9 December 2016.

The Internet has grown to being used by a staggering half of the total world population[2]. However, in its rapid development, most aspects of law have been struggling to keep up with this pace. As an US court put it, trying to apply recognized law "in the fast-developing world of the Internet is somewhat like trying to board a moving bus"[3].

In the digital era, anyone with an internet connection can access, modify, copy and distribute copyrighted materials with little effort and with a relative degree of anonymity. This caused the number of copyright infringements to skyrocket, quantity-wise. Quality-wise, online digital copies of content also have the advantage of not degrading in the course of multiplying as would happen with photocopying[4]. Thus, it quickly became obvious to copyright owners that individually enforcing their rights became substantially more difficult, inefficient, and at times even impossible due to the logistics and economic cost of such a pursuit.

The copyright owners then began looking to other places to satisfy their monetary claims and quickly realized that they could successfully bring action against intermediary bodies, which provide the technological means and platforms to individual infringing users. This course of action proved more efficient given that for multiple individual infringements they could seek reparation from only one intermediary. Moreover, these intermediaries were more often than not big companies, which possess the funds to satisfy such claims[5].

[2] International Communications Union, *Worldwide Internet Users* (2016) http://www.internetworldstats.com/stats.htm accessed 9 December 2016

[3] Benusan Restaurant Copr. V. King, 126 F.3d 25 (sd Cir. 1997)

[4] Eric Schlachter, 'The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet Symposium: Digital Content: New Products and New Business Models' (1997) 12 Berkeley Technology Law Journal 15, 19.

[5] Seth A Miller, 'Peer-to-Peer File Distribution: An Analysis of Design, Liability, Litigation, and Potential Solutions Note' (2006) 25 Review of Litigation 181, 187.

Although a clear-cut definition if Internet/Intermediary[6] Service Providers (ISPs) does not exist, they could be described as players present on the World Wide Web that provide users with essential services needed to properly use the internet[7]. In the same way an operating system allows us to fully benefit from the power of its computer, ISPs are the one who truly make the internet the functional tool that it is today. Search engines, host providers, webstores, social networks are just some examples that show the omnipresence of ISPs.

Seeing as the Internet can be used for both legal and illegal activities and that it certain constraints make it impossible for ISPs to track all the content it stores, it would be unreasonable to hold them liable for all types of infringing behavior of third parties if ISPs are not at fault. If this were the case, it would lead to ISPs taking a more defensive stance by blocking actions even if the infringement is not clear. Such a hypothesis would turn out to "impede the development of new technology"[8].

Thus, in recent years there has been a growing need to establish and regulate the role of ISPs in regards to copyright protection[9]. Regulation in this field needs to strike a balance between the interests of the copyright owners, the protection of the ISPs and the unrestricted movement of information. While there is a number of research studies in the field of ISP regulation, the very volatile nature of the subject at hand means that research cannot always keep up. The growing

[6] The terms can be used interchangeably.
[7] Chris Reed and John Angel, *Computer Law: The Law and Regulation of Information Technology* (Oxford : Oxford University Press, 2007) 233.
[8] Jerry Jie Hua, *Toward A More Balanced Approach: Rethinking and Readjusting Copyright Systems in the Digital Network Era. [Electronic Resource]* (Berlin: Springer, 2014) 106.
[9] Matthew Schruers, 'The History and Economics of ISP Liability for Third Party Content' (2002) 88 Virginia Law Review 205, 209.

number of new variables, new technologies such as artificial intelligence, machine learning and new intermediaries open the door to new grounds for analysis.

In order to find the appropriate balance between all the interests at stake, this thesis will analyze the regulatory trends in the field of ISP liability within the two most experienced jurisdictions in this field: the US and the EU. By examining the *status quo* and assessing the future impact of ISP liability regulation, I will look for the ideal regulatory solutions.

The first part of this thesis covers the legal regime of ISP liability within the EU by looking at the E-Commerce Directive and the recent and future regulatory projects part of the Digital Single Market Strategy. The second part is devoted to comparatively exploring how the same issues are dealt with by the US and what the prospects are in this area. Finally, the third chapter deals with analyzing the directions and prospects in the field of ISP liability.

Chapter I. Regulatory trends in the EU

In the European Union, the ISP liability regime is established in Section 4 of the E-Commerce Directive[10]. However, rather than providing for a fully-fledged legal regime, it just sets out the limitations to it, in which cases the liability under national legislation is excluded[11]. The Directive deals with ISP liability limitations horizontally, which means that it covers all types of online third party illicit activity, irrespective of the area of law[12].

The Directive only provides for a minimum standard of what is needed in order to accomplish the goal of a proper functioning internal digital market[13]. Its purpose is to harmonize legislation and case law in this field, however, by being quite vague and broad, the Directive leaves some space for member states to interpret it in line with their policy decisions[14].

It should be noted that the Directive does not affect the Member States' possibility to require the ISP to terminate or to prevent an infringement[15]. Thus, the limitations to ISP liability set forth are only to liability for damages. Moreover, they are only applicable for certain types of

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031 accessed 9 December 2016

[11] Patrick Van Eecke and Barbara Ooms, 'Isp Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for Isps' (2011) 15 Journal of Internet Law 3.

[12] Pablo Asbo Baistrocchi, 'Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce (2002) Santa Clara Computer and High Technology Law Journal 111.

[13] Recital 10 of the Directive 2000/31/EC

[14] Grunde Jørgen Svensøy, 'The E-Commerce Directive Article 14: Liability Exemptions for Hosting Third Party Content' 6 <https://www.mysciencework.com/publication/show/5f0f35a3b076a605c9d2e69762f6c753> accessed 13 February 2017.

[15] Art. 12.3, 13.3 of the Directive 2000/31/EC.

activities, which will be analyzed separately in the following part: (1) mere conduit, (2) caching, and (3) hosting.

1. Mere conduit

One of the ISP activities that is exempt from liability under Article 12 of the E-Commerce Directive is that of "mere conduit" and is a perfect demonstration of the metaphor "don't shoot the messenger"[16]. According to the same provision, this can occur through "the transmission in a communication network of information provided by a recipient of the service" or by providing "access to a communication network". This provision covers the situations where the intermediary merely provides a "two-way channel by means of which information may be transferred"[17], similarly to a post office or a phone company[18]. ISPs in this situation are basically excepted from all liability, provided that they do not initiate the transmission, select the receiver of the transmission and selector modify the information contained in the transmission.

Article 12 also provides that some storage of the information is allowed as long as it is automatic, and it is not stored for more than it is reasonably necessary for the transmission. This is the case of packet switching transmissions and includes temporary storage in routers.[19] Other examples are Internet Service Providers[20], back-bone operators or wireless hotspot providers.

[16] See Gavin Sutter, '"Don"t Shoot the Messenger?'The UK and Online Intermediary Liability' (2003) 17 International Review of Law, Computers & Technology 73.

[17] Reed and Angel (n 5) 242.

[18] Charlotte Waelde and Lilian Edwards, 'Online Intermediaries and Copyright Liability' (Social Science Research Network 2005) SSRN Scholarly Paper ID 1159640 <https://papers.ssrn.com/abstract=1159640> accessed 9 December 2016, 4.

[19] Van Eecke and Ooms (n 11) 4.

[20] In this case meaning an organization that provides internet access to its subscribers, usually at a monthly or yearly fee. Also called Internet Access Providers.

Regarding wireless hotspots, one very interesting issue arose recently before the CJEU in the preliminary ruling of McFadden C-484/14[21]. The Court was asked to clarify whether a person offering an unprotected Wi-Fi network counts as an online intermediary and what are the remedies that can be brought against him.

The fact pattern of the case was a pretty simple one. Tobias McFadden, a shop owner in Germany owned a Wi-Fi network connection in his store and made the access to the hotspot unrestricted to the public and without any password protection in order to attract customers. In 2010, a person using that network illegally downloaded material copyrighted by Sony. Sony gave McFadden a formal notice, allowing him an opportunity to settle the dispute by giving an undertaking to refrain from further commission of the infringement, coupled with an appropriate contractual penalty. McFadden then turned to the local courts to seek a negative declaration, but to his surprise, the court upheld Sony's claim, holding him directly liable and ordering him to pay damages and costs. Following his appeal, the regional Court held that McFadden would be indirectly liable but sought clarification from the CJEU on the points above.

First, the Luxembourg Court of Justice said that "making a Wi-Fi network available to the general public free of charge in order to draw the attention of potential customers to the goods and services of a shop constitutes an *information society service* under the directive", thus McFadden did act as an intermediary online service provider. This is important because the Court further found that according to the Directive, his actions counted as "mere conduct" and Sony's claim in damages should be unsuccessful.

[21] Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, C-484/14, CJEU, Third Chamber

Second, seeing as the Directive does not prohibit Member States to ordering an injunction[22] on the infringing actions the court held that this can be done by ordering the owner of the network to secure it by means of a password. This was however contrary to opinion of the Attorney General, who held that such an injunction should not go to require demand the provider to terminate or protect the internet connection with a password[23].

The CJEU noticed that this measure will be "striking a fair balance between, first, the fundamental right to protection of intellectual property and, second, the right to freedom to conduct the business of a provider supplying the service of access to a communication network and the right to freedom of information of the recipients of that service"[24]. According to the Court, such a measure could deter users from any infringing behavior, however it could be also strengthened by requiring users to provide some identity details before obtaining the password.

As regards to the costs of the notice and proceedings, CJEU agreed with the Attorney General[25], and noted that "since such a claim cannot be successful, the copyright holder is also precluded from claiming the reimbursement" of such costs[26].

In conclusion, the CJEU upheld the mere conduit safe harbor in the case of having a free, non-password-protected WiFi hotspot. However, more importantly, it still allowed for an

[22] Nedim Malovic, 'Online Copyright Enforcement in Sweden: The First Blocking Injunction' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2940786 2 <https://papers.ssrn.com/abstract=2940786> accessed 5 April 2017.

[23] Advocate General's Opinion in Case C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH para. 86 http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-03/cp160028en.pdf, accessed 1 April 2017.

[24] Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, C-484/14, CJEU, Third Chamber, para. 100

[25] Advocate General's Opinion in Case C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH para. 77 http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-03/cp160028en.pdf, accessed 1 April 2017

[26] Court of Justice of the European Union PRESS RELEASE No 99/16 Luxembourg, 15 September 2016 http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160099en.pdf Accessed 10 December 2016

injunction to be issued against the provider of such a hotspot in order to limit, or restrict the access to such a network, when users on it are infringing copyrighted content.

2. Caching

The Directive defines caching as the automatic, intermediate, and temporary storage of data in local servers, for the purpose of facilitating delivery to users in the quickest way of repetitive, high demand material[27]. Given that such a speeding up of the Internet should not be discouraged[28], the E-Commerce Directive also limits the intermediaries' liability, given that they satisfy the conditions set out in Article 13.

According to them, in order for the provider to benefit from the safe harbor provision, it must not modify in any way the information stored, it must comply with the conditions to access the information and the rules concerning updating the information, which are specified in a manner widely recognized and used by the industry. Most importantly, the provider must act 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".[29]

However, an apparent contradiction seems to arise. How are ISPs to obtain such actual knowledge if monitoring is prohibited under Article 15? First, it should be noted that Recital 48 of the Directive imposes a duty of care on providers to detect and prevent certain types of illegal

[27] Baistrocchi (n 12).
[28] Waelde and Edwards (n 18) 24.
[29] E-Commerce Directive, art. 13.1 (e).

activities. However, some scholars believe that this is too contradictory to Article 15 to be taken into account[30]. Second, other authors believe that such actual information has to be obtained via third party notices and not through its own inquiry[31].

This particular safe harbor provided by the Directive does not raise any big problems. The fact that there have been very few cases regarding the caching requirement set forth in Article 13 effectively shows that it mirrors quite well the actual needs of the industry[32].

3. **Hosting**

Finally, according to the E-Commerce Directive, hosting is "the storage of information provided by a recipient of the service"[33]. When providing such services, an ISP will not be held liable for any infringing content as long as it does not have actual knowledge of the illegal activity and upon obtaining such knowledge it acts expeditiously to remove or to disable access to the information. However, an ISP will not be without liability when "the recipient of the service is acting under the authority or the control of the provider"[34], which emphasizes the rationale behind limiting the liability of providers who don't have any control over the data[35].

As one can notice, the definition of "hosting" is quite vague and can encompass many different actions. While this can often be seen as a bad thing, this vagueness had its purpose in a

[30] Rosa Julià-Barceló and Kamiel J Koelman, 'Intermediary Liability: Intermediary Liability in the E-Commerce Directive: So Far So Good, But It's Not Enough' (2000) 16 Computer Law & Security Review 231-239.

[31] Baistrocchi (n 12) 122.

[32] Svensøy (n 14) 13.

[33] E-Commerce Directive, art. 14(1).

[34] Id., art. 14(2)

[35] Baistrocchi (n 9) 122.

ever developing field such as Internet law. In 2000, when the Directive saw first light, hosting referred mainly to "renting" space on a server where users could store a website[36]. However, almost two decades later, the so-called Web 2.0 features a lot more user-created content thanks to technological developments in speed and storage capacity deemed inconceivable at the beginning of the new millennium[37]. Thus, the interpretation given to "hosting" evolved to accommodate the more content-related meaning.

In the Google France v. Louis Vuitton case[38], the CJEU defined storage of information in the "hosting" sense in a very broad way: holding certain data on its server's memory. More importantly, the same case established in what cases ISPs fall under the host provider category under the Directive. The court held that the ISP should pass a neutrality test, meaning that its conduct should be "merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores"[39].

With respects to the knowledge requirement, the Directive differentiates between criminal liability and civil liability. As such, a provider will not be liable for monetary damages as long as it is not aware of facts that point to an infringing activity. In most member states this condition

[36] Giovanni Sartor, Viola de Azevedo Cunha and Mario, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1604411 370 <https://papers.ssrn.com/abstract=1604411> accessed 13 February 2017.

[37] Svensøy (n 14) 20.

[38] C-236/08, para. 111

[39] Id., para 113

was interpreted as being met as long as there was no gross negligence of the ISP[40]. The awareness has to be not only regarding the content itself but also to its unlawfulness[41].

Nevertheless, an ISP will gain the shield of liability only in exchange for using its sword in a duty to cooperate[42]. As mentioned above[43], because there is no obligation of the providers to actually monitor the hosted content, ISPs will have to become aware of infringing content through the notice of third parties. However, the new proposed Directive on Copyright in the Digital Single Market might indicate a paradigm shift in this regard.

4. The proposal for a Directive on copyright in the Digital Single Market

In their effort to achieve a digital single market, a space where digital networks and services can prosper, which should improve access to digital goods and services, and which should act as a driver for growth[44], the European Commission published its proposed Directive on copyright in the Digital Single Market (proposed directive) on 14 September 2016 shortly after being leaked in August[45]. According to its explanatory memorandum, there was a need to adapt the framework of

[40] Thibault Verbiest, Gerald Spindler and Giovanni Maria Riccio, 'Study on the Liability of Internet Intermediaries' (Social Science Research Network 2007) SSRN Scholarly Paper ID 2575069 37 <https://papers.ssrn.com/abstract=2575069> accessed 14 February 2017.

[41] Svensøy (n 14) 38.

[42] Zucconi Galli Fonseca and Giuseppe Lorenzo, 'Intermediaries Liability for Online Copyright Infringements: The Duty to Cooperate Under E.U. Law' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2714269 10 <https://papers.ssrn.com/abstract=2714269> accessed 14 February 2017.

[43] Supra, 12

[44] The policy areas according to the Digital Single Market website https://ec.europa.eu/commission/priorities/digital-single-market_en accessed 16 February 2017.

[45] For the news on the Directive being leaked, see Eleonora Rosati, 'SUPER KAT-EXCLUSIVE: Here's Draft Directive on Copyright in the Digital Single Market' <http://ipkitten.blogspot.com/2016/08/super-kat-exclusive-heres-draft.html> accessed 16 February 2017.

the copyright environment and to "clarify the role of online services in the distribution of works and other subject-matter"[46].

Interestingly, Article 1(2) of the proposed directive explicitly states that it shall not modify other directives within the copyright legal framework and enumerates them, skipping the E-Commerce Directive. This might be because, as mentioned above, it has a horizontal approach, also dealing with tortious and criminal liabilities. As a result, if the proposed directive is passed in its current version, it can and will change the ISP liability regime within the E-Commerce directive.

Article 13 and Recitals 38 and 39 are the European Commission's way of addressing the issues regarding "distribution of value in the online copyright value chain"[47]. It does so by requiring ISPs "that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users"[48] to collaborate with rightholders, become licensed and to use appropriate and proportionate measures to protect copyrighted works by implementing effective filtering technologies.

Requiring ISPs to use automated means, such as content recognition, to detect illicit content is forcing providers to actively monitor all the data of each of their users and will amount to a general monitoring obligation on these providers[49]. This goes directly against Article 15 of the E-

[46] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market (Text with EEA relevance), Brussels, 14.9.2016
< http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593> accessed 16 February 2017.
[47] Commission Staff Working Document Impact Assessment on the modernisation of EU copyright rules, Accompanying the proposed directive, Brussels, 14.9.2016
<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0301> accessed 16 February 2017
[48] Article 13(1) of the proposed directive
[49] Sophie Stalla-Bourdillon and others, 'An Academic Perspective on the Copyright Reform' (2017) 33 Computer Law & Security Review 3, 4.

Commerce Directive and the established case law[50] to create "systemic inconsistency within EU law"[51].

This blatant contradiction will create a legal uncertainty and as a result an instability on the ISP market. Second, if such a monitoring obligation is imposed it might have the opposite intended effect of increasing the value gap even more. While automatic content recognition technologies might be affordable to giants such as YouTube and Google, it will represent a heavy burden for prospective new players on the market. To put things into perspective, YouTube has reportedly invested years' worth of work and more than $60 million in developing the "Content ID" system[52]. Requiring such a costly technological prerequisite only accessible to some players on the market would have the effect of stifling innovation and discouraging investment in competing platforms[53]. All this would eventually lead to less competition, at the obvious detriment of the consumers[54].

Moreover, the most established market players are US-based[55]. Thus, imposing such a burden on new players on the EU market might "push the Digital Single Market further away, rather than promoting it"[56]. All in all, more thought needs to be given to the proposed directive, as it raises some big problems.

[50] See Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10 (ECJ, November 24, 2011); Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, C-360/10 (ECJ, February 16,.

[51] Giancarlo F Frosio, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2912272 18 <https://papers.ssrn.com/abstract=2912272> accessed 5 April 2017.

[52] How Google Fights Piracy Report, 2016 https://drive.google.com/file/d/0BwxyRPFduTN2TmpGajJ6TnRLaDA/view, accessed 25 March 2017, 6.

[53] Annemarie Bridy and Daphne Keller, 'U.S. Copyright Office Section 512 Study: Comments in Response to Second Notice of Inquiry' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2920871 <https://papers.ssrn.com/abstract=2920871> accessed 27 March 2017, 3.

[54] See Martin Husovec, 'Accountable, Not Liable: Injunctions Against Intermediaries' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2773768 <https://papers.ssrn.com/abstract=2773768> accessed 27 March 2017.

[55] Google, YouTube, Audible Magic (providing filtering technologies to Facebook)

[56] Frosio (n 51) 20.

Chapter II. Regulatory trends in the US

On the other side of the ocean, the Digital Millennium Copyright Act[57] (DMCA) took effect almost two decades ago,[58] establishing a system of safe harbors for ISPs, meant to strike a balance between the interests of content owners and tech companies[59]. Although the E-Commerce Directive, enacted two years later, drew inspiration from the DMCA[60] and the two are similar in their essence, there are several differences between the two systems.

1. The DMCA §512 and E-Commerce Directive common points

In a similar fashion to the E-Commerce Directive, the DMCA grants immunity from liability for damages to ISPS that deal with transitory digital network communications (mere conduit), system caching, information residing on systems or networks at the direction of users (hosting) and providing information location tools.

1.1 Transitory Digital Network Communications

The first safe harbor shields ISPs that are "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such

[57] Digital Millennium Copyright Act, §512. https://www.law.cornell.edu/uscode/text/17/512, accessed 24 March 2017

[58] More precisely, on28 October 1998

[59] Miquel Peguera, 'Secondary Liability for Copyright Infringement in the Web 2.0 Environment: Some Reflections on Viacom v. Youtube' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1716773 2 <https://papers.ssrn.com/abstract=1716773> accessed 24 March 2017.

[60] Miquel Peguera, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1468433 482 <https://papers.ssrn.com/abstract=1468433> accessed 24 March 2017.

transmitting, routing, or providing connections"[61]. In layman terms, this is the mere conduit exception, also adopted by the E-Commerce Directive, which shields ISPs when they transmit data through automatic means without making any changes to the content, the destination and without retaining it for longer than necessary[62]. Moreover, unlike the other safe harbors, mere conduit does not create an obligation for the ISP to remove, or disable access to materials subject to infringement claims from owners.

As this does not create any special difficulties, and is almost identical with the E-Commerce Directive provision[63], which was discussed above, it will not be treated in greater detail.

1.2 System Caching

The provision in 512(b) provides protection to ISPs that intermediately and temporarily store "material on a system or network"[64] as part of increasing its speed and performance[65]. The transmission must be initiated by a third party, transmitted through the system to a second user, and stored via automatic processes.

As the case with the mere conduit safe harbor, the issue of system caching did not present any pressing difficulties in practice and the European approach discussed in a previous chapter is quite similar.

[61] DMCA §512(a)
[62] Jennifer Bretan, 'Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA' (2003) 18 Berkeley Technology Law Journal 43, 49.
[63] Supra, 11
[64] DMCA §512 (b)(1)
[65] Bretan (n 62) 49.

2. Differences from the European model

To begin with, unlike the E-Commerce Directive, the DMCA takes a vertical approach in regulating ISP liability, namely it only deals with such liability arising out of copyright infringement. Thus, in the US, the elements needed to establish ISP liability, or the lack thereof, are different depending on the type of infringing activity[66] and are covered by different legislative acts[67].

Second, under both systems, an ISP whose activity falls under one of the safe harbors will not be liable for any monetary relief[68], however, the US system has certain restrictions in place for granting an injunctive relief[69], whereas in the EU there are no such limits[70]. For example, when an ISP qualifies for the "mere conduit" safe harbor[71], the sole type of injunctive relief possible is an order for the ISP to terminate the accounts of an infringing user or to restrain it "from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States"[72]. Furthermore, a court must take certain specific factors into account before granting these already limited types of injunctive relief[73]. For this, the DMCA put in place a proportionality test to check if the measure is too burdensome on the ISP and whether there are other, more appropriate measures of restraining access to the infringing material.

Third, the DMCA has one important feature that the E-Commerce directive lacks i.e. the obligation on ISPs to put in place a notice and take-down procedure[74]. This system places the

[66] Mark A Lemley, 'Rationalizing Internet Safe Harbors' (Social Science Research Network 2007) SSRN Scholarly Paper ID 979836 <https://papers.ssrn.com/abstract=979836> accessed 25 March 2017.
[67] E.g. The Communications Decency Act
[68] Peguera (n 60) 485.
[69] DMCA §512(j)
[70] See Recital 45 of the E-Commerce Directive
[71] DMCA §512(a)
[72] DMCA §512(j)(B)
[73] Peguera (n 60) 486.
[74] DMCA §512(c)(3)

burden on the copyright holders to notify ISPs of infringing content, after which the providers must take it down in order to avoid liability[75]. More important than creating the obligation of ISPs to quickly respond to such notices, the DMCA also specifically sets out the conditions for such a notice to effectively create this obligation for the providers. This provides a greater certainty to ISPs which will know when a notice is proper and should comply with it. If a notice fails to meet the requirements of §512(c)(3)(A), the text of the next paragraph specifically states that it will not be considered "in determining whether a service provider actual knowledge or awareness of facts or circumstances from which infringing activity is apparent"[76].

In contrast, the E-Commerce Directive adopted a different approach by encouraging self-regulation in this field. Although the directive did indeed foresee in its final provisions[77] the prospect for regulating notice and take-down procedures, out of all Member States, only Finland[78], Hungary[79], and Lithuania[80] have codified notice and take-down procedures for copyright infringements.

Fourth, regarding the level of knowledge required from an ISP to not benefit from liability exceptions the DMCA and the E-Commerce Directive have strikingly similar language[81]. They both to refer to the need for an ISP to have "actual knowledge" or to be "aware of facts and circumstances" from which the infringing activity is "apparent"[82]. However, there is one notable

[75] Eric Goldman, 'How the DMCA's Online Copyright Safe Harbor Failed' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2589751 195 <https://papers.ssrn.com/abstract=2589751> accessed 25 March 2017.
[76] DMCA §512(c)(3)(B)
[77] E-Commerce Directive, art. 21(2)
[78] See First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Brussels, 21.11.2003 COM(2003) 702 final; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF accessed 25 March 2017.
[79] Gerald Spindler, Study on Liability of Internet Intermediaries – Hungary – Executive Summary 12/11/2007; http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/hungary_12nov2007_en.pdf accessed 25 March 2017.
[80] Verbiest, Spindler and Riccio (n 40) 108.
[81] Peguera (n 60) 487.
[82] DMCA §512(c)(1)(A) and E-Commerce Directive, art. 14.1.

difference in treatment of these two different levels of awareness. In the US, an ISP will be liable for monetary relief and will have an obligation to remove the material irrespective of the fact that it had actual knowledge or awareness of the facts and circumstances. On other hand, under the E-Commerce Directive, an ISP might be even criminally liable, however only if it meets the actual knowledge standard[83].

Moreover, both statutes are silent on what amounts to such an actual knowledge or awareness. However, this ambiguity tends to affect more ISPs in the EU precisely because of the lack of a statutory notice procedure. In the US, providers rely more on the rule of the notice and take-down procedure as that is the main source of actual knowledge[84].

Finally, another important difference between the two systems is the fact that §512(d)(2) of the DMCA has an extra prerequisite for the hosting and location tool safe harbors. Thus, to be shielded from liability, an ISP providing hosting or location tools service must 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". According to some scholars, this *financial benefit* requirement creates a loophole in the safe harbor as ISPs will be held liable whenever money is being made and it is proven that there was more that the ISP could have done[85]. As the

3. **Proposed changes**

3.1 The Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA)

[83] Peguera (n 60) 487.
[84] ibid 489.
[85] ibid 491; Edward Lee, 'Decoding the DMCA Safe Harbors' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1333709 5 <https://papers.ssrn.com/abstract=1333709> accessed 26 March 2017; Lemley (n 66) 114.

The declared purpose of SOPA was to "promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property, and for other purposes"[86]. The highly controversial act was mean to improve the enforcement of intellectual property rights, with a focus on infringements coming from entities outside the territory of the US[87]. According to it, a website is dedicated to theft of US property if "enables, or facilitates" copyright infringement. In such a case, an obligation may be born for the providers to take down the entire website and just single files[88]. The bigger problem with this act, as some authors noticed[89] is that the language was considered to be much too vague and uncertain. Such an Act ran the risk of opening the floodgates to infringement claims against ISPs that ran sites which also help others to infringe copyrights[90].

The Protect Intellectual Property Act[91] was the companion statute to SOPA and allowed the Attorney General to sue any ISP owning or operating sites "dedicated to infringing activities" and where this the sole "significant use"[92]. While it may seem at first that the requirements under PIPA are harder to satisfy, the language of this act was too broad as well with no definition on what amounts as "significant use". Moreover, it used the same language as SOPA when defining the sites dedicated to infringing as ones that don't have other significant use other than "enabling or facilitating infringement" which, in turn, means that most of the sites on the Internet could fall under its mischief[93].

[86] The Stop Online Piracy Act Bill, H. R. 3261/2011, https://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf accessed 25 March 2017
[87] Gary Myers, *Principles of Intellectual Property Law* (West Academic 2017) 473.
[88] Michael Rustad, *Global Internet Law* (St Paul, MN : West Academic Publishing, [2016] 796.
[89] Michael A Carrier, 'SOPA, PIPA, ACTA, TPP: An Alphabet Soup of Innovation-Stifling Copyright Legislation and Agreements' (Social Science Research Network 2013) SSRN Scholarly Paper ID 2213034 para 6 <https://papers.ssrn.com/abstract=2213034> accessed 26 March 2017.
[90] ibid.
[91] The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PIPA), S. 968/2011; http://www.gpo.gov/fdsys/pkg/BILLS-112s968rs/pdf/BILLS-112s968rs.pdf accessed 25 March 2017.
[92] Carrier (n 89) para 9.
[93] ibid 11.

Moreover, although the bills' main targets were the "worst of the worst foreign websites", they also applied to US websites[94]. Most importantly, if a website fell under the requirements of the two acts, the ISP could not benefit from the protection of the DMCA safe harbors. Thus, a website could satisfy DMCA's safe harbor requirements, and even comply with cease-and-desist notice but still be dedicated to infringing activity under SOPA and PIPA. Although the DMCA would protect it against damages and other injunctions, the website and ISP would still be subject to the remedies provided by the two acts.

In response to this chilling effect that this act was going to create on the freedom of the Internet, the Internet fought back. Around eight million attempted calls and four million emails were sent to representatives[95]. Some of the biggest websites and ISPs such as Google, Wikipedia, WordPress, Amazon and about 100.000 other websites joined forces in what was to be the largest online protest in the world[96] against an act that would "stifle commerce and discourse on the internet"[97]. The Congress caved under such a pressure, after most of the support for the bills fell and merely two days after the mass protest, on 20 January 2012 both bills were abandoned[98].

3.2 The Trans-Pacific Partnership

The Trans-Pacific Partnership (TPP)[99] is one of biggest regional trade agreements, to which the US made a proposal for a chapter on certain Internet related provisions. Although initially, the

[94] Jonathan Band, 'The SOPA-TPP Nexus' [2012] PIJIP Research Paper Series <http://digitalcommons.wcl.american.edu/research/28>, 5.
[95] For more figures, see 'The Numbers on #SOPASTRIKE' <http://sopastrike.com/numbers> accessed 27 March 2017.
[96] Newton Lee, *Facebook Nation: Total Information Awareness* (Springer Science & Business Media 2012) 128.
[97] Myers (n 87) 152.
[98] Lee (n 96) 128.
[99] The Trans Pacific Partnership Agreement (TPP) Intellectual Property Rights Chapter, available at http://keepthewebopen.com/tpp; accessed 27 March 2017.

negotiations for such a draft were made in secret[100], its text was leaked to the press in March 2011[101]. In it, copyright infringement through internet piracy on a commercial scale was seen as a serious threat that had to be dealt with through criminal penalties[102].

Its text provides that criminal liability could apply in cases of "significant willful" infringement without requiring "direct or indirect motivation of financial gain"[103]. According to scholars, this could have had far-reaching consequences[104]. Also reaching expansively could be the conception of willful infringement for receiving (or even expecting) financial gain, which, again, signifies "anything of value."

3.3 The US Copyright Office final rule regarding registering agents

On November 1, 2016, in an effort to modernize its practices, the US Copyright Office, issued a final rule[105] which put a new electronic registration system in place. Before it, ISPs had to submit paper designations of agents assigned to receive notifications of claimed infringement to the Office, which were scanned and posted on the Office's website to make them available to the public[106]. The rule entered force on December 1, 2016 and grants ISPs a thirteen-month period in which they must make the transition to the online registration system.

However, the more important issue to notice with this new rule is that it adds a periodic renewal requirement, even if the information does not change. Under it, an agent's designation will expire after three years, at which point the ISP should renew it if it wishes to keep its "safe

[100] Carrier (n 89) para 20.
[101] Band (n 94) 14.
[102] Carrier (n 89) para 21.
[103] TPP, Article 15(1)(a)
[104] Band (n 94) para 22.
[105] 37 C.F.R. § 201.38 https://www.law.cornell.edu/cfr/text/37/201.38 accessed 27 March 2017.
[106] Copyright Office, Frequently Asked Questions, Designation of Agents to Receive Notifications of Claimed Infringement https://www.copyright.gov/rulemaking/onlinesp/NPR/faq.html accessed 27 March 2017.

harbor status"[107]. Since renewal was not obligatory before, many companies run the risk of forgetting to re-register and unknowingly leave themselves potentially vulnerable to infringement claims[108]. Precisely because it is an apparent minor change ISPs might fail to comply with the requirements out of ignorance or error. Despite being quite a minor change, it has the potential to have a major practical impact by denying safe harbor protection to companies based on a technicality.

3.4 Changes to the take-down notice system and fair use

As previously stated, the notice and take-down procedure in §512(c) of the DMCA is one of the staples of the ISP liability regime in the US. Under it, once an ISP receives a take-down notice that complies with the DMCA requirements, it must act expeditiously in removing the alleged infringing content to benefit from the immunity to damages. However, several scholars have argued that the ease with which copyright owners can request removing material without any prior notice to the actual publisher, can have chilling effects on the freedom of expression, innovation, and even scientific research[109].

While the DMCA certainly did not mark the end of free speech on the Internet as we know it, as some pessimist scholars perceived it[110], it was plainly open to abuses. This is mostly the case

[107] Jeffrey D Neuburger, 'Copyright Office Establishes New Electronic DMCA Agent Registration' (2017) 29 Intellectual Property & Technology Law Journal 18.
[108] Copyright Office, Frequently Asked Questions, Designation of Agents to Receive Notifications of Claimed Infringement https://www.copyright.gov/rulemaking/onlinesp/NPR/faq.html accessed 27 March 2017
[109] See Derek J Schaffner, 'The Digital Millennium Copyright Act: Overextension of Copyright Protection and the Unintended Chilling Effects on Fair Use, Free Speech, and Innovation Notes' (2004) 14 Cornell Journal of Law and Public Policy 145; Wendy Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1577785 <https://papers.ssrn.com/abstract=1577785> accessed 27 March 2017.
[110] Marc J Randazza, 'Lenz v. Universal: A Call to Reform Section 512(f) of the DMCA and to Strengthen Fair Use' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2773137 105 <https://papers.ssrn.com/abstract=2773137> accessed 27 March 2017.

because take-down notices can be used for other purposes apart from their intended one, and the DMCA provides little to no protection against such claims because even when the notices are not legitimate, content is still taken down out of fear of lawsuits or ignorance[111]. Thus, notices have been used to take down content for reasons other than copyright infringement, such as unfair competition[112], a form of prior constraint or can be simply erroneous[113].

The DMCA attempted to put in place a system in place to counter such frivolous or erroneous notices. Section 512(f) states that any person who "knowingly materially misrepresents" that the material or activity subject to the notice is infringing or was removed erroneously will be held liable for damages. Moreover, §512(g) allows users to submit counter-notices to ISPs that require them to remove the restrictions on the content. However, there are several issues with this system.

First, per §512(g)(2)(B), the content will only be re-uploaded within 10 to 14 working days, which might be enough to effectively cause harm. For example, in 2008, some political advertisements featuring John McCain, a presidential candidate at that time, were subject of take-down based of "dubious copyright claims"[114]. The videos re-appeared online, however only after a ten-day period and as the General Counsel of the McCain campaign noted, this procedure provided "inadequate protection for political speech […] as 10 days can be a lifetime in a political campaign"[115].

[111] See Daniel Seng, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2411915 <https://papers.ssrn.com/abstract=2411915> accessed 28 March 2017.
[112] Jennifer Urban and Laura Quilter, 'Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara High Technology Law Journal 621.
[113] Randazza (n 110) 107.
[114] Matthew Sag, 'Internet Safe Harbors and the Transformation of Copyright Law' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2830184 7 <https://papers.ssrn.com/abstract=2830184> accessed 28 March 2017.
[115] Trevor Potter's letter to Chad Hurley, YouTube's CEO, dated October 13 2008, available at https://www.eff.org/files/mccain_youtube_copyright_letter_10.13.08.pdf, accessed 27 March 28, 2017.

Second, subsection (g)(3)(D) requires the sender of a counter-notification to disclose "name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located"[116]. According to some authors, even the mere possibility of a lawsuit is enough of a deterrent for the average user[117].

Finally, the *Lenz v. Universal*[118] case has uncovered yet another weakness with the notice and take-down system, which is whether when issuing a take-down notice, a copyright should take fair use into account. Fair use is a copyright doctrine enshrined in §107 of the Copyright Act which is meant to be an "exception to the copyright monopoly"[119]. It allows certain limited uses of copyrighted material without prior consent from the owner, such as remixing a song, quoting an author, reviewing a movie and using certain frames. Before the *Lenz* case, the fair use doctrine was interpreted by the Supreme Court as an affirmative defense, although scholars disputed that it should not be so[120].

In *Lenz v Universal*, Stephanie Lenz posted a short video on YouTube of her small child dancing to Prince's song "Let's go crazy" which could be heard in the background. Following a take-down notice from Universal, the video was taken down by YouTube, only to be re-uploaded later pursuant to Lenz's counter-notice[121]. Miss Lenz then filed a suit against Universal on the grounds of §512(f) DMCA, arguing that the take-down notice was in bad faith as it did not take fair use into account.

[116] DMCA §512(g)(3)(D)
[117] See Charles W Jr Hazelwood, 'Fair Use and the Takedown / Put Back Provisions of the Digital Millennium Copyright Act' (2009) 50 IDEA: The Intellectual Property Law Review 307; Randazza (n 110).
[118] Lenz v. Universal Music Corp., 573 F. Supp. 2d 1150 (N.D. Cal., 2008)
[119] Randazza (n 110) 107.
[120] See Tara M Warrington, 'Harry Potter and the Doctrine of Fair Use: Conjuring a New Copyright Complaint' (2008) 10 Florida Coastal Law Review 621.
[121] Lenz v. Universal Music Corp., 573 F. Supp. 2d 1150 (N.D. Cal., 2008) at 1152

The Ninth Circuit in *Lenz* innovated in establishing first, that fair use is not only an affirmative defense but a right in itself[122], and an action that falls under its doctrine will be interpreted as non-infringing use[123]. As a direct consequence, a copyright owner will have the obligation to "consider" fair use before sending a take-down notice[124]. Although at first glance this seems to be a win for users who want to benefit from the fair use doctrine and for the ISPs that get bombarded with a high number of requests[125], on a further analysis the present decision does not seem to change the status quo that much[126].

However, the Ninth Circuit set a very low bar in what "considering" fair use means. Thus, it held that it made no difference how wrong the copyright owner's consideration might be. In its 2016 amended opinion[127] the Ninth Circuit underlined that the owner does not have to look at the existence of fair use as a court should, but only to form a "good faith belief that it was not" present[128]. Thus, as long as there is evidence that a copyright owner did perform *prima facie* examination of the content and its compliance with the fair use doctrine, it will not be liable for misrepresentation under §512(f). The Court held that such consideration of the fair use of the copyrighted material might even be done by automatic means, through copyright detection software[129].

In conclusion, although Lenz won, she was only awarded nominal damages for the damage suffered, which was qualified as "unquantifiable"[130]. But, as Professor Randzza noticed, her case

[122] Lenz v. Universal Music Corp., 801 F.3d 1126, 1133 (9th Cir. 2015) at 1133
[123] Randazza (n 110) 128.
[124] Lenz v. Universal Music Corp., 801 F.3d 1126, 1133 (9th Cir. 2015) at 1134
[125] M Jake Feaver, 'Correcting Computer Vision: The Case for Real Eyes After Lenz' (2017) 68 Hastings LJ 397, 410.
[126] Randazza (n 110) 129.
[127] Lenz v. Universal Music Corp., Nos. 13-16106, 13-16107 U.S. (9th Cir. Mar. 17, 2016)
[128] Id. At *16
[129] Lenz v. Universal Music Corp., 801 F.3d 1126, 1133 (9th Cir. 2015) at 1135
[130] Lenz v. Universal Music Corp., Nos. 13-16106, 13-16107 U.S. (9th Cir. Mar. 17, 2016) at *9

only got that far because it was backed by large media companies, trying to defend the doctrine of fair use[131].

[131] Randazza (n 110) 130.

Chapter III. Proposed changes

The regulations in the field of ISP liability analyzed in the previous chapters are almost as old as the Internet itself. They came in force around the beginning of the new millennium when the internet's infrastructure, reach, and speeds were significantly smaller than they are today. Thus, while both the E-Commerce Directive and the DMCA were designed for an environment where dial-up speeds were the norm, today speeds have exponentially grown[132] to be more than a thousand times bigger[133]. Bearing this in mind, and the fact that now half of the total world population[134] has access to the Internet, it is easy to see why regulators have a hard time keeping up.

Moreover, at the time when the two statues were construed, their purpose was to strike a proper balance between protecting content owners against infringement and enabling the continuous innovation of ISPs who shape the Internet. Although arguably, the two systems were quite successful in obtaining at least a certain degree of balance, the circumstances have changed[135].

Because of these changes, reforms in the field of ISP liability are an ongoing concern of both systems, as examined above. In the present chapter I will use the lessons learned from the analysis on the regulatory trends of ISP liability to establish a proposed system of my own that

[132] See Annemarie Bridy, 'Is Online Copyright Enforcement Scalable' (2010) 13 Vanderbilt Journal of Entertainment and Technology Law 695.
[133] Randazza (n 110) 110 footnote 52.
[134] International Communications Union, Worldwide Internet Users (2016) http://www.internetworldstats.com/stats.htm accessed 9 December 2016
[135] Donald P Harris, 'Time to Reboot?: DMCA 2.0' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2662475 5 <https://papers.ssrn.com/abstract=2662475> accessed 29 March 2017.

will properly balance all the relevant interests in today's digital world, adaptable to further changes, yet stable enough to provide certainty.

1. **A global regime**

As noted by scholars, copyright law has been generally weakened by the differences and idiosyncrasies in national intellectual property enforcement and secondary liability regimes[136]. In addition to that, the borderless nature of the internet has made this even more clear to see. To give a striking example, a user in Germany using a virtual private network (VPN)[137] that gives him/her an IP from the US can download a torrent file from a website operating in Russia which allows him/her to get all the parts of the file from other users scattered all over the world. The fact that most of those jurisdictions have different rules on these issues raises difficulties. To make things easier, an international treaty on ISP liability could prove to be the solution.

Of course, this is easier said than done. Establishing a harmonized global regime in this field is no easy task given how difficult it would be to come up with a treaty that most nations would agree with. International law has shown us time and time again that, usually states are not keen on signing treaties as that means compromising a degree of sovereignty to change their substantive law to be in accord with that of others[138]. Although hard, this is not impossible, and what better example for this than the rather successful Berne Convention[139] and TRIPs

[136] See Scott Burger, 'Eradication of a Secondary Infringer's Safe Havens: The Need for a Multilateral Treaty Addressing Secondary Liability in Copyright Law' (2009) 18 Michigan State International Law Review <http://digitalcommons.law.msu.edu/ilr/vol18/iss1/10>.

[137] 'VPN service provide users with the means of avoiding having their IP addresses connected to their offline identity' through an encrypted connection on a server, after which an user is granted a different, basically anonymous IP. For more, see Ian Phau and others, 'Law, Norms, Piracy and Online Anonymity: Practices of de-Identification in the Global File Sharing Community' (2012) 6 Journal of Research in Interactive Marketing 260.

[138] Burger (n 136) 155.

[139] The Berne Convention for the Protection of Literary and Artistic Works (usually known as the Berne Convention) (Sept. 9, 1886)

Agreement[140]. However, while both delivered several significant positive contributions to international copyright law they are silent on anything relating to secondary liability[141].

2. A need for clear provisions

Both the DMCA and the E-Commerce directive are vague in certain places, from their definitions of ISPs to the indeterminate concepts such as *online services* or actual knowledge. However, interestingly enough, it is precisely this vagueness that has allowed the courts to construe the concepts widely. Although it is difficult to establish the intention of the drafters, some authors argue that at that point in time, the hosting (or storage) safe harbor was merely meant to encompass the "technical activity of providing server space"[142]. With the advent of the Web 2.0, the courts saw an opportunity to give a far-reaching interpretation to this concept as also covering storage of content created and submitted by website users.

However, there is an ongoing need for clear provisions as these provide a greater level of business certainty. As Professor Lee Aptly put it, "[u]ncertainty defeats the whole purpose of a safe harbor because companies are unable to identify the necessary steps to avoid liability"[143] Ambiguous regulations in the copyright area, particularly regarding the likelihood and costs of lawsuits, have a drastic effect on early-stage development of companies, and, thus, on the economy as a whole[144]. In a 2011 study, it was found that 80% of interviewed angel investors and venture

[140] TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, (hereinafter TRIPS Agreement)
[141] Burger (n 136) 148.
[142] Peguera (n 60) 496 footnote 87.
[143] Lee (n 85) 34.
[144] Computer & Communications Industry Associations (CCIA), Copyright Reform for a Digital Economy, available at http://cdn.ccianet.org/wp-content/uploads/2015/08/Copyright-Reform-for-a-Digital-Economy.pdf accessed 29 March 2017

capitalists feel "uncomfortable investing in business models in which the regulatory framework is ambiguous"[145].

Thus, in the present, there is no need as there was at the time of the internet's inception for broad terminology, subject to interpretation. Drafters should not fear to use clear language, in an effort to achieve a greater level of business certainty. As discussed above, proposed regulations such as the SOPA ad PIPA were met with much criticism and even protest, partly because they contained provisions so broad that they could create liability for, virtually, "the entire Internet itself"[146].

3. A fair notice and take-down system

Although eroded partly by the courts, the notice and take-down system in the US has played a key role in properly balancing the interests at stake. It provides ISPs with a degree of certainty of when they need to act on infringing material, while giving copyright owners a sword to fight against such unlawful activities. Although neither the E-Commerce Directive nor the Proposed Directive on the Digital Single Market do not expressly provide for such a system I submit that they would both gain from having it, if implemented properly.

However, learning from the mistakes that the DMCA did, the notice and take-down system in an ideal regulation could deal with some issues in a better way. First, it should do a better job to discourage copyright bullying i.e. copyright owners with a tendency to abuse the notice and take-down regime and send inaccurate notices. Although §512 DMCA does provide for some

[145] Briefing Matthew Le Merle and others, *The Impact of US Internet Copyright Regulations on Early-Stage Investment A Quantitative Study*, p 16 <http://www.fifthera.com/s/Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf> accessed 29 March 2017.

[146] Carrier (n 89) para 3 citing Mike Masnick, The Definitive Post on Why SOPA and Protect IP Are Bad, Bad Ideas, TECHDIRT, http://www.techdirt.com/articles/20111122/04254316872/definitive-post-why-sopaprotect-ip-are-bad-bad-ideas.shtml, accessed 29 March 2017.

measures that apparently protect users and ISPs from inappropriate take-down notices, they are not as effective as intended[147], as discussed above. To better balance all interests, my proposal for a better take-down regime is to impose a more stringent requirement on owners to consider fair use[148]. However, this consideration should be in accordance to an objective test, and failure to comply with such a requirement should imply some pecuniary penalty. It should be high enough to discourage owners from frivolous notices but low enough not to make identifying content infringement unnecessarily costly.

Moreover, there is a need to discourage the *shoot and ask questions later* approach that copyright owners seem to have in the US, where balance is tilted in favor of rapid content removal, without much opposition from "users who make legitimate uses of content"[149].

Plus, as seen above, even if pursuant to a counter-notice the content is found to be non-infringing and is re-uploaded, the harm might be already done. To prevent this and to make the counter-notification system as an even more efficient tool, another change should be made to the American model. Perhaps it would defeat the purpose of the safe harbor to allow ISPs to immediately allow access back to taken down content, and that is why a common ground is needed. I would suggest allowing this permission only for certain type of time sensitive content[150] or putting a fee system for immediate take-down. The fees could go either to the ISP, who must use the money from such fees to invest in better detection systems or they could go to separate, governmental or non-governmental bodies[151] created specifically to deal with issues in this field.

[147] Arthur H Neill and Erika Lee, 'Fixing Section 512 - Legislative Reforms for the DMCA Safe Harbor Provisions' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2879696 2 <https://papers.ssrn.com/abstract=2879696> accessed 26 March 2017.
[148] See Lenz v Universal, discussed above
[149] Neill and Lee (n 147) 5.
[150] As in the case of political commercials, discussed above
[151] Isa Cankar, 'The Search for an Ideal Model of Notice - Takedown System' (Social Science Research Network 2013) SSRN Scholarly Paper ID 2366763 55 <https://papers.ssrn.com/abstract=2366763> accessed 30 March 2017.

Finally, an online registration system for ISP agents that deal with the notices is a good idea. However, it should be implemented in such a way that failure to comply with it, especially by error or ignorance, will not have the quite drastic effect of completely sinking the safe harbor.

4. Monitoring systems

Both the US nor the EU prohibit the imposing of a general obligation on the ISPs to monitor activity. While in the E-Commerce Directive this is expressly stated in art. 15 and the case law also confirmed this[152], the US does not have such an interdiction codified. However, this was later confirmed in the very famous case of *Viacom v. YouTube*[153], where the Second Circuit held that the DMCA liability regime excludes courts from imposing a general obligation on IPS to monitor the content.

Thus, without having to actively look for infringements, ISPs are liable only after receiving a take-down notice or after obtaining actual knowledge of the infringement. The court shed some light on this language stating that the knowledge should be "of specific and identifiable infringements of particular individual items. Mere knowledge of prevalence of such activity in general is not enough"[154]. The same approach was taken in a number of other cases, such as *Perfect 10*[155] or *UMG Recordings v. Veoh*[156].

Therefore, although the facts of the case showed that YouTube had a general knowledge of widespread infringement on the content it hosted, it also had a history of expeditiously complying with take-down notices, and thus was not liable.

[152] See *Scarlet v. Sabam*, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM Case C-70/10, 2011 E.C.R. I-11962
[153] Viacom Int'l, Inc. v. YouTube, Inc. 676 F.3d 19, 35 (2d Cir. 2012)
[154] Id., at 41
[155] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).
[156] UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1108–09 (C.D. Cal. 2009).

That being said, the Proposed Directive for a Digital Single Market seems to embrace the position that ISPs should take appropriate and proportionate measures to protect copyrighted works by implementing effective filtering technologies[157]. On the same note, in the US, many ISPs, usually large companies have already adopted automated monitoring and filtering measures even in lieu of any legal obligations to do so[158]. This was the result of the constant pressure from copyright owners in the form of an overwhelming amount of takedown[159].

Therefore, there seems to be a trend towards embracing some forms of monitoring, even if this is done automatically, by computer algorithms. This is far from surprising when considering the staggering amount of content uploaded constantly on the web. For example, on the media sharing giant, YouTube, more than 300 hours of video are being uploaded every minute[160]. It is only reasonable that to better cope with the extraordinary amount on information, some automated means are necessary. However, such a system is not perfect.

First, an automated pre-emptive filtering system will fail to be perfect. More precisely, presently they have troubles distinguishing infringing content from content that falls under the fair use doctrine[161]. This is understandably so when even courts have difficulties on establishing cases of fair use. Of course, having a program learn how to properly detect fair use is not impossible, especially with the current evolution of artificial intelligence and machine learning, however, such subtleties "will remain beyond the grasp of robotic filters for the foreseeable future"[162]. Although

[157] Supra, 13
[158] Harris (n 135) 25.
[159] Sag (n 114) 40.
[160] Tena B Crews and Karen Bean May, *Digital Media: Concepts and Applications* (Cengage Learning 2016) 380 (Citing YouTube Statistics 2015).
[161] Sag (n 114) 55.
[162] ibid.

technology might evolve to the point where it more accurately recognizes infringing content, this works both ways, as the technology to circumvent it will evolve alongside it[163].

Second, precisely because the inherent less than perfect nature of such an automated filtering system, its effects on content should not be automatic. An ideal content filtering system will examine the degree of possibility that the content is infringing and take several actions depending on them. Thus, a computerized system should take the measure of automatically restricting or blocking access to content only in the rarest of cases. In the rest of the cases, users should be given a chance to show whether their content is infringing or not before any other action is taken against it. This also seems to be the approach taken by YouTube's Content ID, although critics seem to have noticed that it is not entirely effective in protecting users, only those with relatively small channels[164].

Finally, if such measures are found to be much needed to further balance out all the updated interests at stake, its costs should be addressed. As discussed earlier[165], imposing monitoring and filtering measures, especially through automated means, translates to huge costs to companies. Of course, the big tech companies can probably afford such investments, however, for start-ups it would present an impassable barrier.

There are two solutions to this problem. A regulation imposing monitoring and filtering measures could make the differentiation between big and small ISPs. Thus, smaller corporate entities can be exempted from this measure if they satisfy certain criteria. For example, if the quantity of content hosted by an ISP does not cross a threshold, then a notice and take-down system

[163] Sonia Katyal and Jason Schultz, 'The Unending Search for the Optimal Infringement Filter' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2843708 106 <https://papers.ssrn.com/abstract=2843708> accessed 5 April 2017.
[164] Sag (n 114) 56.
[165] Supra, 12

might prove efficient enough to deal with infringements. Second, an independent institutional body could be created that is entrusted with developing such a system and to evaluate disputes arising out of its usage[166]. Such a body could be funded by ISPs that pay, for example, licensing fees for using the systems or other such sources. Moreover, a body like the Copyright Office already has "has all of the necessary information about registered works"[167] so in theory, building a database of content against which scanned content is analyzed to check for infringement is made easy.

[166] Katyal and Schultz (n 163) 95.
[167] ibid.

Conclusion

Today, the internet has made access to information easier than most people could have imagine, except for, perhaps, science fiction authors. Peter Singer, a famous moral philosopher stated that "[t]he internet, like the steam engine, is a technological breakthrough that changed the world"[168]. This thesis examined in how the internet changed copyright law when it comes to ISPs and, in particular, how the law adapted to that change.

Shortly after the internet started becoming available to the general population, it became obvious that it would facilitate copyright infringements by a large margin. Even more obvious was the fact that although an easy solution to this was to hold the ISPs liable, it should be done so within certain limits. Thus, the safe harbor was built, construing a set of conditions needed for the ISP to shelter itself from liability. There is almost a consensus that these safe harbors have empowered the remarkable advance of online communities, e-commerce, and entirely new types of communication, cultural participation and expression[169]. However, precisely because ISP liability regimes are almost as old as the internet itself, they are in need of re-evaluation.

The European Union E-Commerce Directive and the United States' DMCA section 512 are both perfect examples of regimes that prescribe the mechanisms of ISP liability. Although they are similar, as the Directive used the DMCA as a model, several differences remain between the two. As shown, both systems have similar provisions pertaining to safe harbors for mere conduit and caching ISPs, however the E-Commerce Directive has no explicit safe harbor provisions for information location tools such as search engines. More differences start to show up in dealing

[168] Peter Singer, 'The Unknown Promise of Internet Freedom' *The Guardian* (4 April 2010) <https://www.theguardian.com/commentisfree/2010/apr/04/internet-china-google-censorship> accessed 5 April 2017.
[169] Sag (n 114) 61.

with hosting providers, especially in dealing with the actual knowledge concept and where the DMCA explicitly puts in place a notice and take-down system.

The need to revisit both systems and adapt them to better balance all the interests at stake has become clearer in recent years. The US Congress had several failed attempts to increase the overall liability of providers. Because of the imperfect, vague way of doing so, bills such as SOPA and PIPA have been met with strong criticism and protest, and have been subsequently dropped by Congress.

On the other side of the ocean, EU's attempt on updating the ISP liability regime is the Proposed Directive on the Digital Single Market. The proposed directive in question was met with criticism as well, because it contradicts the non-monitoring provision of the E-Commerce Directive. In fact, if it entered force, Member States would have to impose a broad monitoring obligation on providers by means of effective filtering technologies. Thus, two things became clear: there is a need for updating the regimes, and so far, there are not any successful ones.

Using the comparative analysis between the two systems and the trends in how to further regulate ISP liability, several conclusions might be drawn that help in creating an ideal regime for balancing the interests of providers, users, and creators.

First, because of the borderless nature of the internet, a global regime would be ideal. Although it seems unlikely that enough states will agree on one treaty, it is not impossible. Second, such a regime should be clear enough as to not create uncertainty, especially in such a business-driven environment. Despite vagueness having worked for the current regimes, helping them to adapt to the changing online environment, the need for certainty now surpasses the need for adaptation. Third, an effective ISP liability system needs an updated notice and take-down system that protects both the users and ISPs from abusive notices and makes it less burdensome for

copyright holders to take down infringing content. Finally, if filtering technologies are considered necessary, they should be introduced with care and in a clear manner, perhaps considering the cost distribution for such measures.

Whichever path legislators take in updating the regulations on ISP liability, one thing is sure. They should weigh all the interests at stake carefully and objectively. Failure to do so might have dire effects on free speech, economic activity, consumers, protection of rights and many others.

Bibliography

- Angelopoulos, Christina, Beyond the Safe Harbours: Harmonising Substantive Intermediary Liability for Copyright Infringement in Europe (November 28, 2013). Intellectual Property Quarterly, 2013-3, p. 253-274.; Amsterdam Law School Research Paper No. 2013-72; Institute for Information Law Research Paper No. 2013-11. Available at SSRN: https://ssrn.com/abstract=2360997

- Baistrocchi PA, 'Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce [Article]' [2002] Santa Clara Computer and High Technology Law Journal 111

- Band J, 'The SOPA-TPP Nexus' [2012] PIJIP Research Paper Series <http://digitalcommons.wcl.american.edu/research/28>

- Böhme R and Köpsell S, 'Trained to Accept?: A Field Experiment on Consent Dialogs', proceedings of the SIGCHI Conference on Human Factors in Computing Systems (ACM 2010) <http://doi.acm.org/10.1145/1753326.1753689> accessed 9 December 2016

- Bretan J, 'Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA' (2003) 18 Berkeley Technology Law Journal 43

- Bridy A, 'Is Online Copyright Enforcement Scalable' (2010) 13 Vanderbilt Journal of Entertainment and Technology Law 695

- Bridy A and Keller D, 'U.S. Copyright Office Section 512 Study: Comments in Response to Second Notice of Inquiry' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2920871 <https://papers.ssrn.com/abstract=2920871> accessed 27 March 2017

- Burger S, 'Eradication of a Secondary Infringer's Safe Havens: The Need for a Multilateral Treaty Addressing Secondary Liability in Copyright Law' (2009) 18 Michigan State International Law Review <http://digitalcommons.law.msu.edu/ilr/vol18/iss1/10>

- Cankar I, 'The Search for an Ideal Model of Notice - Takedown System' (Social Science Research Network 2013) SSRN Scholarly Paper ID 2366763 <https://papers.ssrn.com/abstract=2366763> accessed 30 March 2017

- Carrier MA, 'SOPA, PIPA, ACTA, TPP: An Alphabet Soup of Innovation-Stifling Copyright Legislation and Agreements' (Social Science Research Network 2013) SSRN Scholarly Paper ID 2213034 <https://papers.ssrn.com/abstract=2213034> accessed 26 March 2017

- Crews TB and May KB, *Digital Media: Concepts and Applications* (Cengage Learning 2016)

- Feaver MJ, 'Correcting Computer Vision: The Case for Real Eyes After Lenz' (2017) 68 Hastings LJ 397

- Fonseca ZG and Lorenzo G, 'Intermediaries Liability for Online Copyright Infringements: The Duty to Cooperate Under E.U. Law' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2714269 <https://papers.ssrn.com/abstract=2714269> accessed 14 February 2017

- Frosio GF, 'Reforming Intermediary Liability in the Platform Economy: A European Digital Single Market Strategy' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2912272 <https://papers.ssrn.com/abstract=2912272> accessed 5 April 2017

- Goldman E, 'How the DMCA's Online Copyright Safe Harbor Failed' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2589751 <https://papers.ssrn.com/abstract=2589751> accessed 25 March 2017

- Harris DP, 'Time to Reboot?: DMCA 2.0' (Social Science Research Network 2015) SSRN Scholarly Paper ID 2662475 <https://papers.ssrn.com/abstract=2662475> accessed 29 March 2017

- Hazelwood CWJ, 'Fair Use and the Takedown / Put Back Provisions of the Digital Millennium Copyright Act' (2009) 50 IDEA: The Intellectual Property Law Review 307

- Hua JJ, *Toward A More Balanced Approach: Rethinking and Readjusting Copyright Systems in the Digital Network Era. [Electronic Resource]* (Berlin, Heidelberg : Springer Berlin Heidelberg : Imprint: Springer, 2014 2014)

- Husovec M, 'Accountable, Not Liable: Injunctions Against Intermediaries' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2773768 <https://papers.ssrn.com/abstract=2773768> accessed 27 March 2017

- Julià-Barceló R and Koelman KJ, 'INTERMEDIARY LIABILITY: INTERMEDIARY LIABILITY IN THE E-COMMERCE DIRECTIVE: SO FAR SO GOOD, BUT IT'S NOT ENOUGH' (2000) 16 Computer Law & Security Review 231

- Katyal S and Schultz J, 'The Unending Search for the Optimal Infringement Filter' (Social Science Research Network 2012) SSRN Scholarly Paper ID 2843708 <https://papers.ssrn.com/abstract=2843708> accessed 5 April 2017

- Le Merle BM and others, *The Impact of US Internet Copyright Regulations on Early-Stage Investment A Quantitative Study* <http://www.fifthera.com/s/Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf> accessed 29 March 2017

- Lee E, 'Decoding the DMCA Safe Harbors' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1333709 <https://papers.ssrn.com/abstract=1333709> accessed 26 March 2017

- Lee N, *Facebook Nation: Total Information Awareness* (Springer Science & Business Media 2012)

- Lemley MA, 'Rationalizing Internet Safe Harbors' (Social Science Research Network 2007) SSRN Scholarly Paper ID 979836 <https://papers.ssrn.com/abstract=979836> accessed 25 March 2017

- Malovic N, 'Online Copyright Enforcement in Sweden: The First Blocking Injunction' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2940786 <https://papers.ssrn.com/abstract=2940786> accessed 5 April 2017

- Miller SA, 'Peer-to-Peer File Distribution: An Analysis of Design, Liability, Litigation, and Potential Solutions Note' (2006) 25 Review of Litigation 181

- Myers G, *Principles of Intellectual Property Law* (West Academic 2017)

- Neill AH and Lee E, 'Fixing Section 512 - Legislative Reforms for the DMCA Safe Harbor Provisions' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2879696 <https://papers.ssrn.com/abstract=2879696> accessed 26 March 2017

- Neuburger JD, 'Copyright Office Establishes New Electronic DMCA Agent Registration' (2017) 29 Intellectual Property & Technology Law Journal 18

- Peguera M, 'The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems' (Social Science Research Network 2009) SSRN Scholarly Paper ID 1468433 <https://papers.ssrn.com/abstract=1468433> accessed 24 March 2017

- Peguera M, 'Secondary Liability for Copyright Infringement in the Web 2.0 Environment: Some Reflections on Viacom v. Youtube' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1716773 <https://papers.ssrn.com/abstract=1716773> accessed 24 March 2017

- Phau I and others, 'Law, Norms, Piracy and Online Anonymity: Practices of de-Identification in the Global File Sharing Community' (2012) 6 Journal of Research in Interactive Marketing 260

- Pranesh Prakash, Don't Shoot the Messenger: Speech on Intermediary Liability at 22nd

- Randazza MJ, 'Lenz v. Universal: A Call to Reform Section 512(f) of the DMCA and to Strengthen Fair Use' (Social Science Research Network 2016) SSRN Scholarly Paper ID 2773137 <https://papers.ssrn.com/abstract=2773137> accessed 27 March 2017

- Reed C and Angel J, *Computer Law : The Law and Regulation of Information Technology* (Oxford : Oxford University Press, 2007)

- Rosati E, 'SUPER KAT-EXCLUSIVE: Here's Draft Directive on Copyright in the Digital Single Market' <http://ipkitten.blogspot.com/2016/08/super-kat-exclusive-heres-draft.html> accessed 16 February 2017

- Rustad M, *Global Internet Law* (St Paul, MN : West Academic Publishing, [2016] 2016)

- Sag M, 'Internet Safe Harbors and the Transformation of Copyright Law' (Social Science Research Network 2017) SSRN Scholarly Paper ID 2830184 <https://papers.ssrn.com/abstract=2830184> accessed 28 March 2017

- Sartor G, Cunha V de A and Mario, 'The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents' (Social Science Research Network 2010) SSRN Scholarly Paper ID 1604411 <https://papers.ssrn.com/abstract=1604411> accessed 13 February 2017

- Schaffner DJ, 'The Digital Millennium Copyright Act: Overextension of Copyright Protection and the Unintended Chilling Effects on Fair Use, Free Speech, and Innovation Notes' (2004) 14 Cornell Journal of Law and Public Policy 145

- Schlachter E, 'The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet Symposium: Digital Content: New Products and New Business Models' (1997) 12 Berkeley Technology Law Journal 15

- Schruers M, 'The History and Economics of ISP Liability for Third Party Content' (2002) 88 Virginia Law Review 205

- Seltzer W, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (Social Science Research Network 2010) SSRN

Scholarly Paper ID 1577785 <https://papers.ssrn.com/abstract=1577785> accessed 27 March 2017

- Seng D, 'The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices' (Social Science Research Network 2014) SSRN Scholarly Paper ID 2411915 <https://papers.ssrn.com/abstract=2411915> accessed 28 March 2017

- Singer P, 'The Unknown Promise of Internet Freedom' *The Guardian* (4 April 2010) <https://www.theguardian.com/commentisfree/2010/apr/04/internet-china-google-censorship> accessed 5 April 2017

- Stalla-Bourdillon S and others, 'An Academic Perspective on the Copyright Reform' (2017) 33 Computer Law & Security Review 3

- Sutter G, '"Don"t Shoot the Messenger?'The UK and Online Intermediary Liability' (2003) 17 International Review of Law, Computers & Technology 73

- Svensøy GJ, 'The E-Commerce Directive Article 14: Liability Exemptions for Hosting Third Party Content' <https://www.mysciencework.com/publication/show/5f0f35a3b076a605c9d2e69762f6c753> accessed 13 February 2017

- Urban J and Quilter L, 'Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (2006) 22 Santa Clara High Technology Law Journal 621

- Van Eecke P and Ooms B, 'Isp Liability and the E-Commerce Directive: A Growing Trend Toward Greater Responsibility for Isps' (2011) 15 Journal of Internet Law 3

- Verbiest T, Spindler G and Riccio GM, 'Study on the Liability of Internet Intermediaries' (Social Science Research Network 2007) SSRN Scholarly Paper ID 2575069 <https://papers.ssrn.com/abstract=2575069> accessed 14 February 2017

- Waelde C and Edwards L, 'Online Intermediaries and Copyright Liability' (Social Science Research Network 2005) SSRN Scholarly Paper ID 1159640 <https://papers.ssrn.com/abstract=1159640> accessed 11 December 2016

- Warrington TM, 'Harry Potter and the Doctrine of Fair Use: Conjuring a New Copyright Complaint' (2008) 10 Florida Coastal Law Review 621

- SCCR of WIPO, July 08, 2011. L. Edwards, The Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights.

Legislation

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031 accessed 9 December 2016
- Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market (Text with EEA relevance), Brussels, 14.9.2016 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0593> accessed 16 February 2017.
- The Berne Convention for the Protection of Literary and Artistic Works (usually known as the Berne Convention) (Sept. 9, 1886)
- The Digital Millennium Copyright Act of 1998 (DMCA) <https://www.copyright.gov/legislation/dmca.pdf> accessed 9 December2016
- The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PIPA), S. 968/2011; http://www.gpo.gov/fdsys/pkg/BILLS-112s968rs/pdf/BILLS-112s968rs.pdf
- The Stop Online Piracy Act Bill, H. R. 3261/2011, https://www.gpo.gov/fdsys/pkg/BILLS-112hr3261ih/pdf/BILLS-112hr3261ih.pdf

- The Trans Pacific Partnership Agreement (TPP) Intellectual Property Rights Chapter, available at http://keepthewebopen.com/tpp
- TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994

Cases

- Advocate General's Opinion in Case C-484/14 Tobias Mc Fadden v Sony Music Entertainment Germany GmbH para. 86 http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-03/cp160028en.pdf, accessed 1 April 2017.
- Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV, C-360/10 (ECJ, February 16.
- Benusan Restaurant Copr. V. King, 126 F.3d 25 (sd Cir. 1997)
- Google France v. Louis Vuitton C-236/08.
- Lenz v. Universal Music Corp., 573 F. Supp. 2d 1150 (N.D. Cal., 2008).
- Lenz v. Universal Music Corp., 801 F.3d 1126, 1133 (9th Cir. 2015) .
- Lenz v. Universal Music Corp., Nos. 13-16106, 13-16107 U.S. (9th Cir. Mar. 17, 2016).
- Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).
- Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10 (ECJ, November 24, 2011).
- Tobias Mc Fadden v. Sony Music Entertainment Germany GmbH, C-484/14, CJEU, Third Chamber.
- UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1108–09 (C.D. Cal. 2009).
- Viacom Int'l, Inc. v. YouTube, Inc. 676 F.3d 19, 35 (2d Cir. 2012).

Online resources

- Commission Staff Working Document Impact Assessment on the modernisation of EU copyright rules, Accompanying the proposed directive, Brussels, 14.9.2016 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0301> accessed 16 February 2017
- Computer & Communications Industry Associations (CCIA), Copyright Reform for a Digital Economy, available at http://cdn.ccianet.org/wp-content/uploads/2015/08/Copyright-Reform-for-a-Digital-Economy.pdf
- Copyright Office, Frequently Asked Questions, Designation of Agents to Receive Notifications of Claimed Infringement https://www.copyright.gov/rulemaking/onlinesp/NPR/faq.html
- Court of Justice of the European Union PRESS RELEASE No 99/16 Luxembourg, 15 September 2016 http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-09/cp160099en.pdf Accessed 10 December 2016
- Digital Single Market website https://ec.europa.eu/commission/priorities/digital-single-market_en
- First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Brussels, 21.11.2003 COM(2003) 702 final; http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0702:FIN:EN:PDF
- Gerald Spindler, Study on Liability of Internet Intermediaries – Hungary – Executive Summary 12/11/2007; http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/hungary_12nov2007_en.pdf accessed 25 March 2017.
- How Google Fights Piracy Report, 2016 https://drive.google.com/file/d/0BwxyRPFduTN2TmpGajJ6TnRLaDA/view, accessed 25 March 2017
- International Communications Union, *Worldwide Internet Users* (2016) http://www.internetworldstats.com/stats.htm accessed 9 December 2016 accessed 9 December 2016

- The Numbers on #SOPASTRIKE' <http://sopastrike.com/numbers> accessed 27 March 2017
- Trevor Potter's letter to Chad Hurley, YouTube's CEO, dated October 13 2008, available at https://www.eff.org/files/mccain_youtube_copyright_letter_10.13.08.pdf accessed 27 March 28, 2017.