2020

Copyright Infringement Liability of Online Content Sharing Platforms in the US and in the EU after the Digital Single Market Directive: A Case Study

Teresa García-Barrero
Columbia Law School

Copyright Infringement Liability of Online Content Sharing Platforms in the US and in the EU after the Digital Single Market Directive: a Case Study

Teresa García-Barrero

Abstract

The EU copyright liability regime for internet service providers has significantly changed after the enactment of article 17 of the Digital Single Market Directive. Where two fairly similar systems once existed in the US and in the EU, there are now significant differences between the regimes with which service providers must comply in each region. This paper seeks to offer a practical view of the differences between both systems through a comparative analysis of the result that the application of each legal framework would have on an identical factual case. Specifically, this paper contrasts the decision reached by US courts in Capitol Records v. Vimeo with the hypothetical result that a EU court would deliver to those same facts in application of the Digital Single Market Directive.

Introduction

During the past two decades user content sharing platforms have navigated a fairly comfortable environment both in the US and in the EU, where they have been able to benefit from the exploitation of works subject to copyright without obtaining an authorization from their underlying rightholders. The relative similarity between so called "safe harbor" regulations on both sides of the Atlantic had also simplified matters for these platforms when designing business models and internal policies compatible with their activities in both markets.

However, the Digital Single Market Directive[1] (the "Directive" or the "DSMD"), which entered into force on June 7, 2019, has notably changed the obligations with which these service providers must comply when rendering services in the EU, and has thus created further obstacles for them to dock in European safe harbors. In particular, article 17 of the Directive

[1] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92–125).

sets out a new liability regime that has been closely followed by all stakeholders involved (notably, copyright holders, online service providers, and user associations).

Most internet companies run on a global scale, and it is therefore important for them to understand the legal framework of each territory in which they operate in order to design and implement an adequate copyright compliance mechanism. Even though the current "Tech Giants"[2] are based in the US, a significant part of their revenue derives from their activities in Europe.[3] Not complying with EU regulations could subject them to important monetary and injunctive remedies. Thus, these companies must become familiar with the differences between the US system under which they were established and the EU regulations to which they must adapt, in order to implement adequate measures compatible with their rendering of global services.

Given the highly controversial legal implications that article 17 involves, as well as the important economic interests underlying its practical application, the provision has been the object of several theoretical analyses by academics and market players. This paper aims to complement these analyses by offering a practical view of article 17 of the DSMD in relation to the US liability regime for online service providers. In particular, this paper contrasts how a same online content sharing service could find itself exempt from liability in the US but subject to remedies in the EU, in light of the different regulations which the courts in each territory apply.

Part I of this paper will lay out a brief legal background of the online service provider liability regimes enacted in each of the two legal systems studied. Part II will outline the facts found in *Capitol Records, LLC v. Vimeo, LLC*[4] and use them as a backdrop through which to contrast the different analyses that courts in the US and in the EU would carry out to decide upon the liability of a content sharing service provider. Part III will point out certain decisions that service providers must make in light of the two legal systems, and Part IV will summarize the main conclusions that can be drawn from the assessment carried out.

[2] The term "Tech Giants" is often used in journalism to refer to the largest companies in the information technology industry such as Alphabet, Amazon, Apple, Facebook, or Youtube. *See*, *e.g.*, NEW YORK TIMES, *We're Stuck With the Tech Giants. But They're Stuck With Each Other* (Nov. 13, 2019) https://www.nytimes.com/interactive/2019/11/13/magazine/internet-platform.html.
[3] For example, 31 per cent of Alphabet's revenue from 2019 was generated in the EMEA region. *See* STATISTA, https://www.statista.com/statistics/266250/regional-distribution-of-googles-revenue/ (last visited April 25, 2020).
[4] *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, (2d Cir. 2016) (hereafter "*Vimeo*").

I. Legal Background

It is a notorious fact that technology advances at an exponential rhythm which promotes the rapid appearance of new business models, means of exploitation, and market players. Thus, legal systems often find themselves a few steps behind when it comes to adapting to an everchanging environment in which the most suitable legal measures are difficult to anticipate. A particularly problematic issue for legislators during the last decades has been adapting to new forms of online exploitation of copyright, and properly allocating the liability for the infringement that takes place over the internet.

In this context, the 1996 WIPO Copyright Treaty (WCT) recognized "the need to maintain a balance between the rights of authors and the larger public interest, particularly education, research and access to information (…)"[5]. Both the US and the EU member states are contracting parties to the WCT, and their legislation reflects an underlying policy to maintain this balance between the protection of copyright and the fostering of internet development.

A. Online Storage Safe Harbor in the United States

The US Congress' implementation of the WCT was the Online Copyright Infringement Liability Limitation Act (OCILLA) passed as part of the 1998 Digital Millennium Copyright Act (DMCA)[6] and often referred to as the safe harbor provisions of 17 U.S.C. § 512.[7] The DMCA encourages the development of online intermediaries by stating that they will not be liable where content uploaded by their users violate rights of third parties.[8] The § 512 safe harbors protect online service providers from liability for copyright infringements carried out by users of their services. As long as specific requirements of the DMCA are satisfied, the online service providers have no liability for money damages, and limited exposure to injunctions.[9]

These exemptions apply to providers of several internet services, including 1) transitory digital network communications; 2) system caching; 3) information residing on systems or

[5] See WCT Preamble, recital 5.
[6] The DMCA was enacted to implement the WCT and to update U.S copyright law to the digital age. *See Viacom*, 676 F.3d at 26 (quoting earlier Universal City Studios, Inc. v. Corley, 273 F.3d 429, 440 (2d Cir. 2011) and Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004)).
[7] Title II of the DMCA, codified at 17 U.S.C. § 512, has the aim to "preserve (…) strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in a digital networked environment." S. Rep. 105–190, at 20 (1998).
[8] Anupam Chander, *Internet Intermediaries as Platforms for Expression and Innovation, Global Commission on Internet Governance*, 42, November 2016, 3.
[9] Mitchell Zimmerman, Your DMCA Safe Harbor Questions Answered, Fenwick & West, 2017, 5.

networks at the direction of users (the Storage Safe Harbor on which this paper focuses); and 4) local information tools that provide links or refer users to online locations containing infringing matter or activity (e.g. search engines).

B. Evolution of Liability under EU Law

Heavily inspired by US regulation,[10] and also seeking to strike "a balance between the different interests at stake",[11] the European response to the WCT was first enacted in the eCommerce Directive of 2000.[12] Section 4 of the text (articles 12 to 15) introduced safe harbor provisions for internet service providers as long as they complied with certain requirements. This meant that, like in the US, host service providers had no obligation to clear rights in copyrighted content posted by their users.

Thus, online service providers found themselves reaping considerable benefits from the content sharing carried out on their platforms without the need to obtain (i.e., pay for) the authorization of rightholders whose rights were being exploited on their platforms. The evolution of online business models and the increasing popularity and scale which these service providers reached gave rise to the problem known as the "value gap".[13] Content industries denounced that online sharing platforms made large amounts of copyrighted works available to the public and reaped important benefits from users who visited their sites in search of those works, while the holders of copyrights in those works saw no monetary compensation in exchange.[14] It soon became apparent that liability exemption provisions that had been designed taking into consideration the technology of the late 90s (the eCommerce Directive was passed in 2000 and the DMCA in 1998) had become obsolete. The innocent bystander approach which

[10] Miquel Peguera, *The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems*, 32 Colum. J.L. & Arts 481 (2008), 482.
[11] 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) (OJ L 178, 17.7.2000, p. 1), recital 41.
[12] 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") (OJ L 178, 17.07.2000 p. 0001 – 0016).
[13] The issue of the value gap has been addressed by several scholars, *e.g* Christina Angelopoulos and JoãO Pedro Quintais, *Fixing Copyright Reform: How to Address Online Infringement and Bridge the Value Gap* (2018) Web publication/site, Information Law and Policy Centre, available at https://infolawcentre.blogs.sas.ac.uk/2018/09/06/fixing-copyright-reform-how-to-address-online-infringement-and-bridge-the-value-gap/
[14] See Julian López Richart, *Un nuevo régimen de responsabilidad para las plataformas de almacenamiento de contenidos generados por usuarios en el mercado único digital*, Pe. i. revista de propiedad intelectual, nº 60 (2018) 85.

service providers had adopted was no longer credible in light of newly available technologies (such as, for example, Youtube's Content ID, referred to below).

The EU's attempt to solve this challenge, after a long parliamentary process and heavy debate, resulted in what is now article 17 of the DSMD which, along with the entire Directive, must be implemented by Member States by June 7, 2021.[15] Even though many internet service providers will continue to benefit from the eCommerce safe harbors (e.g. Google's search engine or Wikipedia), those which fall under the DSMD's definition of Online Content Sharing Service Providers ("OCSSPs") -e.g. Youtube, Vimeo, TikTok, or Instagram- have seen a shift in their legal framework, and they now face *ex ante* obligations and rights clearing burdens when rendering services in Europe.

As discussed below in greater detail, article 17 substantially broadens the concept of "communication to the public" referred to throughout Directive 2001/29[16] and further delimited by the Court of Justice of the European Union.[17] Additionally, it is a rule that *must* ("shall") be adopted by all Member States, i.e., it cannot be excluded as a matter of national policy. This means that where certain disparities existed across the different European national laws regarding the application of direct and secondary liability regimes to content sharing providers,[18] article 17 now makes it clear that these OCSSPs will be considered to be performing an act of communication to the public or an act of making works available to the public when giving access to protected works and subject matter.

The mentioned disparities among different national laws is explained by the fact that the older eCommerce Directive did not establish any rules regarding the liability of internet

[15] See DSMD, article 29.

[16] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10–19).

[17] The Court of Justice of the European Union (CJEU) has shaped the concept by decisions defining the concept of "public", within which the term "new public" was judicially created, and decisions clarifying the term "communication". Within the first set of decisions *see, e.g* CJEU 13 February 2014, C-466/12 (Nils Svensson, Sten Sjögren, Madelaine Sahlman and Pia Gadd v Retriever Sverige AB) and CJEU 21 October 2014, C-348/13 (BestWater International GmbH v Michael Mebes and Stefan Potsch). Within the second set of decisions *see, e.g.* CJEU 7 December 2007, C-306/05 (Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles S); CJEU 14 June 2017, C-610/15 (Stichting Brein v. Ziggo BV). For a more detailed analysis on the "new public" criterion *see* Hugenholtz, and van Velze, S.C*., Communication to a New Public? Three Reasons Why EU Copyright Law Can Do Without a 'New Public'*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2811777 (2016); and Association Littéraire et Artistique Internationale (ALAI), *Opinion of ALAI's Executive Committee on the Right of communication to the public*, available at (http://www.alai.org/en/assets/files/resolutions/2014-opinion-new-public.pdf).

[18] For a compared analysis see Christina Angelopoulos, *Beyond the safe Harbours: Harmonising substantive intermediary liability for copyright infringement in Europe*, Intellectual Property Quarterly, 2013-3, p. 253 and Matthias Leistner, *Structural aspects of secondary (provider) liability*, Journal of Intellectual Property Law & Practice, vol. 9, no. 1, 2014, 78.

service providers, but merely defined those cases in which a service provider could benefit from an exemption or limitation to such liability. Therefore, whenever the eCommerce Directive's safe harbor was found not to apply, it was a matter of national law to determine whether or not the service provider in question should be sanctioned in accordance with the relevant member state's rules for direct or secondary liability.[19] As in the previous European system, the DMCA does not include a special provision for determining when a service provider *is* considered to be liable for infringement, but rather merely states those cases in which it can benefit from the defense that it is *not* liable.

As a result of the determination that OCSSPs are legally considered to directly or primarily carry out acts of communication to the public or to make protected content available to the public, article 17.3 determines that they may not benefit from the safe harbor contained in article 14 of the eCommerce Directive. This safe harbor provision will remain available to limit copyright infringement liability to internet service providers when they carry out services other than those of online content sharing (article 17.3 II DSMD). In lieu of the non-applicable (for OCSSPs) safe harbor, article 17.4 of the DSMD creates a series of affirmative duties that may exempt OCSSPs from liability, exclusively in the sphere of copyright protected content that may be shared through their platforms.[20] These affirmative duties consist of blocking, takedown and "staydown", as further discussed below. Therefore, unless the OCSSP complies with a series of proactive measures, it will be considered directly liable for violating exclusive intellectual property rights. The OCSSP has to obtain the pertinent authorizations for its activity.

However, if a service provider does not qualify as an OCSSP (for example because it is not-for-profit or is an online marketplace),[21] those same acts of communication to the public will not render it a direct actor. It is worth noting that a same activity (storage and display) can be considered to be infringing or non-infringing, not because of the technology behind it or the means in which it is carried out, but as a result of the subjective characteristics of the service provider behind it.

---

[19] See Thomas Riis & Sebastian Felix Schwemer, *Leaving the European Safe Harbor, Sailing towards Algorithmic Content Regulation*, Journal of Internet Law, Vol. 22, No. 7, 2019, 8: "it is possible that the same intermediary providing the same service in all EU Member States is found to be contributory liable in one Member State but not in another".

[20] It is thus conceivable that for activities other than the sharing of protected works (e.g. the sharing of illegal content in light of terrorism or child pornography laws) OCCSPs could continue to avail themselves of the eCommerce Directive safe harbor provision.

[21] See DSMD, article 2(6) excluding certain agents form the OCSSP definition.

II. Safe Harbors: US Court Application in Vimeo Versus Theoretical EU Court Application

This section aims to use a same set of facts to analyze how the behavior and activity carried out by a particular online service provider can render it either subject to or exempt from liability, depending on whether it is reviewed under the legal regime set forth in the DMCA or under the liability provision regime of the DSMD.

Viacom v. Youtube[22] is oftentimes regarded as the landmark case regarding the application of the 17 U.S.C § 512(c) safe harbor. The Second Circuit had the opportunity to readdress some of the matters brought up in *Viacom* in its decision in *Capitol Records v. Vimeo*[23]. Since the latter case incorporates the court's precedent set out in *Viacom* and further explores the application of the rules held in the prior case, it offers a good opportunity to reflect on the difference between the two liability regimes object of analysis.

A. Background of *Capitol Records v. Vimeo*

Vimeo was a copyright infringement case decided in 2016 by the United States Court of Appeals for the Second Circuit, on interlocutory appeal on certified questions from rulings issued by the United States District Court for the Southern District of New York. As a result of the appeal, the Second Circuit was, once again, faced with the task of clarifying the strength of the 17 U.S.C. § 512(c) safe harbor.

Vimeo is an online video sharing platform founded in 2004 and headquartered in New York City, which provides free video viewing services worldwide.[24] As of 2012 (year in which the claim was analyzed by the District Court),[25] it hosted more than 31 million videos and had 12.3 million registered users in 49 countries. It currently (2020) has more than 150 million users.[26] Vimeo could be considered to be a competitor of platforms such as Youtube, which distinguishes itself from other video-sharing sites in that it requires users to have created, or at least have participated in the creation of, the videos they upload. However, the original nature of the created content is not always extended to the music contained in the uploaded videos, which is in great part subject to copyright protection. Even though users must accept the site's Terms and Services before uploading a video, and these terms require that the videos uploaded

[22] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 38 (2d Cir. 2012) (hereafter "*Viacom*").
[23] See fn 4 above.
[24] VIMEO, https://vimeo.com/about (last visited April 17, 2020).
[25] From March 3, 2011, until April 4, 2012, the case was stayed pending the Second Circuit's decision in Viacom.
[26] VIMEO, https://vimeo.com/about (last visited April 17, 2020).

be personally created by the user, they *do* have the technical ability to upload content that contains third party copyrighted works. According to the findings of the case, several videos containing third party copyrighted works were indeed uploaded. Consequently, the plaintiffs (several record and music publishing companies)[27] filed suit against Vimeo in December 2009, asserting claims for direct, contributory, vicarious, and common law copyright infringement, as well as for inducement to infringe copyright and unfair competition. The complaints contained a list of 199 videos in which plaintiffs owned copyrights to the musical recordings used without authorization.

The District Court granted partial summary judgment to the plaintiffs as to 11 videos containing pre-1972 recordings, ruling that these were protected by state, rather than federal, copyright laws and could therefore not benefit from federal safe harbor provisions. Secondly, it granted summary judgment to Vimeo as to post-1972 videos not viewed by Vimeo employees, ruling that Vimeo had no knowledge, actual or so-called "red flag" knowledge, as to those infringements. Finally, it denied summary judgment to both parties for a subset of videos which had been viewed by employees of Vimeo, concluding that there was a question of material fact whether the defendant possessed "red flag" knowledge of circumstances that made infringement apparent.

On appeal, the Second Circuit was asked to review three issues, the first two petitioned by Vimeo and the third petitioned by the plaintiffs: a) whether the DMCA's safe-harbor provisions were applicable to sound recordings fixed prior to February 15, 1972; b) whether, under the holding of *Viacom*, a service provider's viewing of a user-generated video containing all or virtually all of a recognizable, copyrighted song could establish "facts or circumstances" giving rise to "red flag" knowledge of infringement; and c) whether the evidence showed willful blindness that could justify imposition of liability on Vimeo, notwithstanding the safe harbor provisions.

Regarding the first of the questions, as it is not within the scope of this paper, it will merely be stated that the appellate court reversed the District Court's finding and held that the DMCA's safe-harbor provisions did apply to pre-1972 sound recordings.[28] Greater attention

[27] The following parties appear as plaintiffs in the case: Capitol Records, LLC, Caroline Records, Inc., Virgin Records America, Inc., EMI Blackwood Music, Inc., EMI April Music, Inc., EMI Virgin Music Inc., Colgems–EMI Music, Inc., EMI Virgin Songs, Inc., EMI Gold Horizon Music Corp., EMI U Catalog, Inc., EMI Unart Catalog, Inc., Jobete Music Co., Inc. and Stone Diamond Music Corporation.

[28] The CLASSICS (Compensating Legacy Artists for their Songs, Service and Important Contributions to Society) Act consolidated into the Music Modernization Act, H.R. 1551, Pub.L. 115–264 (2018) finally solved this issue

will be dedicated to the court's answer to the second and third questions in the analysis that follows. At this preliminary stage it will simply be anticipated that the answer to both questions was negative, thus exempting Vimeo from copyright liability in the case at hand.

B. Analysis of Vimeo's Liability under US Law

1. Definition of Online Service Provider

As the District Court stated in its decision, for purposes of the § 512(c) safe harbor, the DMCA defines "service provider," in pertinent part, as "a provider of online services or network access, or the operator of facilities therefor."[29] This definition "is clearly meant to cover more than mere electronic storage lockers" and is "intended to encompass a broad set of internet entities."[30] Most internet companies known to the public, such as Youtube,[31] Facebook,[32] Google,[33] and eBay[34] fall under the statute's definition of a service provider. In fact, the court in *In re Aimster*[35] commented that the definition is so broad that it had trouble "imagining the existence of an online service that would not fall under the definitions."[36] Vimeo is no exception.

2. Direct and Secondary Liability

In order to establish copyright infringement, a plaintiff must show: a) ownership of a valid copyright, and b) violation of an exclusive right under 17 U.S.C. § 106. The showing of these elements is a requisite for both direct and secondary liability because, as is evident, secondary liability requires a concurrent direct infringement. In the case at hand, the plaintiffs (record labels) were able to establish that they were the rightholders over multiple musical compositions and that these musical compositions had been included, with no authorization, in at least 199 videos uploaded to Vimeo.

In light of the facts, Vimeo could have been potentially liable for direct copyright infringement if it had been considered that the service provider itself carried out reproduction

---

by providing that pre-1972 sound recordings are covered under § 512 safe harbors and § 230 of the Communications Decency Act.

[29] *Vimeo, LLC, 826 F.3d*, quoting *Viacom*, 676 F.3d at 39.

[30] *Vimeo, LLC, 826 F.3d*, quoting Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 744 (S.D.N.Y. 2012).

[31] *See Viacom*, 676 F.3d 19

[32] *See* Miller v. Facebook, Inc., No. C 10-00264 WHA, 2010 WL 2198204, 7 (N.D. Cal. May 28, 2010).

[33] *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007).

[34] *See* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001).

[35] *In re* Aimster Copyright Litig., 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff'd*, 334 F.3d 643 (7th Cir. 2003).

[36] Id. at 658

and public display of the copyrighted content. This was the direction followed in *Playboy Enterprises, Inc. v. Frena*[37] where the court held that, despite having been uploaded by the user, the service provider's automatic copying, storage, and distribution of copyrighted images infringed exclusive copyrights.[38] However, this approach has been found extreme and has been refused by other courts[39] and, where liability of online service providers is found, the major trend is for the court to base its holding on theories of secondary liability.[40] These theories consider that it is the users who directly infringe the plaintiffs' rights by uploading the infringing content onto the platform, but that, provided certain elements are found in the service provider's conduct, its relationship with the users makes it secondarily liable for their underlying activity.

Although only direct infringement has been codified in the Copyright Act, courts rely on two tort common law doctrines to impose secondary copyright liability: contributory infringement and vicarious liability. The former derives from tort law principles of enterprise liability and imputed intent, while the latter is based on agency principles of *respondeat superior*.[41] Contributory copyright infringement has been described as the action of "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[42] That is, in order to succeed on a claim of contributory infringement, the plaintiff must prove that the defendant a) had specific knowledge of the direct infringement and b) made a material contribution to the infringing activity.[43] Vicarious liability attributes strict liability to a party because of its relationship with the direct infringer. It is often found in cases in which the defendant "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities".[44] The elements required for this doctrine to apply are therefore that the defendant a) obtain a financial benefit from the infringing activity and b) have a power of supervision over the direct infringers.[45] The typical

[37] Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993)
[38] See *id*. at 1556-57.
[39] *E.g.* the Northern District of California rejects this approach in Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995). *See id.* at 1369-70. *See also*, following *Netcom*, Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1178 (N.D. Ill. 1997); and Sega Enters. v. MAPHIA, 948 F. Supp. 923, 931-32 n.5 (N.D. Cal. 1996).
[40] *See* Alfred C. Yen at 10.
[41] *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996).
[42] Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1996). *See* also *Fonovisa*, 76 F.3d and A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001).
[43] Mark Bartholomew and Patrick F. McArdle, *Causing infringement,* Vanderbilt Law Review, Vol. 64, No. 3, 615 (2011), at 7.
[44] Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, Boston College Law School Research Paper No. 2000-03(2000), at 10.
[45] Id.

example of this common law doctrine is the liability of an employer for the tortious conduct of its employee. In cases such as *Fonovisa*[46] or *Napster*[47] the courts based their decisions on the analysis of each of the four elements (two for contributory infringement and two for vicarious liability) in order to determine whether the defendant was secondary liable for the infringements at hand. Additionally, in *Grokster*[48] the Supreme Court developed a theory of secondary liability that has come to be known as "inducement of infringement". It held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[49]

Therefore, if the elements of direct infringement were not found in Vimeo's activity, the plaintiffs had the burden of proving that Vimeo's conduct or relationship with its users rendered it secondarily liable for the direct infringement committed under one of the doctrines described. In the case decided, the plaintiffs charged Vimeo with liability in all its potential forms: direct infringement, contributory infringement, vicarious liability, and inducement of infringement. However, if a service provider successfully claims that it complies with the requirements of one of the four safe harbors foreseen in 17 U.S.C § 512, it will obtain an exemption from any potential copyright infringement liability, whether direct or indirect. Thus, should a court find that that all of the elements of § 512(c) coexist in the case it is deciding upon, it need not even enter into a discussion regarding direct or secondary liability. In Vimeo, the defendant succeeded in its safe harbor defense with the result that neither the District Court nor the Second Circuit addressed the issues of primary and secondary liability, but rather, they exempted Vimeo from copyright infringement entirely.

3. US Online Storage Safe Harbor

a. Threshold Criteria

To qualify for protection under any of the safe harbors listed in § 512 the intermediary must comply, firstly, with a set of "threshold criteria" which are common to all exemption regimes and, secondly, with the specific requirements of the particular safe harbor whose application is claimed.[50] To meet the threshold criteria the party must (i) fall within the

[46] *Fonovisa,* 76 F.3d.
[47] *Napster*, 239 F.3d
[48] MGM Studios Inc. v. Grokster, Ltd., 544 U.S. 903 (2005)
[49] *Grokster, Ltd.*, 544 U.S.
[50] *Viacom* at 27.

definition of a "service provider" contained in 17 USC § 512 (k)(1)(B); and (ii) adopt and reasonably implement a "repeat infringer" policy that provides for the termination of infringing subscribers and account holders of the service [17 USC § 512 (i)(1)(A)].[51]

As stated above, Vimeo falls within the definition of a service provider. Additionally, the court found that Vimeo had implemented a repeat infringer policy that was clearly stated in its terms of use, and its adoption was supported by emails that showed employees terminating accounts based on infringement. Furthermore, the court determined that Vimeo required registered users to agree not to infringe third party copyrights and duly informed them that their accounts would be terminated should this agreement be vulnerated. The platform also provided the contact information for its DMCA agent,[52] thus complying with the threshold criteria to the satisfaction of the fact finder.

b. Specific Criteria

Regarding the specific Storage Safe Harbor criteria, the intermediary enjoys non-liability when it (i) has no actual or red flag knowledge that the material is infringing; (ii) does not receive financial benefit from infringing activity; and (iii) upon notification of alleged infringement expeditiously removes content or blocks access to it (notice and takedown regime).[53]

i. Actual or "Red Flag" Knowledge

A service provider may be disqualified from safe harbor protection if it possesses one of two types of knowledge. First, the service provider must not have "actual knowledge that the material (...) on the system or network is infringing."[54] In other words, the service provider must not know for a fact that its services have been used to infringe a specific or various specific and identifiable copyrights [§ 512(c)(1)(A)(i)]. Second, even without actual knowledge, a service provider may lose its entitlement to safe harbor protection if it is "aware of facts or circumstances from which infringing activity is apparent."[55]

In *Viacom*[56], the Second Circuit clarified the relationship between actual and red flag knowledge stating that actual knowledge will be demonstrated when the provider

[51] *Id.*
[52] *See* 17 USC §512(c)(2).
[53] 17 U.S.C. § 512(c)(1).
[54] 17 U.S.C. § 512(c)(1)(A)(i).
[55] 17 U.S.C. § 512(c)(1)(A)(ii).
[56] See fn 22 above.

"subjectively" knew of specific infringement, while "red flag knowledge" will be shown when the provider was "subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[57] In other words, even if Vimeo did not have actual knowledge of the infringements carried out by its users, plaintiffs could try to prove that it actually knew certain facts which, although not directly an infringement *per se*, would objectively lead any reasonable person to conclude that an infringement was taking place.

In this particular case, what gave rise to the red flag debate was that some employees of Vimeo were found to have viewed user-generated videos containing copyrighted works. Thus, the second question certified to the Second Circuit was whether under *Viacom*, these facts could give rise to "red flag" knowledge of infringement within the meaning of § 512 (c)(1)(A)(ii). The District Court had denied Vimeo's motion for summary judgment regarding a number of videos containing plaintiffs' copyrighted works on the basis that they had been viewed by employees of Vimeo in the course of their activities. For the reasons summarized below, the Second Circuit vacated the court's order denying Vimeo summary judgment as to red flag knowledge with respect to those videos. In other words, the answer to the certified question was that even where a copyright owner proves that a service provider's employee viewed a video containing a recognizable copyrighted song, that evidence is insufficient to establish red flag knowledge.

The court's reasoning lay on the assumptions that a) the employee's viewing could have been brief;[58] b) the purpose of the viewing could have been strictly for technical matters; c) even if the music was "recognizable" or "famous", the employee might not have been familiar with it due to her specific music tastes and culture;[59] and d) employees cannot be assumed to have expertise on copyright and they may not know how to distinguish between uses which may be legal as a consequence of fair use or if the user had an authorization to use the copyrighted music.[60]

It can therefore be observed that the bar set for benefiting from a lack of red flag knowledge is not very high, and courts can be quite flexible in holding that a service provider has no reason to know of the infringement taking place on its site.

[57] Id. at 28.
[58] *Vimeo* at 96.
[59] *Id.* at 97.
[60] *Id.* at 96.

ii. Right and Ability to Control Infringing Content From Which It Financially Benefits

Section 512(c) also provides that, to obtain safe harbor protection, a service provider 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" [17 U.S.C. § 512(c)(1)(B)]. Protection is therefore lost if a service provider (1) has the right and ability to control the infringing activity and (2) receives a financial benefit attributable to that activity.

Ability to control has been found in very few cases in which it is determined that a service provider exerts "substantial influence on the activities of users".[61] In the case at hand, despite some evidence regarding restrictions on the content of uploaded material in Vimeo's guidelines and the existence of direct communications between Vimeo's staff and some of its users regarding content, the District Court concluded (and the appellate decision confirmed) that Vimeo lacked the right and ability to control infringing activity under the terms of § 512(c)(1)(B). It therefore did not need to decide whether Vimeo received a financial benefit.

iii. Notice and Takedown

Rather than monitoring the user uploaded content for possible copyright infringement, online intermediaries may wait for copyright holders to notify them of specific infringements. The intermediary preserves its immunity if it expeditiously takes down the allegedly infringing content as soon as notified by the rightholder. In case the uploading user objects and the rightholder does not initiate legal proceedings, the intermediary must make the content available again.[62]

The court found that Vimeo had an adequate "notice and takedown" mechanism installed on its website and that it had acted with sufficient expeditiousness to comply with the § 512(c)(1)(C) standard (one-day response time for individually identified videos and three and a half weeks for an "in bulk" identification of 170 videos).

4. No Affirmative Duty to Monitor

17 U.S.C. § 512(m)(1) sets forth that no interpretation of the statutory safe harbors should be construed as to impose on the service providers an affirmative duty to monitor their website or platform for copyright infringement. The final issue discussed in the appeal involved

[61] *Viacom*, 676 F.3d and *Grokster, Ltd.,* 544 U.S.
[62] 17 USC § 512 (g)(2).

the application of the "willful blindness" theory and its compatibility with the principle that service providers shall not bear the expense of monitoring the activity carried out by its users.

Willful blindness is a doctrine that originated in criminal law and is found where the defendant knows (subjectively) of the high probability of the existence of a fact and takes deliberate steps to avoid learning of that fact (objectively). [63] In the world of copyright, it may be found when an intermediary takes deliberate steps to avoid learning of a copyright infringement carried out by users of its service. In the famous words of the Seventh Circuit in *Aimster* "willful blindness is knowledge". [64]

The plaintiffs in the case claimed that Vimeo should be found liable under the willful blindness doctrine on account of three arguments: a) Vimeo monitored videos for infringement of visual content but willfully avoided monitoring audio content; b) having awareness of facts that suggested a likelihood of infringement, Vimeo decided not to further investigate and c) Vimeo encouraged users to post infringing matter, and could therefore not turn a blind eye on the infringements that occurred under that encouragement.

The Second Circuit rejected the first arguments on the basis of its prior decision in *Viacom*, where it stated that § 512(m)(1) relieves service providers of any obligation to monitor for infringements posted on its website, arguing that the fact that Vimeo voluntarily undertook to monitor videos for a certain type of infringement did not deprive it of the privilege of not having to monitor for other infringements. As to the second argument, § 512(m)(1) was once again used to shield Vimeo from any obligation to carry out further investigations to obtain more knowledge than that which it possessed. The court stressed the importance that Congress gave to protecting service providers from the expense of monitoring with the objective of encouraging the investment in the furtherance of internet capabilities.[65]

The court admitted that § 512(m) would not shield Vimeo from liability on the grounds of the third argument posed by the plaintiffs, the encouragement of the underlying infringements on behalf of the service provider. However, from the evidence submitted, it was determined there was not enough proof to find that Vimeo had participated in a generalized encouragement of infringement.

---

[63] Fiona Finlay-Hunt, *Who's Leading the Blind - Aimster, Grokster, and Viacom's Vision of Knowledge in the New Digital Millennium*, 2013 Colum. Bus. L. Rev. 906 (2013).
[64] *See* In re *Aimster Copyright Litig*., 334 F.3d 643.
[65] *Vimeo, LLC, 826 F.3d.*

From the above it seems clear that § 512(m)(1) can serve as a powerful shield to deflect liability based on the level of knowledge that a service provider can be expected to acquire.

5. Fair Use

As already stated, when a court finds that a service provider is exempt from liability on the basis of a DMCA safe harbor provision, no further analysis into liability is due. Therefore, in *Vimeo* the court did not undergo a fair use analysis. However, for the purposes of the comparative law exercise carried out in this paper, it is worth noting that even if a service provider could on a *prima facie* basis be considered to be responsible for the content posted on its website, it will not incur liability for such content if it can be found that it is covered by a fair use exemption. The relevant statutory provision (17 USC § 107) describes four factors to consider when evaluating if the use of a work is fair: a) the purpose and character of the use; b) the nature of the work; c) the amount and portion used of the work; and d) the effect of the use upon the potential market for or value of the copyrighted work. This judge-made fair use doctrine, characterized by its flexibility (*numerus apertus*) when weighing the stated factors, contrasts with the EU exceptions and limitations systems which are usually enacted in the form of a closed list.

C. Analysis of Vimeo's liability under EU Law

The following paragraphs will examine the liability that an online content sharing service provider of Vimeo's characteristics could face under the DSMD. It must be pointed out that since *Capitol Records v. Vimeo*, Vimeo has adapted its policies to comply with current global regulations. However, for the academic purposes of this paper, the factual findings of the 2016 US case will be used as the backdrop for a practical application of article 17 of the DSMD. This exercise will serve to hypothesize on the possible decision that a EU court could reach if it were eventually (after June 2021)[66] presented with the same case that the Second Circuit had to decide in 2016.

1. Definition of Online Content Sharing Service Provider (OCSSP)

The first step a European court would have to take in its liability evaluation would be to decide whether Vimeo's activity falls under the scope of article 17 of the DSMD. Even though EU regulation has its own definition of a "service provider",[67] the definition that is

[66] See fn 15 above.
[67] See Article 2 b) and c) of eCommere Directive: a "service provider" is "any natural or legal person providing

pertinent for the application of the obligations and exemptions set forth in article 17 of the Directive is that of an OCSSP, a particular subset of service providers.

Article 2(6) of the Directive provides a general definition to be read in conjunction with a series of exclusions. It describes an OCSSP as an internet service provider that provides services with "the main or one of the main purposes" of storing and giving "the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organizes and promotes for profit-making purposes". The second paragraph of article 2(6) goes on to exclude from the general definition a series of providers, including a) not-for-profit online encyclopedias, b) not-for-profit educational and scientific repositories, c) open source software-developing and-sharing platforms, d) providers of electronic communications services as defined in Directive (EU) 2018/1972,[68] e) online marketplaces, f) business-to-business cloud services, g) and cloud services that allow users to upload content for their own use. The wording of this paragraph, in which the list is preceded by a "such as", hints that this is an open list to which other internet service providers can adhere if they are of an analogous nature to that of the excluded service providers. In the present case, it could easily be argued that Vimeo's main purpose is the storage and public access to a large amount of copyright-protected works or other subject matter uploaded by its users, and that Vimeo "organizes and promotes" such content for "profit-making purposes".[69]

Certain video hosting services may try to argue that the content which they host is exclusively or primarily created originally by their own users, from whom they have obtained all pertinent licenses for the use of their original work, and that its main purpose is not therefore the storage and access granting to a large amount of *third party* (in this case meaning "non-user created") copyright-protected works. However, a literal interpretation of article 2(6) in connection with article 17 of the DSMD inclines towards considering that this "third party" factor is not a requirement for the application of the provisions. It would appear that even if the copyright-protected work is primarily created by the users of the platform, the service provider does have a main purpose of storing and granting access to protected subject matter, and it qualifies as an OCSSP. The fact that the original rights in that protected subject matter belongs

an information society service", and an "established service provider" is a "service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period."

[68] See article 2(4) of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) Text with EEA relevance, PE/52/2018/REV/1 (OJ L 321, 17.12.2018, p. 36–214).

[69] Article 2(6) DSMD.

to users from whom the platform has obtained licenses merely means that the OCSSP has complied with the obligation of obtaining an authorization from the rightholders of the work, as required in article 17.1 of the DSMD. In any case, it appears that Vimeo has accepted that article 17 of the DSMD applies to its services[70] and the platform is frequently cited as one of the "large" content providers envisioned by the European legislator.[71] However, given the ambiguity of the language in the definition, it is possible that a European court could have a different view in light of the particular characteristics of a service provider.

When analyzing Vimeo's responsibility under the US regime, it was observed that its qualification as a service provider opened the door, as a first requisite, to its liability exemption. By contrast, Vimeo's qualification as a OCSSP imposes burdens rather than exemptions on the service provider when operating in the EU, and closes the door to a possible harboring under the eCommerce liability exemptions.

2. Direct Liability Under DSMD Article 17

a. Direct Liability of OCSSPs

As explained above, in the US, the liability of a hosting service provider, when found, is more likely to be considered secondary rather than direct, provided that the service provider did not engage in an active conduct of uploading and promoting infringing content on its site. This also seemed to be the initial trend in the EU[72] where service providers (at large) were considered "intermediaries whose services are used by a third party to infringe an intellectual property right"[73] and against whom the available remedies consist of injunctive relief.[74] However, after the decision rendered in *The Pirate Bay*,[75] the CJEU showed an inclination towards holding service providers directly liable for the infringement of third party

[70] Vimeo was actually a lobbyist against article 13 of the proposal for the Directive, *see* VIMEO, https://vimeo.com/blog/post/article-13-day-of-action/ (last visited April 22, 2020); and it appears that it has currently adapted its service to comply with article 17, *see* https://www.termsfeed.com/blog/eu-copyright-directive-article-17/#Do_The_Rules_Apply_To_All_Types_Of_Content (last visited April 22, 2020).

[71] *See, e.g.* Tobias Kempas, *The New Copyright Directive: Are OCSSPs Now Required to Carry Certain Content?*, Lexology, 2019: "Article 17 thus applies not only to large content providers such as YouTube, Dailymotion and Vimeo, but to any type of user-upload service provider that fits the broad definition." Available at https://www.lexology.com/library/detail.aspx?g=efb1d490-adb8-4058-be28-52adbb3d3bc4

[72] See *GS Media* (CJEU, C-160/15, ECLI:EU:C:2016:644 – GS Media.), *The Pirate Bay* (CJEU, C-610/15, ECLI:EU:C:2017:456 – Stichting Brein/Ziggo) and *Filmspeler* (CJEU, C-527/15, ECLI:EU:C:2017:300 – Stichting Brein/Wullems).

[73] *See* article 8.3 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10–19).

[74] Id.

[75] See fn 72.

copyrights.[76] As anticipated above, the concepts of direct and secondary liability were not codified on a EU level, and different member states applied their own national laws to address this issue.

Article 17.1 DSMD harmonizes this matter, thus further aiding in the EU's objective of creating a unified single market. It does so by considering that it is the OCSSP who directly performs the act of communicating to the public or making available to the public protected subject matter uploaded by its users. Thus, for the hypothetical case at hand, unless Vimeo can prove that it has complied with the requirements of article 17.4 (discussed below), an unauthorized offering of protected content on its website will render the host *directly* liable. This means that in order to succeed under an article 17 claim, the plaintiff's burden of proof is limited to showing that a) it is the rightful owner of the copyright or neighboring right over a work or related subject matter and b) such protected content is harbored and displayed on the OCSSP's website. The provision ends the discussion which took up a great deal of analysis in the CJEU's case law regarding whether an act constituted a "communication" and whether that communication could be considered to be made "to the public."[77] Article 17 makes it clear: if an OCSSP provides public access to copyright-protected works or other protected subject matter uploaded by its users, it is performing an act of communication to the public and thus exploiting an exclusive right of the relevant rightholders. Proof and analysis of additional elements such as the level of knowledge of the service provider is no longer required, significantly lightening the burden on rightholders.

In the case at hand, there is no question that Vimeo is considered, for purposes of the DSMD, to be performing an act of communication to the public. Specifically, Vimeo would be considered to be performing an act of communication to the public in the modality of making the works and other subject matter available to the public. Making available to the public is defined in article 3.1 of Directive 2001/29/EC as providing availability of works "in such a way that members of the public may access them from a place and at a time individually chosen

[76] For further detail on this issue *see* Eleonora Rosati, *Intermediaries and IP: 5 key principles of EU law*, IPKat (May 21, 2018), http://ipkitten.blogspot.com/2018/05/intermediaries-and-ip-5-key-principles.html

[77] *See* CJEU 13 February 2014, no C-466/12 (Nils Svensson, Sten Sjögren, Madelaine Sahlman and Pia Gadd v Retriever Sverige AB) and CJEU 21 October 2014, no C-348/13 (BestWater International GmbH v Michael Mebes and Stefan Potsch). For further detail on the CJEU's case law regarding communication to the public see Jane C. Ginsburg, *The Court of Justice of the European Union Creates an EU Law of Liability for Facilitation of Copyright Infringement: Observations on Brein v. Filmspeler [C-527/15] (2017) and Brein v. Ziggo [C-610/15] (2017)*, AUTEURS & MEDIA, VOL. 2017, P. 7, 2017 (IN FRENCH); COLUMBIA LAW & ECONOMICS WORKING PAPER NO. 572; COLUMBIA PUBLIC LAW & LEGAL THEORY PAPER NO. 14-557 (2017), available at: https://scholarship.law.columbia.edu/faculty_scholarship/2053

by them."[78] Unlike an act of direct broadcasting or streaming carried out, for example, by a TV broadcaster or an internet radio, a user of Vimeo's services can decide when and where (as long as the selected location offers internet access) to view a desired video uploaded to the platform. Whether an act is considered to be an act of communication to the public in the broad sense or in its modality of making available to the public has certain consequences regarding the types of rightholders whose authorization becomes necessary to carry out the activity. Whereas authors of copyrighted works have an exclusive right to authorize the public communication of such works in any modality, holders of certain neighbouring rights such as performers, phonogram producers, film producers and broadcasting organisations only have a right to authorize the communication to the public of the subject matter on which their rights fall if it is carried out in the modality of making available to the public.[79]

Regarding videos uploaded by its users, Vimeo would therefore need to obtain the authorization of any pertinent (i) authors, (ii) performers (e.g., singers or actors), (iii) phonogram producers (record labels), and (iv) film producers. From the findings of the proceedings it appears that most videos uploaded to the website were original creations of their uploading users in terms of their "visual" aspects, but they included unauthorized musical copyrighted material. This means that Vimeo had obtained, through direct licenses granted by its users when accepting the site's Terms and Conditions, the necessary authorizations to communicate to the public and publicly perform the works and related subject matter pertaining to authors, performers, and producers of the "movie". However, they were lacking the authorization of authors and performers of the musical composition, and of phonogram producers, i.e., rights held by the plaintiff record labels in the case brought to court.

b. What About Users that Obtain a Profit?

The text considers that both OCSSPs and users of their services carry out acts of communication to the public. OCSSPs must always obtain a license to cover themselves from the act of communication to the public that is considered to be carried out by them (e.g. the uploading of content by the platform) and, the text specifies, this license shall also cover the

[78] For an analysis of the application of the WTC concept of "making available" and the Berne Convention concept of "communication to the public" see Ginsburg, Jane C., The (New?) Right of Making Available to the Public. INTELLECTUAL PROPERTY IN THE NEW MILLENNIUM, ESSAYS IN HONOUR OF WILLIAM R. CORNISH, David Vaver, Lionel Bently, eds., pp. 234-47, Cambridge University Press, 2004. Available at SSRN: https://ssrn.com/abstract=602623

[79] *See* United States Copyright Office, *The making available right in the United States, a report of the register of copyrights* (February 2016), available at https://www.copyright.gov/docs/making_available/making-available-right.pdf on the implementation of this right in the US legal system.

acts carried out by users of the services when they are not acting on a commercial basis or where their activity does not generate significant revenues.

Where the activity of the users of the services provided by OCSSPs *does* have a commercial basis or generate significant revenues, it is the user who must also obtain its own license in order to upload the protected content onto the OCSSP's platform. This license obtained by the user will cover the activity of the OCSSP (recital 69 DSMD). The vague terms, commercial basis, and significant revenues, will have to be interpreted by the courts and possibly by the Member States when they transpose the content of the Directive into their national law.[80]

3. Affirmative Duties Under Article 17.4 DSMD

The DSMD sets forth a series of duties that can be divided into two variants: the first, applicable to OCSSPs in general (article 17.4 DSMD), and, the second, applicable exclusively to those OCSSPs which have been established in the EU for less than three years and have an annual turnover below € 10 million (article 17.6 DSMD) i.e., to "startups" which may not possess the resources necessary to properly comply with all the requirements set forth in article 17.4. In the case of Vimeo, established in 2004 and with an annual turnover (in 2018) of over $160 million,[81] it is the first variant that could potentially apply.

a. Duty to actively seek an authorization

OCSSPs are responsible for obtaining an authorization from rightholders, which will cover the activity of their non-commercial users. They must, therefore, employ their "best efforts" to obtain the relevant authorization [article 17.4 a) DSMD]. These best efforts shall consist of using the means that, according to their particular characteristics, seem reasonable and proportional (article 17.5 DSMD). This means that if an OCSSP does not obtain an authorization, it should generally be because of the difficulty of localizing the rightholder over a work or protected subject matter or because, having been tracked down, the rightholder has refused to grant such authorization. It should be recalled that, as the rights that the OCSSP must obtain are exclusive rights (as opposed to rights of equitable remuneration), the rightholders may refuse to grant a license or may decide to withhold their authorization for a certain period

[80] Rafael Sánchez Aristi, Nora Oyarzabal Oyonarte, *La Directiva (UE) 2019/790, de 17 de abril de 2019, sobre los derechos de autor y derechos afines en el Mercado Único Digital*, LA LEY MERCANTIL Nº 60, 31 (2019).
[81] REUTERS, *Vimeo revenue jumps 54 percent in 2018, paying subscribers near 1 million*, available at https://www.reuters.com/article/us-vimeo-results/vimeo-revenue-jumps-54-percent-in-2018-paying-subscribers-near-1-million-idUSKCN1PW2OJ

of time (in order to, for example, comply with exclusivity agreements with other service providers). The case may also be that the OCSSP is not interested in accepting the economic terms offered by the rightholder, even though a certain good faith attempt to negotiate should be expected.[82]

In *Vimeo*, it was found that the service provider had not obtained or even tried to obtain an authorization from any of the rightholders of the copyrighted works that were being displayed on its website. As the requirements listed in article 17.4 are cumulative, the non-compliance by Vimeo of the duty to actively seek an authorization would have rendered it directly liable under article 17.1. However, in the following paragraphs, and for the academic purposes of this paper, the remaining requirements which Vimeo would hypothetically have to comply with in order to benefit from the Directive's safe harbor will also be reviewed.

b. Duty to Block Unauthorized Works and Protected Subject Matter

Where an OCSSP actively seeks an authorization but, having complied with the diligence required of it, is unsuccessful in obtaining it, the OCSSP must deploy its best efforts to ensure that those works or subject matter are not available on its site. In order for the OCSSP to do so, the cooperation of the rightholders providing the information necessary for the "blocking" of this content to take place is essential.

This *ex ante* requirement is a novelty that contrasts with the traditional "notice and takedown" system foreseen in US law and in the eCommerce Directive (and also, subsequently, in article 17 DSMD itself), under which service providers do not have a duty to be proactive in aiding to block infringing content from their sites, but rather their obligations are not created until they receive a notification from the alleged holder of an infringed copyright. It is to be noted that proactivity is also required of the injured rightholder, as it must cooperate in providing the information (e.g., fingerprint) that will enable the OCSSP to successfully prevent infringing content from even appearing on its site. The burden of this "blockage" is therefore distributed between rightholders and platforms.

Thus, for Vimeo to comply with this obligation, it must first actively filter the content which a user tries to upload and, before it is even uploaded, check whether that content has been licensed to the platform or not. This can be done by using measures such as Content ID

[82] *See* Matthias Leistner, *European Copyright Licensing and Infringement Liability Under Art. 17 DSM Directive Compared to Secondary Liability of Content Platforms in the U.S. – Can We Make the New European System a Global Chance Instead of a Local Challenge?*, Intellectual Property Journal (IPJ) 22 (forthcoming 2020).

(known for its implementation by Youtube) or Copyright Match, which was in fact implemented by Vimeo in 2014 (the suit giving rise to the *Vimeo* case was filed in 2009). These measures began as a private filtering mechanism installed by service providers on a voluntary basis, but the text of the DSMD raises questions as to whether there is an existing alternative to filtering in order to comply with the mandatory requirements of article 17.

The technologies mentioned are based on digital fingerprinting that matches content which a user tries to upload to the platform's database in order to determine whether or not it is copyrighted.[83]In simplified terms, Content ID works by classifying uploaded works in three types of "lists": blacklisted content, whitelisted content, and greylisted content. Blacklisted content consists of protected works for which rightholders have expressly denied an authorization (until now, generally through the platform's notice and takedown system). Whitelisted content is made up of copyrighted works that have been authorized (generally in exchange for remuneration) to be used by the service provider. Content in the grey list of a platform is characterized by having unknown ownership because the potential holder of rights over it has not contacted the service provider in order to ascertain its rights.

Under the voluntary Content ID systems initially implemented by platforms such as Youtube, a work would only be prevented from being uploaded onto the website if it matched with a work included in the service provider's blacklist. This meant that content on the service's grey list could be freely uploaded and would not be taken down until an infringement notice was received, and content matching the provider's whitelist would freely go up in accordance with whatever terms had been reached between the exploiting platform and the underlying rightholders.[84]

Until now service providers had benefitted from a large stock of "grey" listed content, which could be uploaded and exploited without sharing any benefits of such exploitation with any potential rightholders. The EU regulation changes this scenario as it will heavily increase the incentives for an OCSSP to include as many works as possible on its whitelist and to negotiate with their rightholders the economic terms for the authorization to use such works. If a service provider such as Vimeo considers that it benefits from making copyrighted work available on its site, it should seek to enter into agreements with rightholders and their

[83] Giancarlo Frosio, *Reconciling Copyright with Comulative Creativity: The Third Paradigm*, Edward Elgar Publishing Limited (2018).
[84] For more information regarding how Content ID works *see, e.g.*, YOUTUBE, https://support.google.com/youtube/answer/2797370?hl=en (last visited, April 26, 2020).

representatives (e.g., film producers, music producers, collective management organizations) by negotiating in accordance with industry standards in order to obtain pertinent authorizations and "whitelist" any exploited works. If the OCSSP is not able to obtain an authorization, it must ask the copyright holder to provide it with information, such as the work's "fingerprints," necessary to include the work in its blacklist. Thus, the "list" scheme will eventually develop into, on the one hand, a whitelist including non-copyrighted work that can be freely uploaded and copyrighted work for which an authorization has been obtained that can be uploaded in accordance with the terms of such authorization, and on the other hand, a blacklist that will prevent any works included in it from accessing the service provider's platform at all. However, the OCSSP can also maintain a "grey list" and will not incur liability as to those works when best efforts could not find the rightholder (or when the rightholder gave no instructions).[85]

c. Notice, Takedown, and Staydown

Despite the first two defense mechanisms listed in sections a) and b) of article 17.4, it is possible that certain protected content manages to appear on the OCSSP's website. In such a circumstance, the holder of a copyright or neighboring right over the protected content can send a "sufficiently substantiated notice"[86] to the OCSSP identifying the infringing material. Upon receipt of such notice, the OCSSP must act expeditiously to block or remove the content from its site and to block future uploads of those works or protected subject matter. This blocking obligation is potentially perpetual unless the rightholder grants an authorization in the future.[87] Thus, the DSMD shares the "notice and takedown" provision of § 512 (c)(1)(A)(iii) but adds a new "stay down" requirement which has not been codified in US law. Rather, the DMCA introduced a takedown and "put back up" provision in 17 USC § 512 (g). Relying on the fingerprint technology example used in the previous section, this would mean that any infringing content that is duly notified by its rightholder would shift to Vimeo's blacklist and thus not be able to be uploaded again as a consequence of its *ex ante* blocking.

4. Exceptions

The Directive's provision that will likely be among the most difficult to apply in practice, is the mandatory exceptions or limitations that must be available for users when

[85] DSMD, article 17.4.
[86] Id., sec.(c).
[87] Montigliani at 23.

uploading copyrighted works. Article 17.7 establishes that the measures implemented by OCSSPs in order to comply with their *ex ante* filtering obligations should not prevent users from uploading content that is either not protected by copyright or that is covered by an exception or limitation.[88] The article specifically lists the exceptions of quotation, criticism, review,[89] caricature, parody, or pastiche.[90] As anticipated above, only where the use of copyright falls under one of these types of use will it benefit from an exception. Thus, unlike the US, the EU limitation system does not contemplate broadening the scope of the list to new judge-made exceptions, regardless of how "fair" the use could appear to be.

While OCSSPs are required to filter and block unauthorized copyrighted works from their services, they must be wary of "over-blocking."[91] Filtering systems must be developed in a way that protects not only copyright, but also other third party interests and fundamental rights. Determining whether a content contains copyrighted work and, furthermore, whether that copyrighted work can be used under the protection of an exception, is not always an easy task. There does not appear to be, in the current state of the art, a machine capable of judging whether a work is protected by copyright and whether an exception to its use may apply.[92] Additionally, the complaint and redress mechanism foreseen in article 17.9 DSMD states that decisions to disable access or remove uploaded content "shall be subject to human review." In light of the strict liability an OCSSP may face if it posts unauthorized copyrighted content, a provider could be inclined to block in excess. In other words, when in doubt, avoid the risk of being found liable for infringement. However, these agents are faced with an added problem: excess blocking can also be an infringement of the Directive. It seems rather excessive that the OCSSP be liable for both not blocking enough and for blocking too much. An OCSSP should be able to shield itself from an "excess blocking" claim by proving that it has installed a reasonable complaint and redress mechanism in terms of article 17.9 DMSD which permits users to make a claim for the legality of the use of the works they have uploaded. The OCSSP should be able to prove that this redress mechanism follows reasonable internal guidelines and,

[88] As Montagnani states, this approach codifies in the EU the jurisprudential principle developed in the US *Lenz* case. *See* Maria Lillà Montagnani, *Virtues and Perils of Algorithmic Enforcement and Content Regulation in the EU- A Toolkit for a Balanced Algorithmic Copyright Enforcement*, Journal of Law, Technology & the Internet, Vol. 11, 26 (2019-2020).
[89] DSMD, article 17.7(a).
[90] DSMD, article 17.7(b).
[91] *See* Tobias Kempas, at 2: "CJEU, technical filtering and/or blocking measures must be strictly targeted in the sense that they must serve to bring an end to an infringement of copyright or related rights without affecting the accessibility of lawful information". *See also* cases C-70/10 (Scarlet Extended), at 52, C-360/10 (SABAM), at 50 and C-314/12 (UPC Telekabel), at 56.
[92] Id. at 2.

even if the mechanism does not render the same result that a court would eventually dictate, it should not be considered liable if it provides evidence that it employed its best efforts to create an adequate private resolution system. The "human review" required by article 17.9 DSMD must take into consideration that reviewing humans cannot be required to have a solid background in copyright, as this would impose unreasonable costs on the OCSSP. A flexible assessment of OCSSPs' compliance with their obligations to make non-infringing content available is therefore advisable. This view is reinforced by the fact that the requirement that service providers host and provide access to certain content appears to limit their freedom to conduct business in accordance with their own criteria.

5. No General Obligation to Monitor

Article 17.8 DSMD clarifies that the provisions set forth in article 17 should not be construed as to impose "any general monitoring obligation" on OCSSPs. The general monitoring obligation which the article refers to is the one established in article 15 of the eCommerce Directive. The article states that service providers shall not have a duty to generally monitor the information which they transmit or store or to actively seek facts or circumstances which indicate illegal activity. 17 USC § 512(m)(1) discussed above also establishes that service providers have no duty to monitor nor to "affirmatively seek" facts indicating infringing activity.

Article 17.8 DSMD has sparked debate among academics, as it may appear a contradiction that an OCSSP is, on the one hand, required to both filter uploaded content in order to block works identified by unauthorizing or non-localized rightholders, and prevent the blockage of non-protected works and works that can benefit from an exception or limitation but, on the other hand, it cannot be burdened with a general monitoring obligation.[93] A possible interpretation that would render the conflicting provisions compatible is that, while there may not be a *general* obligation to monitor, EU regulation can impose *specific* monitoring obligations on service providers.[94] That is, OCSSPs can be required to implement proactive monitoring mechanisms regarding specific works for which they have obtained the necessary information from their users to identify specific works.[95] What the DSMD then does, is impose an active duty on OCSSPs to obtain *specific* information regarding copyrighted work and use

[93] *See e.g.* Andrej Savin et al., *Open Letter to the European Commission - On the Importance of Preserving the Consistency and Integrity of the EU Acquis Relating to Content Monitoring within the Information Society* (2016).
[94] *See* Leistner at 15.
[95] *Id.*

this information for its *ex ante* filtering. Under the premise that European legislative bodies create legislation that is consistent, this interpretation appears reasonable. It would further support the consideration that the review of an OCSSP's out-of-court redress mechanism foreseen in article 17.9 DSMD should be assessed in light of the specific information that the service provider has received through rightholders' cooperation, and that platforms should not be found to be strictly liable for making, perhaps incorrect, blocking decisions when analyzing whether a user falls under a non-infringement exception.

III. Strategic Considerations for Global Service Providers

Within the current legal framework, there are a series of decisions that service providers such as Vimeo must make when developing their business strategies. Firstly, they must decide whether to operate in Europe at all, in light of the obligations forced upon them. In this regard, big tech service providers will likely decide to do so given the significant revenue derived from the European market, and smaller market players should be able to benefit to some extent from the laxer system devised for startups in article 17.6 DSMD. However, a service provider might decide that its target market is mostly US-based and that it is not economically sound to invest in an EU compliance mechanism. It could employ tools such as geoblocking[96] in order to ensure that its website is not available in EU Member States, thus avoiding having to comply with the DSMD's provisions.

Secondly, service providers should decide whether it is more beneficial for them to design two different systems of copyright compliance, one for services rendered in the US and another for services rendered in Europe. A service provider may decide that its business will be better off by taking advantage of the more lenient liability framework that the US provides and to invest in a second compliance mechanism designed exclusively for its activity in Europe. However, tech companies should be aware that the US Congress is currently reviewing certain provisions of the 1976 Copyright Act, and might be influenced by the European system when and if it alters the § 512 safe harbor regime.[97] Although it is hard to predict the US legislative outcome, it might be sound for service providers to protect copyright holders more strongly than currently required in the US, and design a compliance mechanism consistent with the

[96] For more information on geoblocking *see e.g.* Marketa Trimble, *Geoblocking, Technical Standards and the Law* (2016). *Scholarly Works*. 947.

[97] In this regard, the Subcommittee on Intellectual Property held a hearing on March 10, 2020 to discuss *Copyright Law in Foreign Jurisdictions: How are other countries handling digital piracy?*. A recording of the hearing is available at https://www.judiciary.senate.gov/meetings/copyright-law-in-foreign-jurisdictions-how-are-other-countries-handling-digital-piracy (last visited, April 26, 2020).

stricter EU obligations, in order to prepare for a potential future adaptation of US policies.

Should a service provider decide to install a US-EU compatible filtering and blocking system, it will face challenges designing internal compliance mechanisms that take into account both the DSMD's defined exceptions and the US broader fair use exceptions. In practice, some companies adopted a proactive monitoring approach, on their own initiative, before they were strictly legally obliged to do so. They invested in the technology that other market players will now have to develop or acquire. Their next challenges are numerous. First, they will have to decide how to adapt these technologies developed in-house to the requirements of the DSMD, especially in light of the provision that prevents them from "overblocking" non-infringing content and the requirement that they employ humans to review such content. Second, they now must determine what constitutes a quotation, criticism, review, caricature, parody, or pastiche. Third, their policies should also (even though, for now, on a voluntary basis) set guidelines for determining, for example, whether the use of a work is "transformative"[98] or if it complies with the "purpose and character" element of 17 USC § 107(1). Finally, potentially having to coincide with a judge's opinion regarding the amount (for the case of music and videos, the amount of time) considered to be "substantial" in terms of 17 USC § 107(3), in order to comply with US "fair use" provisions, could prove to be a tricky proposition.

Tools such as Content ID and Copyright Match have been useful to shorten the value gap between service providers and large copyright holders,[99] as the latter have the means necessary to provide service providers with the information required to create their "online ID" and to monitor and notify any infringing uses of their works. The DSMD now places the burden of proactivity regarding the protection of all copyrighted works (whether owned by small independent authors or large publishing companies) on the service providers. The latter now have an incentive to invest in technology that makes it easier to coordinate with smaller creators and performers and not just with larger rightholders.

IV. Conclusion

Throughout this paper, it has been shown that the existing differences underlying the US DMCA and the EU DSMD can subject a service provider to distinct copyright liability schemes when operating in one region or the other. The disparity can be as extreme as finding

[98] *See e.g.* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1166 (9th Cir. 2007), citing Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).

[99] *See* Jane C. Ginsburg, *A United States Perspective on Digital Single Market Directive art. 17*, for EU COPYRIGHT LAW: A COMMENTARY, Irini Stamatoudi and Paul Torremans, eds., (2d ed. Edward Elgar, (forthcoming 2020), 19.

that a multimillion company that hosts millions of videos on its site, such as Vimeo, has absolutely no liability for copyright infringement under one system, and could theoretically be found directly liable for exploiting unauthorized works under the other.

It appears that, in this instance, the EU has acted at a faster pace than the US in order to provide a solution to the participants' complaints about sharing the value derived from the exploitation of copyrighted works online. It is likely that the adaptation by service providers operating in Europe to the EU Directive will help identify which of its provisions pose the biggest challenges for internet companies. In addition, the case law of the CJEU and of EU member states' national courts will help define some of the ambiguous terms contained in the DSMD. This presents the US Congress and industry stakeholders with an excellent opportunity to learn from the virtues and mistakes of the European legislator in order to potentially revise the current § 512 safe harbors and adapt them to the new technological capabilities of internet companies.[100] Such companies appear to be capable of sharing part of their revenues with the copyright holders that have helped in their earning. In fact, this paper has described that, in practice, many companies have adopted an in-house system which uses available technology to remunerate copyright holders. Until now, it has mainly been large copyright holders with strong negotiating power that have been able to participate in the profits created by their works. Ideally, article 17 will arm smaller copyright holders with the tools necessary to join in the reaping of the revenues which they help generate. Hopefully, the US legislator will take due note of what is happening in Europe in order to review its national legislation. This review should rebalance the promotion of progress not only through the advancement of technology, but also through the protection of the arts. Indeed, authors' creations have very recently proven to be the motor that keeps the spirit of humanity alive in times of a crisis such as a worldwide pandemic.

[100] Id.