

# **U.S. Copyright Law, Technology and Litigation. A National Approach and its International Consequences**

*La tecnología, el copyright norteamericano y su litigio.  
Un enfoque nacional con consecuencias globales*

Roberto **GARZA BARBOSA\***

SUMMARY: I. *Introduction*. II. *Revisiting Previous Litigation*. III. *The DMCA Safe Harbor and Litigation*. IV. *Proposed Actions*. V. *Conclusions*. VI. *Bibliography*.

\* Ph. D. Professor of Law, Tecnológico de Monterrey, Campus Monterrey. LL.B. 1997, UANL; LL.M. 1999, Tecnológico de Monterrey; LL.M. 2001, Tulane University; Ph.D. 2006, Tulane University.

Artículo recibido el 11 de abril de 2015  
Aprobado para publicación el 31 de agosto de 2015

**ABSTRACT:** U.S. copyright law is facing an interesting moment, where technology is far ahead of the law, and where the evolution of law seems to lead nowhere. This article focuses on recent technological evolution and subsequent legal developments, especially the safe harbor provisions for Internet service providers established by the Digital Millennium Copyright Act (DMCA) and its judicial interpretation. The main idea is to suggest a different direction on the evolution of U.S. copyright law. The proposal is based on a rather simple approach that would adapt copyright law to new technology. It is about redefining the red flag knowledge contained on the safe harbor provisions of the DMCA. In order to overcome opposition, the article suggests discontinuing the use of ineffective approaches.

**Key words:** DMCA, U.S. Copyright Litigation, Internet Service Providers Liability, ACTA, SOPA, PIPA.

**RESUMEN:** El presente artículo está enfocado en desarrollos tecnológicos recientes y la subsecuente evolución de los preceptos legales sobre derechos de autor o *copyrights* en el sistema jurídico norteamericano, específicamente en la limitante de responsabilidad de los proveedores de servicios de Internet, contenida en el denominado *Digital Millennium Copyright Act (DMCA)* y su interpretación judicial. La idea principal es proponer un cambio en la dirección en esta evolución. Es una propuesta basada en un enfoque sencillo consistente en redefinir las definiciones que la legislación prevé en el DMCA, respecto la responsabilidad de los proveedores de servicios de Internet. También se propone dejar de perseguir objetivos que en el pasado han probado ser ineficaces.

**Palabras clave:** DMCA, litigio derechos de autor en EEUU, responsabilidad proveedores de servicios de Internet en EEUU, ACTA, SOPA, PIPA.

**RÉSUMÉ:** Cet article se concentre sur les développements technologiques récents et l'évolution ultérieure des dispositions juridiques sur le droit d'auteur ou le Copyright dans le système judiciaire américain, en particulier la limitation de la responsabilité des fournisseurs de services Internet contenues dans la soi-disant *Digital Millennium Copyright Act (DMCA)* et son interprétation judiciaire. L'idée principale est de proposer un changement de direction dans cette évolution. Il est une proposition basée sur une approche simple de redéfinir les définitions prévues dans la loi DMCA, concernant la responsabilité des fournisseurs de services Internet. Il a également l'intention d'arrêter la poursuite d'objectifs dans le passé se sont avérées inefficaces.

**Mots-clés:** Droit d'auteur DMCA contentieux aux Etats-Unis, la responsabilité des fournisseurs de services Internet aux États-Unis, l'ACTA, SOPA, PIPA.

## I. INTRODUCTION

The present article is about U.S. Copyright Law. The relevance of this comparative study is the result of the global consequences Internet gives to many of the regulated activities here described. Also, this article may show the path that legislators of other jurisdictions may follow or, better avoid.

Copyright law was created as a result of a new technology, and has continued to evolve and adapt to each new invention. The starting point established by the creation of print set the recurrent path over years: any important new invention or technology results sooner or later in some sort of legal adaptation. That is copyright history. However, today copyright law is facing an interesting moment, where technology is far ahead of the law. Legal developments and technology affecting copyright law, and reactive strategies taken by a number of holders have led to an environment that does not protect copyrights effectively. On the contrary, simple measures are perceived as over-reactive. As a result, in some cases, copyright infringement is no longer perceived as a reprehensive behavior in society. Nevertheless, the original purpose of copyright law still matters: the encouragement of the learned men to produce useful works for society.

This article is focused on recent technological evolution and subsequent developments in copyright law, like the safe harbor provisions for Internet service providers established by the Digital Millennium Copyright Act (DMCA) and its judicial interpretation. These developments put copyrights in a difficult situation. The great number of protected works hosted without authorization in services like *Grooveshark* proves how difficult the problem has become. Those services are located not in a copyright heaven but in the U.S. and are offered by U.S.-based companies. Highly popular web service providers and highly unpopular measures taken by a number of copyright holders seem to lead to a dead end. The reaction of the copyright industry includes failed bills like the Stop Online Piracy Act (SOPA), or the Protect IP Act (PIPA). In the international arena, efforts included the unsuccessful proposal called Anti-counterfeiting Trade Agreement (ACTA).

The importance of copyrights is related to the production of new works. If there is not adequate protection of copyrights, there will be less production of new works in the future. A business model based on trespassing on

another's rights will result in weakening those rights. Therefore, the cost of such a business model will be the lack of new works

There is something wrong when copyright holders cannot make a case against huge Internet service providers, who have complacently blinded while hosting hundreds of thousands of infringing materials, but prevailing in cases condemning around one million dollars against individuals for having shared about a dozen of music files, without even understanding how.

I will revisit recent evolution in law related to such issues and suggest a direction for the evolution of copyright law. The proposal is based on a rather simple approach that would adapt copyright law to new technology. This approach is not based on actions like the SOPA, the PIPA, the ACTA, or even suing individuals to face statutory damages because such actions have created more problems than they have solved. In fact, similar actions should be avoided. The proposed approach is a legislative revision to clarify section 512 of the Copyright Act.

The first chapter presents important cases related to comparatively recent technological developments, starting with *Sony v. Universal City Studios, Inc.*,<sup>1</sup> and completing the saga with *Metro Goldwyn Mayer Studios v. Grokster*.<sup>2</sup> Those cases show how outcomes can be different when the legal issue is related to the scope of judiciary created doctrines, such as secondary liability or fair use. Then, the second chapter covers representative DMCA safe harbor litigation like *Viacom International v. YouTube*, and *UMG Recordings, Inc. v. Veoh Networks Inc.*<sup>3</sup> Finally, the third chapter identifies current problems, proceedings to avoid, and also proposes a change in the evolution of copyright law.

## II. REVISITING PREVIOUS LITIGATION

In this chapter I will revisit several copyright law developments caused by technological evolution, from video home recording to sharing mu-

<sup>1</sup> 464 U.S. 417 (1984).

<sup>2</sup> 545 U.S. 913 (2005).

<sup>3</sup> *Viacom International v. YouTube, Inc.* 676 F. 3d 19 (2nd Cir. 2012), *UMG Recordings, Inc. v. Veoh Networks Inc.* 667 F.3d 1022 (9th Cir. 2011).

sic files. As recognized, in the U.S. legal system, legal principles evolve through legislative process and also through litigation. Case law and *stare decisis* principles seem to respond to technological changes at an earlier stage. In some cases, technology developments are perceived as a response of a legal development, either judicial or legislative.<sup>4</sup> The starting point is the *Sony* case, a litigation occurring in the 80's, and subsequent litigation, that twenty years later concerned the very same legal argument, called contributory infringement. Other cases also cover vicarious infringement, a form of secondary liability not present in *Sony*. These cases were about defendants making available technology frequently used to infringe, or defendants inducing infraction.<sup>5</sup>

### 1. *Sony Corp. v. Universal City Studios, Inc.*<sup>6</sup>

The first case to mention is about the famous *Betamax* video tape recorder (VTR). Defendants were sued not for direct copyright infringement, but for contributory infringement. This is an important case because it was the first one in which the U.S. Supreme Court interpreted the U.S. Copyright Act of 1976,<sup>7</sup> particularly, the relation of statutory provisions with the judicially created doctrine of contributory infringement. This decision also briefly discussed vicarious liability, even though defendants were not sued for it. The case was initially filed in the Central District Court of California, for the infringement committed by "some individuals," using the VTR manufactured and marketed by the defendants.<sup>8</sup> The District Court denied any relief, holding that the defendants were not liable for copies made by their consumers such as homemade recording for time shifting purposes,

<sup>4</sup> See Liebowitz, Stan, "MP3s and Copyright Collectives: A Cure Worse than the Disease?", in Takeyama, Lisa N. *et al.*, *Developments in the Economics of Copyright*, Cheltenham, Edward Elgar Publishing Limited, 2005, p. 37.

<sup>5</sup> See Ginsburg, Jane C., "Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs", *Arizona Law Review*, vol. 50, 2008, pp. 577, 582, 583.

<sup>6</sup> 464 U.S. 417 (1984).

<sup>7</sup> See Menell, Peter S. and Nimmer, David, "Unwinding Sony", *California Law Review*, vol. 95, 2007, p. 941.

<sup>8</sup> See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 420 (1984).

because it considered such recording a fair use.<sup>9</sup> It also introduced into the copyrights field the patent doctrine called “staple article”.<sup>10</sup> None of the consumers allegedly committing the direct infringement were sued.

The Supreme Court granted certiorari in order to review the decision in which the Court of Appeals for the Ninth Circuit reversed the previously mentioned District Court judgment. The Supreme Court set aside the Ninth Circuit conclusions, reaffirming the original District Court decision.<sup>11</sup> After stating the facts of the case, and both decisions below, the Supreme Court proceeded to describe copyrights from constitutional basis to statutory definitions, remedies and the fair use defense contained in section 107 of the Copyright Act.<sup>12</sup> The Supreme Court also stated that: “[f]rom its beginning, the law of copyright has developed in response to significant changes in technology”.<sup>13</sup>

Noting that contributory infringement is not expressly provided by the Copyright Act as it is in the Patent Act, the Supreme Court recognized that in spite of the differences between patents and copyrights, the application of this doctrine is adequate for the copyright area in order to protect the monopoly granted by Congress to authors.<sup>14</sup> Then it upheld the application of the patent doctrine staple article to copyrights in order to balance holders’ rights and the right of others to engage in commerce.<sup>15</sup> Recognizing that unauthorized “time shifting” recording is a fair use;<sup>16</sup> the Supreme Court concluded that since the VTR is “capable of substantial non-infringing uses,” the marketing of such product is not copyright contributory infringement.<sup>17</sup>

Therefore, the manufacturer of a device that can be used by users to infringe copyrights, but also capable of substantial non infringing uses, like

<sup>9</sup> See *ibidem*, pp. 425, 455.

<sup>10</sup> See *ibidem*, p. 426. See also Menell, Peter S. and Nimmer, David, *op. cit.*, p. 951, for an explanation of how the “staple article doctrine” present in the Patent Act was introduced into the copyright field without paying too much attention to legislative history or the structure of both statutes.

<sup>11</sup> See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 420, 421 (1984).

<sup>12</sup> See *ibidem*, pp. 421- 435.

<sup>13</sup> *Ibidem*, p. 430.

<sup>14</sup> See *ibidem*, pp. 434, 442.

<sup>15</sup> See *idem*.

<sup>16</sup> See *ibidem*, p. 455.

<sup>17</sup> See *ibidem*, p. 456.

time shifting is not liable for copyright contributory infringement. The next case, twenty years later, exemplifies how *Sony* was argued and interpreted later with different technology, players, and circumstances, thus obtaining a different result. However, the case relates to the same principles; the only change is the vehicle, from atoms to bits.<sup>18</sup>

## 2. *A & M Records, Inc. v. Napster, Inc.*<sup>19</sup>

The enabling device developed by the defendant in this case was a system to share *MP3* music files among users.<sup>20</sup> This system operated through a process called *peer to peer*, in which different users acquired a computer program called *MusicShare* from the Napster Internet homepage.<sup>21</sup> After installing the software on his or her personal computer, a user would be able to store *MP3* music files in a special folder located on the hard drive of his or her computer.<sup>22</sup> Then, by accessing the defendant's system using the *MusicShare* software, the user could make those files available to other users by listing them in a directory hosted by the defendant.<sup>23</sup> The defendant hosted no specific music files, but only the directory containing users' music files; and when a particular user looked for a specific song, which happened to be on another user's computer, the system would redirect to it.<sup>24</sup> Therefore, the transmission and copying of music files occurred between users' computers. This *peer to peer* system allowed users to share their music files and search for more music files on other users' computers.

Napster did not infringe music rights directly, but contributed to infringement by providing the means by which its users would directly infringe music copyright. This action was based on the doctrine of contributory in-

<sup>18</sup> See Nimmer, David, "Brains and other Paraphernalia of the Digital Age", *Harvard Journal of Law & Technology*, vol. 10, 1996, pp. 1, 7.

<sup>19</sup> 239 F.3d 1004 (9th Cir. 2001).

<sup>20</sup> The format was originally called MPEG-3 in reference to its creators: "Moving Pictures Experts Group." See *ibid*, p. 1010. This format allows music to be stored in less space than the traditional "audio CD" format called WAV. See *idem*.

<sup>21</sup> See *ibidem*, p. 1011.

<sup>22</sup> See *idem*.

<sup>23</sup> See *idem*.

<sup>24</sup> See *ibidem*, p. 1012.

fringement just like *Sony*, the previously mentioned case. The Ninth Circuit first analyzed the infringement made by Napster users, including fair use defenses those users may have, and then it analyzed Napster's secondary liability under the doctrine of contributory infringement.

As recognized by this decision, in order to prevail in a copyright infringement action, the plaintiff must prove ownership of a valid copyright, and also prove the infringement of at least one of the exclusive rights contained in section 106 of the Copyright Act.<sup>25</sup> In this case, the plaintiffs demonstrated copyright ownership of over 70% of the files available on the system. They also proved that over eighty seven percent of the files were copyright protected songs.<sup>26</sup> Moreover, the Ninth Circuit recognized that two exclusive rights contained in section 106 of the Copyright Act were infringed: reproduction and distribution right.<sup>27</sup> Users who uploaded the music files names to the index violated the distribution right, and users who downloaded the files violated the reproduction right.<sup>28</sup>

Then, the decision went on the analysis of the fair use defense alleged by Napster. As any copyright contributory or vicarious infringement action, such a defense was in relation to the direct infringement committed by users.<sup>29</sup> The fair use defense, enacted in section 107 of the Copyright Act,<sup>30</sup> enumerates four factors to consider: 1) the purpose, whether commercial or not; 2) the nature of the work, referring to the originality of the work; 3) the amount taken in relation to the entire work; and 4) the effect upon the market, a factor strongly related to the first one. The doctrine was developed by series of nineteenth-century cases. According to legislative history of the Copyright Act of 1976, the codification of these four factors was meant to endorse those judicial developments, with no intention to freeze them, but allow them to evolve: "there is no disposition to freeze the

<sup>25</sup> See *ibidem*, p. 1013.

<sup>26</sup> See *ibidem*, p. 1014.

<sup>27</sup> See *idem*.

<sup>28</sup> See *idem*.

<sup>29</sup> For an analysis of the appropriateness or inaptness of such a defense in the digital era in relation to private uses see Litman, Jessica, "Lawful Personal Use", *Texas Law Review*, vol. 85, 2007, p. 1871.

<sup>30</sup> 17 U.S.C. § 107.

doctrine in the statute, especially during a period of rapid technological change”.<sup>31</sup> Thus, courts have great deference in considering these factors.

According to the Ninth Circuit, the fair use first factor weighed against Napster users because the “repeated and exploitative unauthorized copies of copyrighted works were made to save the expense of purchasing authorized copies”.<sup>32</sup> This interpretation was a departure from the traditional meaning of commercial use, in which individuals receive money in exchange for something that in this case would be the unauthorized distribution or reproduction. This has been considered as an unjustified expansion of the meaning of “commercial,” thus turning otherwise private non-commercial uses into commercial ones, when the individual committed the unauthorized action in order to avoid paying for the original material.<sup>33</sup> However, even if users of Napster did not receive money for their infringing actions, the alleged private non-commercial use is quite different than traditional private uses, like the *Sony* time shifting, because it involves pervasive distribution of files in an environment outside the privacy of a household.

In relation to the second factor, the original and creative character of the work, in this case songs, the balance weighted against the infringers because the works were “closer to the core of intended copyright protection”,<sup>34</sup> which means originality. Since the works were copied entirely, the third factor also weighed against the infringers. As for the fourth factor, the Ninth Circuit upheld the District Court findings that the infringing activities harmed the market of those protected music songs in two different ways: reducing the sale of original CDs among young college students, and precluding the entrance of plaintiffs into the online digital market.<sup>35</sup>

After analyzing and rejecting the fair use defense, the Ninth Circuit went on to analyze Napster contributory infringement. It quoted a defi-

<sup>31</sup> H. R. Rep. No. 94-1476, at 66. For a discussion of the appropriateness of those fair use factors, technology and balancing between copyright and public benefit, see Lunney, Jr., Glynn S., “Fair Use and Market Failure: Sony Revisited”, *Boston University Law Review*, vol. 82, 2002, p. 975.

<sup>32</sup> *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1015 (9th Cir. 2001).

<sup>33</sup> See Litman, Jessica, *op. cit.*, note 29, pp. 1913, 1914.

<sup>34</sup> *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1016 (9th Cir. 2001).

<sup>35</sup> See *idem*.

dition from the Second Circuit,<sup>36</sup> establishing that “one who with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‘contributory’ infringer”.<sup>37</sup> According to this accepted definition, the first element of contributory infringement is the knowledge of the infringing activity. The Ninth Circuit upheld the District Court findings that Napster had actual and constructive knowledge of “specific acts of infringement”.<sup>38</sup> In order to held actual knowledge of infringement, the District Court relied on the following circumstances: one of the cofounders accepted in a document that they should ignore real identities and IP addresses of users because “they are exchanging pirated music”;<sup>39</sup> evidence of 12,000 infringing files still available at that time; and some Napster executives had experience in the music industry even enforcing copyrights; furthermore, those executives had downloaded music files by themselves, and had promoted the site listing infringing music files.<sup>40</sup>

Having upheld District Court findings about actual knowledge, the Ninth Circuit established that the alleged defense of Napster based on the *Sony* staple article doctrine for potential non infringing uses of its system was inapplicable to Napster.<sup>41</sup> This was because of the previously mentioned knowledge that Napster had of particular acts of infringement. According to the Ninth Circuit, in *Sony* the limited knowledge of the defendant about infractions was relevant to limiting the liability based on the possibility of substantial non infringing uses.<sup>42</sup> Therefore, *Sony* was distinguished because of the actual knowledge of the defendant in this case.

Napster was also held liable for vicarious infringement. The Ninth Circuit acknowledged that Sony’s staple article doctrine was inapplicable to vicarious infringement liability.<sup>43</sup> The two elements needed for the application of this doctrine were explained as “the right and ability to supervise the

<sup>36</sup> See *Gershwin Publ’g Corp v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2nd Cir. 1971). This case was also cited by the Supreme Court in *Sony*.

<sup>37</sup> *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1016 (9th Cir. 2001).

<sup>38</sup> See *ibidem*, p. 1020.

<sup>39</sup> *Idem*.

<sup>40</sup> See *idem*.

<sup>41</sup> See *idem*.

<sup>42</sup> See *idem*.

<sup>43</sup> See *ibidem*, p. 1022.

infringing activity and also... a direct financial interest in such activities”.<sup>44</sup> In this instance, Napster fulfilled both elements, because the infringing materials attracted more users, and more users would increase the defendant’s future revenues. As for the second element, it was determined that Napster had “the right and ability to police its system”, and failed to do so.<sup>45</sup>

During the same litigation, the District Court held that Napster was not covered by any of the limitations of liability for Internet service providers established by the DMCA.<sup>46</sup> According to the District Court, the statute requires that information be “transmitted or routed through the Napster system,” in order to fit the statutory definition of service provider.<sup>47</sup> In this case the information was transmitted through users’ computers, beyond Napster’s system.

### 3. *Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd*<sup>48</sup>

*Metro-Goldwyn Mayer Studios, Inc. v. Grokster, Ltd* is the next case in the legal and technological evolution described in this article. The *peer to peer* technology here did not need any central server containing a directory like Napster’s technology did. Each of the defendants, Gorkster, Ltd. and StreamCast Networks, Inc, developed its own *peer to peer* software in order to share files. Users only needed to access the webpage of one of the defendants in order to obtain the chosen software. Grokster’s software employed a technology called *FastTrack*, and StreamCast a technology called *Guntella*, and each software was compatible with the others.<sup>49</sup> Without a central server, the system was still capable of enabling users to upload music files and make them available to other users using the same or compatible software.<sup>50</sup>

<sup>44</sup> *Idem.* quoting *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996), and *Gershwin Publ’g Corp. v. Columbia Artists Mgmt., Inc.* 443 F.2d 1159, 1162 (2nd Cir. 1971).

<sup>45</sup> *See ibidem*, p. 1023.

<sup>46</sup> *See* 17 U.S.C. §512.

<sup>47</sup> *See* *A & M Records, Inc. v. Napster* 2000 U.S. Dist. LEXIS 6243, 1, 13 (2000).

<sup>48</sup> *See* 545 U.S. 913 (2005).

<sup>49</sup> *See ibidem*, p. 921.

<sup>50</sup> *See idem.* The Supreme Court noted several characteristic features of this peer-to-peer system. *See ibidem*, p. 920.

The District Court held that the defendants were not liable for direct infringement, because the music files were transmitted directly by the users.<sup>51</sup> The defendants were also not liable for contributory infringement because the system did “not provide [them] with actual knowledge of specific acts of infringement”.<sup>52</sup> The Ninth Circuit affirmed, holding that defendants were not liable for contributory infringement if the product they distribute is capable of substantial non infringing uses, as long as they have no knowledge of specific infringements.<sup>53</sup> This decision was based on the Ninth Circuit interpretation of *Sony v. Universal City Studios*.<sup>54</sup> Since the system was decentralized, defendants lacked the required actual knowledge of particular infringements that would have been possible within a central directory. The Supreme Court granted certiorari and reversed.<sup>55</sup>

The record of the case showed that 90% of the files available in the system were protected copyright works.<sup>56</sup> More than a 100 million copies of the software were downloaded and “billions” of music files were shared each month; according to the Supreme Court those numbers represented a “staggering” copyright infringement.<sup>57</sup> There was also evidence that defendants encouraged infringement and distributed their free software with the announced purpose of downloading copyrighted works.<sup>58</sup> The business model of both defendants was to attract users, usually those of Napster, and provide them with software, free of charge, for downloading copyrighted music songs. The revenue was to come from advertising; the more users, the greater revenue from advertising.<sup>59</sup>

According to the Supreme Court, the Ninth Circuit misapplied *Sony*, because it “has read Sony’s limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties’ infringing use of it... even when actual purpose to cause infringing use is shown... unless the distributors had ‘spe-

<sup>51</sup> See *ibidem*, p. 927.

<sup>52</sup> *Idem*.

<sup>53</sup> See *ibidem*.

<sup>54</sup> See *idem*. See also *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

<sup>55</sup> See *Metro-Goldwyn Mayer Studios Inc. v. Grokster, Ltd* 545 U.S. 913, 928 (2005).

<sup>56</sup> See *ibidem*, p. 923.

<sup>57</sup> See *idem*.

<sup>58</sup> See *ibidem*, p. 924.

<sup>59</sup> See *ibidem*, p. 926.

cific knowledge of infringement...”.<sup>60</sup> For the Supreme Court, *Sony* did not displace the intention on secondary liability cases, so evidence on the purpose of causing infringement should not be ignored.<sup>61</sup> Defendants had alleged potential non infringing uses such as new performers trying to gain new audiences by distributing freely their songs in *peer to peer* networks, or even the distribution of unprotected works like Shakespeare.<sup>62</sup> However, the Supreme Court distinguished *Sony* from the present case because in *Sony* there was no evidence of intentional inducement of infringement;<sup>63</sup> while in this case, the record was “replete” with such evidence and the unlawful objective to cause infringement was “unmistakable.”<sup>64</sup>

### III. THE DMCA SAFE HARBOR AND LITIGATION

#### 1. *DMCA, the nineties and the Web 2.0*

*Viacom International, Inc. v. YouTube, Inc.*<sup>65</sup> is different than the above mentioned cases. The legal discussion here was about a statutory limitation of liability having different origins than the previously analyzed doctrines, such as fair use defense, or the doctrines of contributory and vicarious infringement, coming from judicial developments.<sup>66</sup> Therefore, in *YouTube* the legal

<sup>60</sup> *Ibidem*, p. 934.

<sup>61</sup> *See idem*.

<sup>62</sup> *See ibidem*, p. 923.

<sup>63</sup> *See ibidem*, p. 937.

<sup>64</sup> *See ibidem*, pp. 937, 940.

<sup>65</sup> *See* 676 F.3d 19 (2nd Cir. 2012).

<sup>66</sup> *See* Imfeld, Cassandra and Smith Ekstrand, Victoria, “The Music Industry and the Legislative Development of the Digital Millennium Copyright Act’s Online Service Provider Provision”, *Communication Law & Policy*, vol. 10, 2005, p. 291, discussing and analyzing legislative process, debate, negotiations and even case law arisen prior DMCA enactment. This process was contrary to the enactment of the fair use defense on §107 of the Copyright Act, which aimed to recognize judicial evolution and let it evolve. Doctrines of contributory and vicarious infringement are not even present in the Copyright Act. *See* Lunney, Jr, Glynn S., *op. cit.*, p. 997, noting that the fair use doctrine was originally developed at the beginnings of the nineteenth century. *See also* *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 430, 434, 442 (1984).

analysis was limited to statutory interpretation, regardless of the purpose of the service or even if infringement was pervasive. Since this liability limitation came from the statute itself, courts have focused on the statutory interpretation. The factual context is also different, because the underlying facts occurred in what has been called “Web 2.0”, which implies Internet services focused on users and interactivity, and abundant “user generated content”, referring to materials uploaded by users.<sup>67</sup> Another important feature of Web 2.0 is that technical capacities are higher than those of the nineties when the statutory limitation of liability was enacted.<sup>68</sup>

Internet service providers have different kinds of services and activities including, among others, hosting, Internet access, caching and searching. It is also common for providers to receive and send packets of digital information not directed to their own consumers. Most of these activities are part of automated processes requiring no human intervention, and occurring in seconds. All this information may include protected works, transmitted or made available without proper authorization.<sup>69</sup> Therefore, Internet service providers are potentially exposed to liability for either direct copyright infringement, or contributory and vicarious infringement. Section 512 of the Copyright Act contains limitations of liability for different kinds of Internet service providers’ activities.<sup>70</sup> The case is about the scope of this provision, especially paragraph (c), designed to limit liability of providers for hosting activities.<sup>71</sup>

<sup>67</sup> See Robins, Martin B., “A Good Idea at the Time: Recent Digital Millennium Copyright Act §512(c) Safe Harbor Jurisprudence Analysis and Critique of Current Applications and Implications”, *Tulane Journal of Technology & Intellectual Property*, vol. 2012, p. 1, 4. SEE ALSO ARSHAM, BRYAN E., “Monetizing Infringement: A New Legal Regime for Host of User-Generated Content”, *Georgetown Law Journal*, VOL. 101, 2013, P. 778. For discussion about origins and definitions of the term Web 2.0 see Murley, Diane, “What is all the Fuss about Library 2.0?”, *Law Library Journal*, vol. 100, 2008, p. 197.

<sup>68</sup> See Monseau, Susanna, “Fostering Web 2.0 Innovation: The Role of the Judicial Interpretation of the DMCA Safe Harbor, Secondary Liability and Fair Use”, *John Marshall Intellectual Property Law Review*, vol. 12, 2012, pp. 69, 84.

<sup>69</sup> See Steerling, J. A. L., *World Copyright Law*, 2nd. ed., London, Sweet & Maxwell, 2003, §13.42

<sup>70</sup> See 17 U.S.C. §512

<sup>71</sup> It reads as follows: “[...] [a] service provider shall not be liable for monetary relief... for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the

Copyright holders played an active role and influence in DMCA legislative process, achieving advantageous provisions for themselves, like the subpoena judicial power under section 512(h), which has been considered an important tool in *peer to peer* cases.<sup>72</sup> The legislative process also included other actors like Internet service providers and was intended to balance Internet innovation and copyright protection.<sup>73</sup> The detailed and lengthy prose of the entire section 512 resulted from these lobbying efforts; the final provision was 10 times longer than the original draft.<sup>74</sup>

Nevertheless, years have passed and section 512 has proven to be uncertain and problematic at the least. While, section 512 safe harbor provisions have been criticized as lacking to provide certainty to Internet service providers,<sup>75</sup> courts have interpreted them broadly, putting the burden to search for infringing materials on copyright holders.<sup>76</sup> It has been noted that “take-down” provisions included on section 512 do not bind to “stay-down”, representing double efforts to copyright holders which have to send take down notices several times.<sup>77</sup>

service provider— (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing...”, 17 U.S.C. §512(c).

<sup>72</sup> See Imfeld, Cassandra and Smith Ekstrand, Victoria, *op. cit.*, p. 310.

<sup>73</sup> See Katyal, Sonia K. and Schultz, Jason M., “The Unending Search for the Optimal Infringement Filter,” *Columbia Law Review Sidebar*, vol. 112, 2012, pp. 83, 85.

<sup>74</sup> See Imfeld, Cassandra and Smith Ekstrand, Victoria, *op. cit.* pp. 310 and 311.

<sup>75</sup> See Helman, Lital and Parchomovsky, Gideon, “The Best Available Technology Standard”, *Columbia Law Review*, vol. 111, 2011, pp. 1194, 1200. See also Castree, III, Sam, “Cyber-Plagiarism for Sale!: The Growing Problem of Blatant Copyright Infringement in Online Digital Media Stores”, *Texas Review of Entertainment & Sports Law*, vol. 14, 2012, p. 25, 44.

<sup>76</sup> See Helman, Lital and Parchomovsky, Gideon, *op. cit.*, p. 1214; See also Castree, III; Sam, *op. cit.*, p. 29.

<sup>77</sup> See *ibidem*, p. 1204.

## 2. *Viacom International, Inc. v. YouTube, Inc*

In the present case, several copyright holders, among them Viacom International Inc. and the Football Association Premier League Ltd. sued YouTube, Inc., YouTube LLC., and Google, Inc. for direct and secondary copyright infringement.<sup>78</sup> The alleged infringed exclusive rights were public performance, display and reproduction of about 79,000 audiovisual works appearing on the YouTube webpage.<sup>79</sup> The District Court favored YouTube and plaintiffs appealed.

The legal issue in front of the Court of Appeals for the Second Circuit was whether section 512(c) requires “actual knowledge” or “awareness” of “specific and identifiable infringements”.<sup>80</sup> There were two possible interpretations. The first one, considers that in order to be covered by the safe harbor provision, the Internet service provider should not have any “general awareness that there are infringements”,<sup>81</sup> which were evident in this case. Under this interpretation, a general knowledge of infringing materials would put the service provider out of the safe harbor. This interpretation is based on what it is known as “red flag” knowledge. For the second interpretation, the safe harbor provision prevails unless the service provider has “actual or constructive knowledge of specific and identifiable”,<sup>82</sup> infringing material. Under this interpretation the only way to get this knowledge is through the notification made by the copyright holder to the Internet service provider’s designated agent.<sup>83</sup> In this case, failing to remove such material would make the limitation of liability inapplicable. According to this interpretation, YouTube could be aware of hundreds or even thousands of infringing materials; and would not need to remove any video until receiving a specific notification for each infringing video.

The District Court read section 512 according to the second interpretation, meaning that in order to lose safe harbor, there should be knowledge of specific infringing material; it held that general awareness of infringing

<sup>78</sup> See *Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19, 20 (2nd Cir. 2012).

<sup>79</sup> See *ibidem*, pp. 28, 26.

<sup>80</sup> See *idem*, p. 30.

<sup>81</sup> See *Viacom International, Inc. v. YouTube, Inc.* 718 F. Supp. 2d 514, 519 (S.D.N.Y. 2010).

<sup>82</sup> See *idem*.

<sup>83</sup> See *idem*.

videos was not enough.<sup>84</sup> According to the District Court, the service provider would not even have to make any kind of search to look for evidently infringing videos.<sup>85</sup> The resolution analyzed legislative history and case law, concluding that “[g]eneral knowledge that infringement is ‘ubiquitous’ does not impose a duty on the service provider to monitor or search its service for infringements.”<sup>86</sup>

In addition, the District Court interpreted the notification elements of section 512(c)(3), as requiring not only the name of the work, but also the exact uniform resource locator (URL) of each alleged infringing video.<sup>87</sup> This holding is different than previous case law and other circuits’ interpretation, making the notification mechanism more difficult for copyright holders.<sup>88</sup> A reading criticized as a rewriting of section 512(c)(3)(iii), because the statute literally only establishes that information only should be: “...reasonably sufficient to permit the service provider to locate the material”.<sup>89</sup> A resulting aspect of this holding is that a single notification of X work, posted several times, is no longer enough; now copyright holders have to make a new notification for every single uploaded video. So, if there are 300 videos of the very same work, there should be 300 notifications.

The Court of Appeals for the Second Circuit affirmed in part and modified in part the District Court’s decision.<sup>90</sup> It remanded the case to the District Court to determine several questions. Two important issues to determine on remand were: “...whether... YouTube had knowledge or awareness of any specific infringements...; whether... YouTube willfully blinded

<sup>84</sup> See *ibidem*, p. 523.

<sup>85</sup> See *ibidem*, p. 522. See also Xu, Jing, “DMCA Safe Harbors and the Future of New Digital Music Sharing Platforms”, *Duke Law & Technology Review*, 2012, pp. 45, 155.

<sup>86</sup> *Ibidem*, p. 525.

<sup>87</sup> See *ibid*, pp. 528, 529.

<sup>88</sup> See Schachter, Jeremy A., “Substantially Perfect: The Southern District of New York’s Problematic Rewrite of the DMCA’s Elements of Notification”, *Cardozo Arts & Entertainment Law Journal*, vol. 29, 2011, pp. 495, 505-515.

<sup>89</sup> 17. U.S.C. §512(c)(3)(iii). See also *ibid*. pp. 495, 503. The note analyzes this aspect of the present judgment. It starts with a very interesting analogy: “[i]maging you enter a taxi in New York City and instruct the driver to take you to Great Restaurant on forty-ninth Street and Seventh Avenue. The driver says he cannot take you anywhere unless you provide him with the exact street address of your desired destination.” *Ibid*. p. 495.

<sup>90</sup> See *Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19, 25 (2nd. Cir. 2012).

itself to specific infringements...”<sup>91</sup> However, the Second Circuit affirmed the most important part of the District Court decision, the part that stated that the knowledge or awareness should be of “specific and identifiable instances of infringement...”<sup>92</sup> This is the second interpretation of section 512 explained above. In the resolution, the Second Circuit also noted from the record several e-mails and certain reports made by defendants showing at least general awareness of infringing materials.<sup>93</sup> Therefore, the Second Circuit considered that it was premature for the District Court to grant the summary judgment favoring the defendants.<sup>94</sup> Based on the evidence of general awareness found on the record, it held that it could be possible for plaintiffs to demonstrate that YouTube was aware of specific infringements.<sup>95</sup> This may be considered a winning outcome for Internet service providers because it did not substantially modify the District Court’s decision, but only avoided to precipitate it. However, others think this played against Internet service providers.<sup>96</sup> Contrary to the District Court’s view in which the only way to have knowledge or awareness of infringement is by receiving the notification of copyright holders,<sup>97</sup> for the Court of Appeals the e-mails and reports could probe such knowledge, leaving the service provider outside the safe harbor.

<sup>91</sup> *Ibidem*, pp. 59, 60.

<sup>92</sup> *See ibidem*, p. 58.

<sup>93</sup> *See ibidem*, pp. 33, 34. The Second Circuit quoted a report prepared by one of the YouTube founders: “[a]s of today[,] episodes and clips of the following well-known shows can still be found...: Family Guy, South Park, MTV Cribs, Daily show... although YouTube is not legally required to monitor content... we would benefit from preemptively removing content that is blatantly illegal...”, *ibid.* p. 33. Another example discussed was a survey conducted by defendants showing that about 75 to 80 percent of the materials were copyrighted, and also a Credit Suisse report acting showing that 60% of the uploaded videos were copyrighted materials and only 10% of those videos were authorized. *See ibidem*, p. 33. The record also showed e-mails among YouTube founders discussing if they should remove infringing materials. *See idem*.

<sup>94</sup> *See ibidem*, p. 34.

<sup>95</sup> *See ibidem*, pp. 35, 36.

<sup>96</sup> *See* Arsham, Bryan E., *op. cit.*, p. 778. *See also* Drath, Ross, “Hotfile, Megaupload, and the Future of Copyright on the Internet: What Can Cyberlockers Tell Us about DMCA Reform”, *John Marshall Review of Intellectual Property Law*, vol. 12, 2012, pp. 204, 229.

<sup>97</sup> *See* Hassanabadi, Amir, “Viacom v. YouTube –All Eyes Blind: The Limits of the DMCA in a Web 2.0 World,” *Berkeley Technology Law Journal*, vol. 26, 2011, pp. 405, 437.

According to section 512(c), the limitation on liability is applicable if the service provider has no knowledge or awareness of infringing activities or materials. However, section 512(m)(1) establishes that the service provider is not conditioned to monitor contents to seek for infringing activities.<sup>98</sup> As a result, there is an unclear line between not having actual knowledge of infringing activities, and not being conditioned to search for infringing contents in order to be covered by the limitation of liability. No matter which interpretation prevails, the one in which the District Court established that the only way to have this knowledge is through the notification, or that of the of the Court of Appeals, who opened the door to other circumstances like those shown on the record; it is very difficult for plaintiffs to prove such knowledge unless they have made a notification for each infringing content, and such material has not been removed by the service provider.<sup>99</sup>

The resulting problem is that an Internet service provider may have knowledge of pervasive infringement over its service, and simply choose to turn a blind eye. Or it may even design its business model based on infringement, promoting infringement and yet be covered by the safe harbor because it has no obligation to monitor contents. The Second Circuit held that section 512(m)(1) did not abrogate the common law principle called “willful blindness,” which it defines as: “[a] person is «willfully blind» or engages in «conscious avoidance»... where the person «was aware of a high probability of the fact in dispute and consciously avoided confirming that fact»”.<sup>100</sup> Applying this doctrine to section 512, a defendant could be liable if it can be shown that it willfully blinded itself from infringing activity. However, the Second Circuit held that this doctrine could only be applied to “specific instances of infringement under the DMCA”.<sup>101</sup> While the doctrine could be applied to section 512, the requirement of specific acts of infringement would kept immune to those generally blind, and even to

<sup>98</sup> See Castree, III, Sam *op. cit.*, p. 29.

<sup>99</sup> See *idem*.

<sup>100</sup> See *Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2nd Cir. 2012). Citation omitted.

<sup>101</sup> See *ibidem*, p. 35. See also Recent Case, “Copyright Law Willful Blindness –Second Circuit Holds that Willful Blindness is Knowledge in Digital Millennium Copyright Act Safe Harbor Provision.—*Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2nd. Cir. 2012)”, *Harvard Law Review*, vol. 126, 2012, pp. 645, 647-649.

those who design business models at the expense of copyright holders. The whole litigation process seems to lead to a strict requirement of specificity: Internet service providers are immune until they receive notification of each infringing material which they would have to remove to keep themselves immune, or when they are aware of specific acts of infringement.

A determination from the District Court on remand about YouTube's actual knowledge of specific infringements, based on the evidence on the record, would be a significant precedent for future cases. However, before the District Court rendered the new resolution on remand, the parties settled the dispute and made the following joint statement: "This settlement reflects the growing collaborative dialogue between our two companies on important opportunities, and we look forward to working more closely together".<sup>102</sup>

This litigation shows two opposite arguments. The first one is that copyright holders were trying to win what they have already lost in Congress,<sup>103</sup> or the fact that by reading out the red flag knowledge from section 512, courts have misinterpreted the statute and its legislative history.<sup>104</sup> As mentioned before, the statute establishes two different ways to obtain knowledge that, without acting upon it, would result in the loss of the safe harbor protection.<sup>105</sup> However, courts have ignored the second way to get that knowledge, the red flag knowledge. In this regard, legislative history reveals that even if the statute does not bind service providers to monitor contents, "if the service provider becomes aware of a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it

<sup>102</sup> Rabil, Sara, "Google, Viacom Settle YouTube Copyright Suit, Terms Not Disclosed," *BNA World Intellectual Property Report*, vol. 28, 2014, p. 24.

<sup>103</sup> See Reichman, Jerome H. *et al.*, "A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works", *Berkeley Technology Law Journal*, vol. 22, 2007, pp. 981, 994.

<sup>104</sup> See Chang, Liliana, "The Red Flag Test for Apparent Knowledge Under the DMCA §512(c) Safe Harbor," *Cardozo Arts & Entertainment Law Journal*, vol. 28, 2010, pp. 195, 203.

<sup>105</sup> See Sirichit, Methaya, "Catching the Conscience: An Analysis of the Knowledge Theory Under §512(C)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags," *Albany Law Journal of Science and Technology*, vol. 23, 2013, pp. 85, 129. EVEN THOUGH THE PURPOSE OF THIS ARTICLE IS TO SHOW THAT COURTS HAVE FOUND APPARENT RED FLAG KNOWLEDGE IN A SERIES OF CASES, THE ARTICLE RECOGNIZES "JUDICIAL RELUCTANCE" IN FIND RED FLAG KNOWLEDGE. SEE *IBIDEM*, P. 142. THE DISTRICT COURT DECISION ON THE ABOVE CASE VIACOM INTERNATIONAL, INC. V. YOUTUBE, INC, IS AN EXAMPLE OF THIS RELUCTANCE.

takes no action...”.<sup>106</sup> In order to determine this red flag knowledge, the legislative history mentions a test containing a subjective standard and also an objective standard.<sup>107</sup> Nonetheless, courts have been reluctant to hold knowledge besides the take-down notification of section 512(c)(1)(A)(i), and by doing so, they have disregarded section 512(c)(1)(A)(ii) from the statute.<sup>108</sup> Hence, the willful blindness discussion of the Second Circuit was a departure of this prevailing interpretation that eliminates red flag knowledge from the statute.<sup>109</sup>

### 3. *UMG Recordings, Inc. Veoh Networks Inc.*<sup>110</sup>

This Ninth Circuit case is very similar to *Viacom International, Inc. v. YouTube, Inc.* Defendant Veoh Networks, Inc. had a service allowing individuals to share video materials over the Internet. UMG Recordings, Inc. and others filed suit against Veoh for direct infringement, vicarious infringement, and contributory infringement.<sup>111</sup> The District Court held that Veoh was covered by the DMCA safe harbor and the Ninth Circuit affirmed.

UMG argued that Veoh’s service was outside of the statutory meaning of “by reason of the storage at the direction of the user..” contained on section 512(c)(1) because the service took the videos and made them available to the public through an automated process.<sup>112</sup> During this automated process, some software changed the format of submitted videos in order to make them accessible to other users.<sup>113</sup> Therefore, under UMG’s argument, this automated process was outside the term “storage” required by the statute. However, the Ninth Circuit disagreed and established that the automated process was only intended to convert the video format in order to make it available to users, and that Veoh did not select, preview, upload, or supervise the file uploading.<sup>114</sup>

<sup>106</sup> S. Rep. No. 105-190, at 44 (1998) [hereinafter DMCA S. Rep.]

<sup>107</sup> See *idem*.

<sup>108</sup> See Drath, Ross, *op. cit.*, p. 228.

<sup>109</sup> See *idem*.

<sup>110</sup> 667 F.3d 1022 (9th Cir. 2011).

<sup>111</sup> See *ibidem*, p. 1029.

<sup>112</sup> See *ibidem*, p. 1031.

<sup>113</sup> See *ibidem*, p. 1035.

<sup>114</sup> See *ibidem*, p. 1031.

Regarding the knowledge that would be required to take action under section 512, the Ninth Circuit focused on the red flag knowledge. This was because UMG did not dispute that Veoh had removed videos upon receiving the DMCA notification contained in §512.<sup>115</sup> The Court noticed that UMG had not notified Veoh of any infringing video in accordance to 512(c)(1)(A)(i). On the contrary, UMG argued that Veoh “must have known... content was unauthorized, given its general knowledge”.<sup>116</sup> However, the Court held that hosting copyrighted materials with general knowledge that the service could be used for infringement does not meet the knowledge requirement of § 512(c)(1)(A)(i), nor the one required by § 512(c)(1)(A)(ii).<sup>117</sup>

The Ninth Circuit established that Congress put the red flag burden to determine infringing materials on the copyright holders and not on the service providers. The Court based this reasoning on §512(m), which establishes that “[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on...a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.” The court also relied on its own case law, specifically *Perfect 10, Inc. v. CCBill LLC*,<sup>118</sup> a case in which domain names like “illegal.net”, and “stolence-lebritypics.com”, were not considered red flag knowledge by the Ninth Circuit.<sup>119</sup> Therefore, the Court held that the alleged general knowledge was not enough to constitute a red flag.<sup>120</sup>

As evidence of red flag knowledge, UMG presented several press articles establishing that Veoh hosted infringing materials. There was also testimony from the Veoh CEO, acknowledging that he had heard about those articles and admitted that “from time to time,” there were infringing contents on the service.<sup>121</sup> However, the Ninth Circuit held that this evidence was insufficient to demonstrate red flag knowledge. The Court noted that “the notice and takedown procedures would make little sense”,<sup>122</sup> if safe harbor

<sup>115</sup> See *ibidem*, p. 1036.

<sup>116</sup> *Idem*.

<sup>117</sup> See *ibidem*, p. 1038.

<sup>118</sup> 488 F.3d 1102, 1114 (9th Cir. 2007).

<sup>119</sup> See *idem*.

<sup>120</sup> See *UMG Recordings, Inc. v. Veoh Networks Inc.*, 667 F.3d 1022, 1038 (9th Cir. 2011).

<sup>121</sup> See *ibidem*, pp. 1039-1040.

<sup>122</sup> *Ibidem*, p. 1040.

could be nullified in this way. The Court also rejected as red flag evidence, an e-mail sent by the CEO of a copyright holder stating that several materials were on the Veoh service without authorization.<sup>123</sup> The Court noted that this informal e-mail came from a copyright holder and therefore was subject to the take-down notice notification requirements established by section 512(c)(1)(A)(i).<sup>124</sup> Moreover, it noted that even if that e-mail would be actual knowledge or red flag knowledge, the answering e-mail by Veoh executives indicated that they would take down the materials immediately and that UMG was unable to demonstrate that the materials were not taken down.<sup>125</sup> The Ninth Circuit also rejected an e-mail coming from a user who was not a copyright holder as evidence to create red flag knowledge. The court held that UMG was unable to show that the defendant did not take down the infringing materials at issue.<sup>126</sup>

Even with this favorable outcome, Veoh did not obtain attorney's fees, and expenses incurred in litigation sent the company to bankruptcy.<sup>127</sup>

#### IV. PROPOSED ACTIONS

##### 1. *Analyzing Current Trends and The Big Problem*

This part of the article identifies what I consider the biggest challenge that technological, statutory and case law developments have posed on copyrights. Chapter one revisited cases involving the interpretation and evolution of judicial created principles such as contributory infringement, vicarious infringement, as well as fair use, citing the cases of *Sony*, *Napster*, and *Grokster*. However, technology involved in those cases has evolved into more developed and convenient ways of copying, distributing, and obtaining copyrighted materials. Having installed *peer to peer* software could be troublesome for many, besides the risk of facing large statutory damages in a possible lawsuit. In this regard, new and more user-friendly platforms

<sup>123</sup> See *idem*.

<sup>124</sup> See *idem*.

<sup>125</sup> See *idem*.

<sup>126</sup> See *idem*.

<sup>127</sup> See *ibidem*, p. 1050. See also Lital Helman and Gideon Parchomovsky, *op. cit.*, p. 1208.

have emerged. A user may find it easier to get a video or a song from services like *YouTube* or *Grooveshark* rather than installing *peer to peer* software. Additionally, there are platforms involving authorized distribution of copyrighted works like *iTunes*, the first platform making authorized recordings available over the Internet. This has been very convenient, even for those users initially attracted by *Napster*, because before *iTunes* they could not find a place that made authorized recordings available.<sup>128</sup>

Many users may prefer authorized services over unauthorized ones. In this regard, platforms like *iTunes*, *Netflix*, *Spotify* or similar ones are a good response to new technologies. However, infringement is still pervasive; *peer to peer* technology has evolved into *BitTorrent* technology, offering greater speeds and still posing a very serious concern, which now also includes large movie files.<sup>129</sup>

Nevertheless, the sharing of music or videos is not the main problem. The big issue is the pervasive number of unauthorized works available in services like *YouTube*, or even the mere existence of a service called *Grooveshark*. The latter is considered an abuse of §512 safe harbor. It is a service focused on music files for users to upload, as with *YouTube*. However, it has been alleged that employees of the company offering the service Escape Media Group, Inc. have uploaded thousands of music files following orders of their employers.<sup>130</sup> The site contains millions of songs and has millions of subscribers, obtaining revenue from advertising, subscription to its plus service, and from mobile apps.<sup>131</sup> While it has obtained a license from EMI, it has not been authorized by UMG, VMG, or Sony, and yet it offers music recordings from all of these companies and others.

<sup>128</sup> See Menell, Peter S., "This American Copyright Life: Reflections on Re-Equilibrating Copyright for the Internet Age," *UC Berkeley Public Law Research Paper*, No. 2347674, (April 4, 2014), <http://ssrn.com/abstract=2347674>, p. 23.

<sup>129</sup> See Ren, Patience, "The Fate of Bit Torrent John Does: A Civil Procedure Analysis of Copyright Litigation," *Hastings Law Journal*, vol. 64, 2013, p. 1343, 1350.

<sup>130</sup> See *Digital Music News LLC v. The Superior Court of Los Angeles County*, 2014 Cal. App. LEXIS 422, 6 (2014). See also Menell, Peter S., "Jumping the Grooveshark: A Case Study in DMCA Safe Harbor Abuse", *SSRN Working Paper Series*, (December 21, 2011), <http://ssrn.com/abstract=1975579>, p. 2. *UMG Recordings, Inc. v. Escape Media Group, Inc.* 2013 N.Y. App. Div. LEXIS 2642 (2013).

<sup>131</sup> See Menell, Peter S., *op. cit.*, p. 1.

The service is also characterized by offering free access to infringing copies of every “song in the world”.<sup>132</sup> Nonetheless, it is disturbing to realize that, at the beginning, an action taken by a copyright holder against this obviously infringing site was not based on the Copyright Act of 1976; instead it was a common law copyright action filed in a New York state court.<sup>133</sup> The argument was that among those infringing files were recordings done prior to February 15, 1972, not covered by the federal Copyright Act, but by the New York common law copyright.<sup>134</sup> The statutory provision on this regard establishes that “[w]ith respect to sound recordings fixed before February 15, 1972, any rights or remedies under the common law or statutes of any State shall not be annulled or limited by this title until February 15, 2067. The preemptive provisions... shall apply... after February 15, 2067”.<sup>135</sup> Therefore, the plaintiff argued that a common law copyright infringement is not subject to the safe harbor provisions established by section 512 of the federal Copyright Act.<sup>136</sup> Even if the Court of Appeals accepted this interpretation,<sup>137</sup> this action is a call for reformation of the outdated DMCA safe harbor provisions.

<sup>132</sup> See Silver, Joseph, “A Shark-Proof Cage for Interactive Streaming Music Services? Testing the Limits of the DMCA Safe Harbor Immunity in the Era of Grooveshark”, *SSRN Working Paper Series*, (October 6, 2013), <http://ssrn.com/abstract=2335563>, p. 2

<sup>133</sup> See *UMG Recordings, Inc. v. Escape Media Group, Inc.* 2013 N.Y. App. Div. LEXIS 2642 (2013).

<sup>134</sup> See *ibidem*, pp. 3, 4.

<sup>135</sup> Copyright Act, 17 U.S.C. §301(C).

<sup>136</sup> See *UMG Recordings, Inc. v. Escape Media Group, Inc.* 2013 N.Y. App. Div. LEXIS 2642, 4 (2013).

<sup>137</sup> See *ibid*, p. 8. As a result of the discovery that took place at the state action, plaintiff obtained evidence showing that Escape Media Group, Inc., and several of its employees, including its director illegally uploaded more than 4,053 plaintiff’s protected works into the Grooveshark website. See *UMG Recording, Inc. v. Escape Media Group, Inc.*, 2014 U.S. Dist. LEXIS 137491, p. 55. (2014). As a result, plaintiff decided to file an action based on the infringement of the federal Copyright Act. The action was filed at the District Court for the Southern District of New York. The District Court held defendants liable for copyright infringement and also for contributory and vicarious infringement. See *id*, pp. 57-70. The DMCA safe harbor did not insulate defendants from liability. In a different litigation, this time filed by Capitol Record, LLC. and EMI Music, the same defendant Escape Media Group, Inc. was held liable for the infringement of plaintiffs’ common law and federal copyrights. *Capitol Records, LL.C. v. Escape Media Group, Inc.* 215 U.S. Dist. LEXIS 38007 (2015). The site was finally shut down. However, the argument I propose continues the same, DMCA safe harbor

As the previous analyzed cases show, a judicial reinterpretation of the confusing statutory terms seems unlikely. This is contrary to cases involving judicial created principles, where the judiciary has taken an active role interpreting those principles. For instance, in *Grokster*, the Supreme Court heard the case and established that the Ninth Circuit misinterpreted *Sony* because it read its limitations on liability “to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties’ infringing use of it...even when actual purpose to cause infringing use is shown...unless the distributors had ‘specific knowledge of infringement...’”.<sup>138</sup> The Supreme Court used different reasoning than the Ninth Circuit, taking into consideration the purpose of the service, and holding that *Grokster* was liable because its unlawful objective was “unmistakable”.<sup>139</sup> In this regard, one may wonder whether the purpose of *Grooveshark* is also “unmistakable”. Nonetheless, in *Grokster*, the Supreme Court was analyzing the scope of contributory infringement liability, which invokes a different standard than the statutory limitation of liability argued in *YouTube*, *Veoh*, or *Grooveshark*.

Common law doctrines like secondary liability developments are unlikely to guide DMCA safe harbor cases.<sup>140</sup> Both are different issues, probably each irrelevant for the interpretation of the other.<sup>141</sup> However, even if *Grokster* was not a service provider and section 512 was not invoked, some have found it similar to *YouTube* in the sense that both cases involve the liability of an enterprise for infringement of its clients.<sup>142</sup> I would not accept that assumption completely, because in *Grokster*, the defendant could not be held liable for direct infringement, and in the case of *YouTube*, the videos were hosted on its servers and therefore the defendant could be held liable for both, direct infringement and secondary liability. While it is true that the Second Circuit cited *Grokster* in its *YouTube* ruling, it did so in order to reject the plaintiff’s argument establishing that Congress had included the

regime, enabled this abusive site. However, discovery proceedings to gather evidence, probed helpful to solve these cases.

<sup>138</sup> *Metro-Goldwyn Mayer Studios Inc. v. Grokster, Ltd* 545 U.S. 913, 934 (2005).

<sup>139</sup> *See ibid*, pp. 937, 940.

<sup>140</sup> *See Monseau, Susanna, op. cit.*, p. 103.

<sup>141</sup> *See idem*.

<sup>142</sup> *See Robins, Martin B., op. cit.*, p. 18.

vicarious liability doctrine on subsection 512(c)(1)(B).<sup>143</sup> This would make me think that courts will probably not use a common law principle to guide DMCA interpretation.

Still, the Second Circuit accepted the application of the common law doctrine called willful blindness to DMCA section 512 cases in certain circumstances, holding that since the statute does not mention said doctrine, then the interpretation is that it did not abrogate it.<sup>144</sup> Since the case was settled, the District Court did not issue a new resolution on remand nor did the case reach the Supreme Court on certiorari. As I mentioned before, both resolutions, the District Court and the Second Circuit were criticized as rewriting the statute, misinterpreting legislative history, and also having an uncertain result for copyright holders and also for Internet service providers.

The resulting problem is an open door allowing infringing services to grow up at the expense of copyright holders. While popular among users, the outcome will be less production of new copyrighted materials like song recordings. New artists may find it more difficult to make a living based on the sale of their recordings, or even to get funding from the music industry to produce a single recording.<sup>145</sup> Since Napster, the music industry is facing challenging economic times, and contract terms between recording labels and artists are less favorable to artists than before, to the point that some of them have gone bankrupt.<sup>146</sup> While the cost of distributing music recordings has decreased with Internet technology, the cost of producing good “compelling content” remains high.<sup>147</sup> So, artists seem to suffer the worst

<sup>143</sup> See *Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19, 36-38 (2nd Cir. 2012).

<sup>144</sup> See *Viacom International, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2nd Cir. 2012).

<sup>145</sup> See Menell, Peter S., *op. cit.*, p. 38.

<sup>146</sup> See *ibidem*, pp. 38, 46-50, explaining difficulties of new artists and less favorable terms in their contracts with music labels, even less favorable when the distribution of the recordings is through online services like iTunes, and others. See also Mascetti, Jaquelyn L., “Going for Broke in the Music Industry: Aligning the Code with the Interests of Recording Artists”, *American Bankruptcy Institute Law Review*, vol. 19, 2011, p. 185, discussing the cases of several successful singers that filled bankruptcy and the effects of bankruptcy procedures over the contracts they had entered into before with music labels. See also Lemley, Kevin Michael, “Protecting Consumers from Themselves: Alleviating the Market Inequalities Created by Online Copyright Infringement in the Entertainment Industry”, *Albany Law Journal of Science & Technology*, vol. 13, 2003, pp. 613, 625, noting annual losses of recording labels since Napster.

<sup>147</sup> See *ibidem*, p. 42.

part, being pressure on two sides, from recording labels with disadvantageous contact terms and also from infringing sites making money at the expense of their recordings.

## 2. *Ineffective Approaches*

A judicial precedent to properly interpret the troubled DMCA safe harbor provisions is desirable. However, it is unlikely that a future case will reach the Supreme Court for the reinterpretation of statutory provisions. What litigation in *YouTube* and *Veoh* proved is that two different circuits are heading in the same direction. Both of those cases should have been significant enough to reach the Supreme Court. If neither of them was reviewed by the Supreme Court, it would seem unlikely that a future DMCA safe harbor case attract the attention of Supreme Court. The alternative is a legislative change on the statute to rebalance the safe harbor regime. However, any attempt to change the equation may suffer important opposition. The following trends have proven unsuccessful to deter or stop infringement, and have furthermore raised serious opposition and public outrage about copyrights in general.

### A. *The SOPA and the PIPA*

Prior attempts of statutory reform have faced serious opposition and eventually have failed, e.g. the SOPA,<sup>148</sup> and the PIPA.<sup>149</sup> Both bills targeted foreign infringing Internet websites, those registered under foreign domain names, hosted in servers abroad, beyond jurisdiction of U.S. courts.<sup>150</sup> With only slight differences, both bills established that upon an action filed by the Attorney General, a court may order a measure directed to Internet service providers in order to prevent access by their consumers located within the U.S., to infringing foreign sites.<sup>151</sup> Other measures included were: in rem

<sup>148</sup> Stop Online Privacy Act. H.R. 3261, 112th Cong. (2011).

<sup>149</sup> Protect IP Act. S. 968, 112th Cong. (2011).

<sup>150</sup> See Band Jonathan, "The SOPA-TPP Nexus", *American University International Law Review*, vol. 28, 2012, p. 31, 33.

<sup>151</sup> See H. R. 3261, 112th Cong. §102 (e)(2)(A)(i) (2011). See also S. 968, 112th Cong. § (2011).

actions against foreign infringing domain names; judicial orders preventing domain systems to resolve the IP address of foreign infringing sites, so the user's browser would not connect to the it; search engines would disable access to foreign infringing sites; payments systems like Visa or MasterCard would not process payments to foreign infringing sites; also, advertising would not be installed in those foreign infringing pages.<sup>152</sup>

The bills received criticism for several reasons. For instance, although supposed to target only foreign sites, they also included U.S. sites.<sup>153</sup> In addition, a small amount of infringing materials within a site would be enough to block the entire site, in which a case the DMCA safe harbor provisions would be inapplicable.<sup>154</sup> Domain name blocking would present security issues due to unencrypted communications and even those measures would be useless if consumers would use foreign domain name numbers to circumvent the blockage.<sup>155</sup> Moreover, payment systems would have to suspend their services to alleged infringing sites within five days after notification from the rights holder, without a judicial declaration of infringement, which could represent a due process concern.<sup>156</sup> Criticisms also included in rem provisions, extraterritorial application of U.S. law, excessive expansion of copyright, and the suppression of free speech.<sup>157</sup>

Both bills finally failed. There were several factors that contributed to their failure. Among them, were protests of popular service providers and their numerous users, scholarly criticism, and also a White House statement against the bills: "while we believe that online piracy by foreign websites is a serious problem that requires a serious legislative response we will not support legislation that reduces freedom of expression, increases cybersecurity risk, or undermines innovative global Internet."<sup>158</sup> This general opposition and concerns about the proposals had international influence

<sup>152</sup> See Band, Jonathan, *op. cit.*, p. 33. Analyzing several provisions of proposed bills.

<sup>153</sup> See *ibidem*, p. 35.

<sup>154</sup> See *idem*.

<sup>155</sup> See *idem*.

<sup>156</sup> See *idem*.

<sup>157</sup> See *idem*. See also Menell, Peter S., *op. cit.*, p. 77.

<sup>158</sup> Espinel, Victoria *et al.*, "Combating Online Piracy while Protecting an Open and Innovative Internet," <https://petitions.whitehouse.gov/response/combating-online-piracy-while-protecting-open-and-innovative-internet>, (last visited September 3, 2014).

and greatly influenced the failure of a different proposal, this time in the international arena, the ACTA.<sup>159</sup>

## B. *The ACTA*

ACTA negotiations were different than previous international IP treaties that are well known today. To illustrate this point it is worth considering that the Berne Convention, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) and the World Intellectual Property Organization (WIPO) Internet treaties of 1996 were publicly negotiated under the umbrella of an international organization like the WIPO or in the TRIPs case, the World Trade Organization (WTO). However, ACTA has a different history; it was secretly negotiated until related documents were posted on *WikiLeaks*,<sup>160</sup> one of the many controversies related to this failed proposal. Stricter enforcement measures, frequently tagged as draconian, without exceptions like fair use, caused this proposal to face great opposition.<sup>161</sup>

Since TRIPs agreement negotiations under Uruguay Round, IP exporting countries moved the negotiating table from WIPO to WTO. The complaint about WIPO several years ago was that IP protection was weak or even nonexistent in developing countries.<sup>162</sup> WIPO was not considered as a solution because its one nation, one vote policymaking process gave developing countries control over the agenda, including discussions about any proposal.<sup>163</sup> Therefore IP holders pressured their governments and managed to move the negotiating table to WTO, where noncompliance countries may face commercial retaliatory measures under its Dispute Settlement Understanding.<sup>164</sup> Still, the role of WIPO was important under the TRIPs scheme, as were teaching and helping developing countries to implement

<sup>159</sup> See Band, Jonathan, *op. cit.*, p. 46.

<sup>160</sup> See Ayoob, Emily, "The Anti-Counterfeiting Trade Agreement," *Cardozo Arts & Entertainment Law Journal*, vol. 28, 2010, p. 175, 180.

<sup>161</sup> See Kaminski Margot, "The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)," *Yale Journal of International Law*, vol. 34, 2009, pp. 247 and 248.

<sup>162</sup> See Ryan, Michael P., *Knowledge Diplomacy. Global Competition and the Politics of Intellectual Property*, Washington, Brookings Institution Press, 1998, p. 91.

<sup>163</sup> See *idem*.

<sup>164</sup> See *ibidem*, pp. 71-77.

TRIPs agreement.<sup>165</sup> Yet this trend did not end here; copyright holders have pressed for even more convenient negotiating conditions, and WTO was not the forum to negotiate the ACTA. On the contrary, it was negotiated outside any international organization with the subsequent lack of checks and balances in the negotiation process, lack of any recording system, and also lack of publicity for the negotiation process.<sup>166</sup> Those conditions generated a draft obviously lacking any degree of legitimacy, a perfect target for opposition and criticism.

There were about five known drafts, the last one less ambitious than the first one.<sup>167</sup> Even in this last draft, terms were wider than those in the TRIPs agreement and included, among other things: broader border measures; statutory damages; criminal procedures against infringement without any economic advantage, instead of TRIPs “commercial scale” requirement; mandatory attorney’s fees instead of the permitted approach under TRIPs; requirement of service providers to disclose information of infringing users; circumvention measures in similar terms to those in DMCA.<sup>168</sup> The scope of all ACTA provisions were obviously broader than those included in any intellectual property international treaty, however a major concern was that the treaty terms as written would require member states to criminalize activities like file sharing and also would require searching infringing files in laptops or mobile devices at borders or airports, which could then result in criminal prosecution.<sup>169</sup>

It was suggested that countries participating in the negotiating table were those less likely to object to the proposed provisions.<sup>170</sup> However, countries like Brazil, China and India did not participate in negotiations and openly opposed the proposal.<sup>171</sup> Another legitimacy problem would be the fact that these ACTA standards would make their way into bilateral

<sup>165</sup> See *ibidem*, p. 125.

<sup>166</sup> See Kaminski, Margot E., “An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement”, *Albany Law Journal of Science & Technology*, vol. 21, 2011, pp. 385, 390.

<sup>167</sup> See *idem*.

<sup>168</sup> See *ibidem*, pp. 397-414,

<sup>169</sup> See McManis, Charles R., “The Proposed Anti-Counterfeiting Trade Agreement (ACTA): Two Tales of a Treaty”, *Houston Law Review*, vol. 46, 2009, pp. 1235, 1246.

<sup>170</sup> See Weatherall, Kimberlee, “Politics, Compromise, Text and the Failures of the Anti-Counterfeiting Trade Agreement”, *Sydney Law Review*, vol. 33, 2011, p. 229, 236.

<sup>171</sup> See *ibidem*, p. 235

treaties and countries that would have to make major changes in their internal law in order to comply with these standards were not seated at the negotiations table.<sup>172</sup>

Finally, ACTA was rejected by the European Union Parliament; a voting of 478 against and 39 in favor showed how strong the opposition was.<sup>173</sup> Declarations given by European Parliament President Martin Schultz, also voiced concerns about the proposal: “the rejection was driven by the concern that ACTA is too vague, leaving the room for abuses and raising concerns about its impact on consumer’s privacy, civil liberties, on innovation and the free flow of information... ACTA was negotiated by a group of industrialized countries in a process that provoked complaints for its lack of transparency”.<sup>174</sup> After this rejection, eight countries signed the agreement anyway: Australia, Canada, Korea, Japan, New Zealand, Morocco, Singapore, and the United States.<sup>175</sup> However, ratification processes stalled for good in all countries but Japan; therefore, the sixth ratification required to put the agreement into force never occurred.<sup>176</sup>

### 3. Questionable Litigation

Litigation efforts have not always been directed at big companies. Suing a multimillion dollar enterprise is not quite the same as suing a 12-year-old honor roll student or a 66-year-old retired nurse.<sup>177</sup> Those are only two examples of suits among thousands directed against *peer to peer* users

<sup>172</sup> See *ibidem*, pp. 235 and 236.

<sup>173</sup> See Kirwin, Joe, “European Parliament Overwhelmingly Votes to Reject ACTA”, *BNW World Intellectual Property Report*, vol., 2012, p. 9.

<sup>174</sup> *Idem*.

<sup>175</sup> See Office of the United States Trade Representative, “Anti-Counterfeiting Trade Agreement,” <http://www.ustr.gov/acta>, (last visited September 3, 2014).

<sup>176</sup> See Flynn Sean M. *et al.*, “The U.S. Proposal for an Intellectual Property Chapter in the Trans-Pacific Partnership Agreement”, *American University International Law Review*, vol. 28, 2012, pp. 105, 111.

<sup>177</sup> See Witt, Amanda M., “Burned in the USA: Should the Music Industry Utilize its American Strategy of Suing Users to Combat Online Piracy in Europe?”, *Columbia Journal of European Law*, vol. 11, 2005, pp. 375, 381, describing the record industry strategy of suing peer-to-peer users between 2003 and 2005; by May 2005 the recording industry had filed suits against nearly 10,000 users.

for copyright infringement. Public opinion recognizes how large statutory damages can be when a jury extends a \$1.92-million-dollar verdict against an individual who shared twenty-four songs.<sup>178</sup> By 2008, about 30,000 users have been threatened with lawsuits by the recording industry. This kind of litigation has not only proven unsuccessful to deter copyright infringement, but also has been the seed of strong opposition to any initiative favoring copyright holders, similar to those mentioned above, from statutory reform to an international treaty.

*Peer to peer* technology has evolved since *Napster* or *Grokster* and communications are now more efficient. A new protocol has emerged, under which files do not come from a single computer but are fragmented in packs coming from different computers, and users do not have the option let them have materials downloaded, without allowing the uploading of contents they already have in their computers.<sup>179</sup> So, all users allow the uploading. This highly popular *peer to peer* protocol known as *BitTorrent* mandates simultaneous uploading and downloading of files in multiple packs, often described as a torrent or swarm.<sup>180</sup> Although the transfer of files is more stable and speedy, this method of exchanging files has legal consequences. If an individual wants to download a song or other protected work, the file would come from different users and not just from one user as before.

Since this *BitTorrent* protocol sets simultaneous sharing from different sources, many users could be engaged jointly in acts of infringement. As a result, the so-called John Doe litigation has increased dramatically. Defendants, named John Does, are originally identified only by their IP addresses.<sup>181</sup> Then a District Court issues a subpoena requesting Internet service providers to identify those users based only on the IP addresses provided.<sup>182</sup> After obtaining the names, supposedly for the purpose of serving the defendants, plaintiffs will use the names and private information in order to obtain monetary settlements from prospective defendants.<sup>183</sup> Each action is against a large number of defendants, reaching in some cases hundreds or

<sup>178</sup> See Lunney, Jr., Glynn S., "Copyright, Private Copying and Discrete Public Goods", *Tulane Journal of Technology & Intellectual Property*, vol. 12, 2009, pp. 1 and 2.

<sup>179</sup> See Ren, Patience, *op. cit.*, p. 1352.

<sup>180</sup> See *ibidem*, p. 1353.

<sup>181</sup> See *ibidem*, p. 1348.

<sup>182</sup> See *idem*.

<sup>183</sup> See *idem*.

even thousands of IP addresses.<sup>184</sup> Even copyright holders of pornographic movies use these tactics, and individuals often accept to settle in order to avoid the embarrassment of being exposed on trial as sharing pornographic materials or just to avoid the odds of litigation.<sup>185</sup> Even grandmothers unaware of wireless securing have been accused of sharing pornographic copyrighted materials.<sup>186</sup>

These cases are composed by two legal inquiries; the first is related to discovery and the second to the joinder of defendants. Under the first point, John Doe subpoenas are directed to third parties in order to learn the name of an alleged *peer to peer* infringer, and are based on rule 26(d) (1) of the Federal Rules of Civil Procedure. This rule precludes discovery unless a conference between parties is held in order to arrange discovery planning.<sup>187</sup> Since the plaintiff does not even know the name of the defendant, just his IP address, then the route is to file for a subpoena according to rule 45 of the Federal Rules of Civil Procedure in order to obtain the name from the defendant's Internet service provider. Courts have broad discretionary powers and circuits are split over the standard required to grant the subpoena.<sup>188</sup> For instance, the Ninth Circuit has developed the good cause standard, and other circuits have developed their own standards as well, like the *Notaro* standard or the reasonableness standard.<sup>189</sup>

The second legal inquiry in these cases is the joinder of defendants. The legal standard in order to put several defendants in one proceeding is established by rule 20(a)(2) of the Federal Rules of Civil Procedure, which allows several defendants to join in one action if: "(A) any right to relief is asserted against them jointly, severally, or in the alternative with respect to or arising out the transaction, occurrence or series of transactions or occurrences; and (B) any question of law or fact common to all defendants

<sup>184</sup> See *idem*.

<sup>185</sup> See Menell, Peter S., *op. cit.*, p. 32.

<sup>186</sup> See Ren, Patience, *op. cit.*, p. 1349.

<sup>187</sup> See *ibidem*, p. 1355. See also *Malibu Media, LLC v. John Does 1 through 13*, 2012 U.S. Dist. LEXIS 94705, at 8 (E.D. Cal. 2012).

<sup>188</sup> See *ibidem*, p. 1355 -1356.

<sup>189</sup> See *ibidem*, p. 1355. See also *Malibu Media, LLC v. John Does 1 through 13*, 2012 U.S. Dist. LEXIS 94705, at 9 (E.D. Cal. 2012). See also Panoff, Jesse N., "Rescuing Expedited Discovery from Courts & Returning It to FRCP 26(d)(1): Using a Doctrine's Forgotten History to Achieve Legitimacy", *Arkansas Law Review*, vol. 64, 2011, pp. 651, 661.

will arise in the action”.<sup>190</sup> In the case of *BitTorrent* protocol, this is particularly easy since all defendants are arguably sharing the same protected work in the so-called swarm or torrent. Therefore, defendants are allegedly incurring in infringement together in the same series of transactions with copyrighted materials. However, courts are also in split on the procedure, and have developed several tests in order to determine joinder, like the “same transaction test” or even an extra requirement called “fundamental fairness”.<sup>191</sup> In this regard, even privacy concerns have arisen.<sup>192</sup> Other concerns are related to IP addresses, e.g. several individuals having access to the same IP, or public IP addresses in coffee shops, or users having unsecured wireless networks.<sup>193</sup> At present, the result is uncertain, but it is illustrative to quote a judge’s opinion about this kind of litigation. In no other copyright case, have I read a judge describe the plaintiff’s legal tactics as an “extortion scheme.” An excerpt from his opinion reads as follows:

The Court is familiar with lawsuits like this one. These lawsuits run a common theme: plaintiff owns a copyright to a pornographic movie; plaintiff sues numerous John Does in a single action for using BitTorrent to pirate the movie; plaintiff subpoenas the ISPs to obtain identities of these Does; if successful, plaintiff will send out demand letters to the Does; because the embarrassment, many Does will send back a nuisance-value check to the plaintiff. The cost to the plaintiff: a single filing fee, a bit of discovery, and stamps. The rewards: potentially hundreds of thousands of dollars. Rarely do these cases reach the merits... The Court will not idly watch what is essentially an extortion scheme, for a case that plaintiff has no intention to bringing to trial... [i]f Malibu desires to vindicate its copyright rights, it must do it the old-fashioned way and earn it.<sup>194</sup>

This is not the only case where a court has found inappropriate the use of court’s subpoena powers in order to obtain the defendants’ personal information with no intention to litigate, but rather to force monetary settle-

<sup>190</sup> Fed R. Civ. P. 20(a)(2).

<sup>191</sup> See Ren, Patience, *op. cit.*, pp. 1366 and 1367.

<sup>192</sup> See Rosen, Amy, “The Big Lawsuits Keep on Coming: An Analysis of Extortive Pornographic “Trolling Lawsuits” and Preventive Approaches,” *Journal of the Patent and Trademark Office Society*, vol. 95, 2013, p. 165, 191.

<sup>193</sup> See *ibidem*, p. 192.

<sup>194</sup> *Malibu Media, LLC v. John Does 1 through 10*, 2012 WL 5382304, at, 3-4 (C.D. Cal. 2012).

ments. In some cases, courts have initiated sanction procedures under rule 11 of the Federal Rules of Civil Procedure. In *Raw Films v. Does 1 through 32*, the District Court for the Eastern District of Virginia, Richmond Division held that: “plaintiffs’ conduct in these cases indicates an improper purpose for the suits... the joinder of unrelated defendants does not seem to be warranted by existing law or a non-frivolous extension of existing law... the Court, therefore, will direct the plaintiff and its counsel to show cause why the conduct specifically described in this Memorandum Order has not violated Rule 11(b)”.<sup>195</sup> It is important to note that purposes and strategies of the adult movie industry are different than those of the music recording industry. While the adult film industry system was labelled as an “extortion scheme” by judges, the purpose of the music industry is to deter copyright infringement.<sup>196</sup> As a result of the negative publicity and unsuccessful deterrence results, the Recording Industry Association of America (hereinafter RIAA) has stopped these lawsuits.<sup>197</sup> However, the pornography industry continues this trend, and negative public opinion about those actions still reach the recording industry, which after all, started the trend of suing individuals by filing what it is recognized as the first copyright John Doe case.<sup>198</sup>

#### 4. *Getting Back to the Basics. Proposed Approach*

What I propose is very simple: a legislative change to apply section 512(c) (1)(A)(ii) containing the red flag knowledge: “in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent...” Certainly, its reading alongside section 512(m)(1), which establishes that service providers are not conditioned to monitor contents to seek for infringing activities, should be limited in order to avoid courts interpreting red flag knowledge from the statute. These basic

<sup>195</sup> *Raw Films v. Does 1 through 32*, 2011 U.S. Dist. LEXIS 114996, at 7 (E.D.Va. 2011).

<sup>196</sup> *See Ren, Patience, op. cit.*, p. 1347.

<sup>197</sup> *See idem.*

<sup>198</sup> *See Natividad, Kim F., “Stepping It Up and Taking It to the Streets: Changing Civil & Criminal Copyright Enforcement Tactics”, Berkeley Technology Law Journal*, vol. 23, 2008, pp. 469, 473. Describing Capitol Records, Inc. v. Thomas (citation omitted), as the first John Doe case, in which defendant was a Native American, single mother of two.

changes would remove from DMCA's safe harbor those services whose business model is based on copyright infringement and yet are currently covered by the safe harbor.

As mentioned before, section 512 establishes two different ways to get the knowledge that would take away the safe harbor protection if the service provider takes no action. The first one is the take-down notification made by copyright holder, which is established by section 512(c)(1)(A)(i). The problem, as previously analyzed, is that courts have deemed this way of obtaining knowledge as the only one, eliminating section 512(c)(1)(A)(ii) from the statute. While Congress did enact the later red flag knowledge into the statute, several factors, such as its interaction with section 512(m)(1), have made courts ignore it. Negotiations during the legislative process, including different positions from several interest groups, resulted in confusing or apparently contradictory provisions.<sup>199</sup> Although it has been argued that Copyright holders were trying to win in litigation what they had already have lost in Congress,<sup>200</sup> Congress must have added section 512(c)(1)(A)(ii) into the statute with the intention of making it applicable. Besides the intent of Congress to include safe harbor provisions, or courts failure to interpret statutory terms, there is another important factor that begs for statutory revision. During the nineties, when the bill was introduced in Congress, the boundless scope of present Internet capabilities could not be foreseen.

Internet access and capabilities were different in the nineties. At that time, users had to access Internet through dial-up connections with restricted capacities. Internet speed was slower, computers and mobile devices were quite limited compared to today's equipment, and compression software was inadequate. The kind of service providers Congress must have had in mind were like those in *Religious Technology Center v. Netcom On-line Communication Services, Inc.*,<sup>201</sup> a decision rendered in 1995. One of the service providers was the operator of an online bulletin containing discussion forums, where one of its users allegedly committed direct copyright infringement by uploading a manuscript containing literary criticism and

<sup>199</sup> See Imfeld Cassandra and Smith Ekstrand, Victoria, *op. cit.*, p. 312.

<sup>200</sup> See Reichman, Jerome H. *et al.*, *op. cit.*, p. 994.

<sup>201</sup> 907 F. Supp. 1361 (N.D. Cal. 1995).

fragments of a work; the other defendant was the Internet service provider who gave the operator of the online bulletin access to Internet.<sup>202</sup>

An online discussion forum of the nineties or an Internet service provider hosting that forum are very different services from what Internet providers can offer today. Downloading a song or a high definition movie in 1998 would have taken hours or even days. Today, the same uploading or downloading of copyrighted works can be accomplished in seconds or a few minutes. This new technological power automatically increases the number of protected works on stage. Therefore, the take-down-notice approach does not represent the same burden today as in 1998. Problems arise when a given Internet service provider, well aware of this gap in the law, designs its business model at the expense of protected works.

Evolution in technology does not always cause the law to evolve at the same rate. This is especially true in the case of DMCA's safe harbor provisions that were the product of legislative will. Other statutory provisions were originally created by case law and later recognized and incorporated into the statute, allowing, in this way, natural judicial evolution. When Congress incorporates a principle originating in case law into a statute, this will usually be interpreted as recognition of the principle behind it, without the intention of freezing it in the statute. However, when judges interpret DMCA's safe harbor, they are more cautious. This is not a judiciary creation like the fair use defense, incorporated in section 107 of the Copyright Act. As a result, those principles have been frozen in a way incapable of easy adaptation to new technologies.

One approach to statutory revision would be to import knowledge definitions from judicially created contributory infringement doctrine, allowing those definitions to evolve in future cases. However, this approach would undoubtedly suffer great opposition and could create more confusion about the scope of the safe harbor. Nevertheless, in cases where the record clearly shows an "unmistakable" unlawful objective,<sup>203</sup> it could prove effective to apply this approach. As another option, the statutory change could establish a test in order to determine knowledge, or to detect a business model based on copyright infringement. Since any chosen approach

<sup>202</sup> See *ibidem*, p. 1365.

<sup>203</sup> See *Metro-Goldwyn Mayer Studios Inc. v. Grokster, Ltd* 545 U.S. 913, 937, 940 (2005).

would suffer great opposition, something should be offered in exchange for its acceptance.

In order to overcome great opposition and the failure of the proposal, I suggest that copyright holders stop using all the ineffective approaches described above. This include not to intend any other draconian initiative like SOPA, PIPA, or a secretly international proposal like the ACTA, criminalizing sharing activities by users. Also, it is suggested to avoid litigation against private individuals engaged in noncommercial sharing like those described above. The John Doe litigation extortion schemes must be avoided. What I propose here is not to target private individuals or users but big companies.

In order to have DMCA's safe harbor reviewed, I would even suggest the establishment of a reasonable limit on statutory damages in cases where the defendant is an individual infringing protected works with no commercial purposes, like those in the previously mentioned cases. A monetary judgment raising over one or two million dollars against an individual sharing only a limited number of songs seems unreasonable, when at the same time a safe harbor is protecting from liability a big enterprise like Grooveshark with a business model based on copyright infringement. The proposal in this sense is not about reducing statutory damages in any way, but only to consider "innocent infringement".

Section 504 of the Copyright Act establishes actual damages and profits, and also statutory damages. A copyright holder may choose actual damages and profits or statutory damages. In the case of statutory damages, the sum ranges from \$750 to \$30,000 for each infringed work.<sup>204</sup> However, if the infringement was committed willfully, the sum can reach \$150,000 for each infringed work. For innocent infringers, the statute only establishes \$200 for each infringed work: "[if] infringer was not aware and had no reason to believe that his her acts constituted an infringement of copyright, the court in its discretion may reduce the award of statutory damages to a sum of not less than \$200."<sup>205</sup> However, section 402 of the Copyright Act precludes an innocent infringement defense if the phonorecord of a sound recording has the copyright notice in accordance with such section. For music files, the issue is that section 402 refers only to phonorecords, defined by section 101 as "material objects." In a case concerning this is-

<sup>204</sup> See 17 U.S.C. §504(c)(1).

<sup>205</sup> See *id* §504(c)(2).

sue, the Supreme Court denied certiorari; however, the dissenting opinion written by Justice Alito is illustrative:

I would grant the petition to consider the question whether 17 U.S.C. §402(d) applies when a person is found to have engaged in copyright infringement by downloading digital music files... In this case, a 16-year-old was found to have infringed... digital music files. The District Court held that there were genuine issues of fact on whether she qualified as an innocent infringer, but the Court of Appeals reversed concluding that another provision... foreclosed the innocent-infringer defense as a matter of law... There is a strong argument that §402(d) does not apply in a case involving the downloading of digital music files. This provision was adopted... well before digital music files... a person who downloads a digital music file generally does not see any material object bearing a copyright notice.<sup>206</sup>

Having this issue clarified by Congress would not jeopardize the whole copyright notice regime. Furthermore, a small change, focused simply on file sharing cases would be reasonable, since there is no material object in a sound file. Obviously, this revision would not benefit any enterprise engaged in commercial activity. It would merely limit awards containing huge statutory damages against individuals that have shared only a few files.

The actual safe harbor regime, needs a revision. A proposal should be as subtle as the one here proposed, simply redefining the red flag knowledge contained in section 512(c)(1)(A)(ii).

## V. CONCLUSIONS

Copyright is important to encourage learning and new creative works. Copyright law has evolved alongside technology. However, the purpose of copyright has not changed due to these current trends. If no change is made, then at one point, we will be left with large popular web platforms offering dated content and only a few new works. Therefore, legislation referring to red flag knowledge needs to be rewritten to make it applicable to the copyright needs of today.

<sup>206</sup> Whitney Harper v. Maverick Recording Company, 131 S.Ct. 590, 590-591 (2010).

## VI. BIBLIOGRAPHY

- ARSHAM, Bryan E., “Monetarizing Infringement: A New Legal Regime for Host of User-Generated Content”, *Georgetown Law Journal*, vol. 101, 2013.
- AYOUB, Emily, “The Anti-Counterfeiting Trade Agreement”, *Cardozo Arts & Entertainment Law Journal*, vol. 28, 2010.
- BAND, Jonathan, “The SOPA-TPP Nexus”, *American University International Law Review*, vol. 28, 2012, p. 31.
- CASTREE, III, Sam, “Cyber-Plagiarism for Sale!: The Growing Problem of Blatant Copyright Infringement in Online Digital Media Stores”, *Texas Review of Entertainment & Sports Law*, vol. 14, 2012.
- CHANG, Liliana, “The Red Flag Test for Apparent Knowledge Under the DMCA §512(c) Safe Harbor”, *Cardozo Arts & Entertainment Law Journal*, vol. 28, 2010.
- DRATH, Ross, “Hotfile, Megaupload, and the Future of Copyright on the Internet: What Can Cyberlockers Tell Us about DMCA Reform”, *John Marshall Review of Intellectual Property Law*, vol. 12, 2012.
- FLYNN, Sean M. *et al.*, “The U.S. Proposal for an Intellectual Property Chapter in the Trans-Pacific Partnership Agreement”, *American University International Law Review*, vol. 28, 2012.
- GINSBURG, Jane C., Separating the Sony Sheep from the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs, *Arizona Law Review*, vol. 50, 2008.
- HASSANABADI, Amir, “Viacom v. YouTube –All Eyes Blind: The Limits of the DMCA in a Web 2.0 World”, *Berkeley Technology Law Journal*, vol. 26, 2011.
- HELMAN, Lital and PARCHOMOVSKY, Gideon, “The Best Available Technology Standard,” *Columbia Law Review*, vol. 111, 2011.
- IMFELD, Cassandra and SMITH EKSTRAND, Victoria, “The Music Industry and the Legislative Development of the Digital Millennium Copyright Act’s Online Service Provider Provision”, *Communication Law & Policy*, vol. 10, 2005.
- MASCETTI, Jaquelyn L., “Going for Broke in the Music Industry: Aligning the Code with the Interests of Recording Artists”, *American Bankruptcy Institute Law Review*, vol. 19, 2011.

- MCMANIS, Charles R., “The Proposed Anti-Counterfeiting Trade Agreement (ACTA): Two Tales of a Treaty”, *Houston Law Review*, vol. 46, 2009.
- MENELL, Peter S. and NIMMER, David, “Unwiding Sony”, *California Law Review*, vol. 95, 2007.
- , “This American Copyright Life: Reflections on Re-Equilibrating Copyright for the Internet Age”, *UC Berkeley Public Law Research Paper*, No. 2347674, (April 4, 2014), <http://ssrn.com/abstract=2347674>.
- MURLEY, Diane, “What is all the Fuss about Library 2.0?”, *Law Library Journal*, vol. 100, 2008.
- NATIVIDAD, Kim F., “Stepping It Up and Taking It to the Streets: Changing Civil & Criminal Copyright Enforcement Tactics”, *Berkeley Technology Law Journal*, vol. 23, 2008.
- NIMMER, David, “Brains and other Paraphernalia of the Digital Age,” *Harvard Journal of Law & Technology*, vol. 10, 1996.
- PANOFF, Jesse N., “Rescuing Expedited Discovery from Courts & Returning It to FRCP 26(d)(1): Using a Doctrine’s Forgotten History to Achieve Legitimacy,” *Arkansas Law Review*, vol. 64, 2011.
- KAMINSKI, Margot, “The Origins and Potential Impact of the Anti-Counterfeiting Trade Agreement (ACTA)”, *Yale Journal of International Law*, vol. 34, 2009, p. 247.
- , “An Overview and the Evolution of the Anti-Counterfeiting Trade Agreement”, *Albany Law Journal of Science & Technology*, vol. 21, 2011.
- KATYAL, Sonia K. and SCHULTZ, Jason M., “The Unending Search for the Optimal Infringement Filter”, *Columbia Law Review Sidebar*, vol. 112, 2012.
- KIRWIN, Joe, “European Parliament Overwhelmingly Votes to Reject ACTA”, *BNA World Intellectual Property Report*, 2012.
- LEMLEY, Kevin Michael, “Protecting Consumers from Themselves: Alleviating the Market Inequalities Created by Online Copyright Infringement in the Entertainment Industry”, *Albany Law Journal of Science & Technology*, vol. 13, 2003.
- LIEBOWITZ, Stan, “MP3s and Copyright Collectives: A Cure Worse than the Disease?”, in TAKEYAMA, Lisa N. *et al.*, *Developments in the Economics of Copyright*, Cheltenham, Edward Elgar Publishing Limited, 2005.
- LITMAN, Jessica, “Lawful Personal Use”, *Texas Law Review*, vol. 85, 2007.
- LUNNEY, Jr., Glynn S., “Copyright, Private Copying and Discrete Public Goods”, *Tulane Journal of Technology & Intellectual Property*, vol. 12, 2009.

- RABIL, Sara, “Google, Viacom Settle YouTube Copyright Suit, Terms Not Disclosed”, *BNA World Intellectual Property Report*, vol. 28, 2014.
- REICHMAN, Jerome H. *et al.*, “A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works”, *Berkeley Technology Law Journal*, vol. 22, 2007.
- REN, Patience, “The Fate of Bit Torrent John Does: A Civil Procedure Analysis of Copyright Litigation”, *Hastings Law Journal*, vol. 64, 2013.
- ROBINS, Martin B., “A Good Idea at the Time: Recent Digital Millennium Copyright Act §512(c) Safe Harbor Jurisprudence Analysis and Critique of Current Applications and Implications”, *Tulane Journal of Technology & Intellectual Property*, vol. 2012.
- ROSEN, Amy, “The Big Lawsuits Keep on Coming: An Analysis of Extortive Pornographic «Trolling Lawsuits» and Preventive Approaches”, *Journal of the Patent and Trademark Office Society*, vol. 95, 2013.
- RYAN, Michael P., *Knowledge Diplomacy. Global Competition and the Politics of Intellectual Property*, Washington, Brookings Institution Press, 1998.
- SCHACHTER, Jeremy A., “Substantially Perfect: The Southern District of New York’s Problematic Rewrite of the DMCA’s Elements of Notification”, *Cardozo Arts & Entertainment Law Journal*, vol. 29, 2011.
- SIRICHT, Methaya, “Catching the Conscience: An Analysis of the Knowledge Theory Under §512(C)’s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags”, *Albany Law Journal of Science and Technology*, vol. 23, 2013.
- STEERLING, J. A. L., *World Copyright Law*, 2nd. ed., London, Sweet & Maxwell, 2003.
- WEATHERALL, Kimberlee, “Politics, Compromise, Text and the Failures of the Anti-Counterfeiting Trade Agreement”, *Sydney Law Review*, vol. 33, 2011.
- WITT, Amanda M., “Burned in the USA: Should the Music Industry Utilize its American Strategy of Suing Users to Combat Online Piracy in Europe?”, *Columbia Journal of European Law*, vol. 11, 2005.