Whose Burden Is It Anyway? Addressing the Needs of Content Owners in DMCA Safe Harbors

Greg Jansen*

---

* Greg Jansen has a Bachelor of Science degree in Entrepreneurship and Marketing from Indiana University's Kelley School of Business. He expects to complete his Juris Doctorate degree from the Indiana University Maurer School of Law—Bloomington in May 2010. The Author would like to thank Professor Kevin Collins for his help in developing this Note.

I. INTRODUCTION

The struggle between intellectual property (IP) rights and innovation has reached a crucial moment in this country. On one hand, IP rights provide incentives for people to create artistic, literary, and technological works, which benefit society. On the other hand, ongoing innovation has brought us to a point where information has never been more accessible and ideas have never been easier to share. Interestingly, many of the protected creations would not exist but for cumulative innovations that at

times can threaten IP rights (and the incentives they provide). In reality, both schemes encourage creation of new goods, technologies, and art in different ways.

Nowhere is this tension more palpable than on the Internet, where digital technology and widespread adoption have made it simple and inexpensive to copy, distribute, and display creative works to millions, almost instantaneously. The ongoing $1 billion lawsuit between Viacom and YouTube is the pinnacle of this conflict.[1] Viacom asserts, among other contentions, that YouTube bears liability for direct and secondary copyright infringement resulting from YouTube users' video uploads of Viacom content.[2] In response, YouTube invoked the protections afforded by the Digital Millennium Copyright Act (DMCA) to defend its activities.[3]

The DMCA's Online Copyright Infringement Liability Limitation Act (Section 512) provides a framework for limiting an Online Service Provider's (OSP) liability for a third party's infringing use of its service.[4] The Act also provides a means for content owners to remove the infringing material from the OSP's Web site.[5] Nonetheless, copyright owners continue to pursue litigation against service providers as a means to prevent third-party infringement.[6]

Large content owners frequently sue facilitators of copyright infringement rather than pursuing individual infringers.[7] Copyright holders understand that many OSPs generate advertising revenue from page views arising from users viewing copyrighted content.[8] Content owners realize shutting down an entire online network capable of facilitating infringement is more effective at curtailing the amount of infringing material available than targeting millions of individual users.[9] These suits also attempt to shift

---

1. First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, Viacom Int'l, Inc. v. YouTube, Inc., No. 1:07-cv-02103, 2008 WL 2062868 (S.D.N.Y. Apr. 24, 2008).

2. *Id.* at 23-28.

3. Defendants' Answer to First Amended Complaint and Demand for Jury Trial at 10, Viacom Int'l, Inc. v. YouTube, Inc., No. 1:07-cv-02103, 2008 WL 2260018 (S.D.N.Y. May 23, 2008).

4. 17 U.S.C. § 512(c)(1) (2006).

5. *Id.* § 512(c)(3).

6. *See generally* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); IO Group, Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

7. Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1346 (2004).

8. First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 38.

9. Lemley & Reese, *supra* note 7, at 1349.

the burden of discovering copyright infringement away from the copyright holder and onto the OSP.[10]

Traditional defenses to secondary infringement liability have withered as a result of recent cases.[11] Further, the strict framework of Section 512 struggles to fit as applied to new technologies. Indeed, the case history raises confusing contradicting opinions about whether the DMCA's "safe harbor" provides any protection at all. The resulting uncertainty for entrepreneurs and innovators demands a more predictable framework to reduce the inevitable confrontations between copyright owners and OSPs.

This Note addresses the need to clarify the roles of copyright holders and innovative new services on the Internet, using *Viacom v. YouTube* as an illustration. Part II describes the litigious history of copyright owners' confrontations with innovative OSPs, highlighting the urgent need for protections on both sides. It also introduces the safe-harbor provisions provided in Section 512 of the DMCA. Part III proposes a solution for notification that will limit the monitoring burden on copyright owners while adequately protecting OSPs. Finally, Part IV discusses the need to impose a knowledge requirement throughout the safe harbor.

II. BACKGROUND

In *Viacom v. YouTube*, the plaintiffs assert claims of direct infringement, inducement of infringement, contributory infringement, and vicarious infringement.[12] The realities of the Internet challenge traditional notions of direct infringement. For instance, when sending data through a server, the server will make a temporary copy in its own memory. Servers that host third-party content pose a greater challenge since they, by definition, store content more permanently, though the owner may have had no part in determining whether the content infringes a copyright. Section 512 addresses these issues effectively,[13] but fails to adequately address more complicated secondary liability issues.

Under current law, the impact of the secondary liability claims on the future of Internet innovation far exceeds the impact of the direct liability claims. Copyright owners, like Viacom, rely on a line of cases that find noninfringers liable for the infringing activities of third parties. The level of

---

10. *See* First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 6 (alleging that YouTube, in fact, has shifted the burden of monitoring to copyright owners).

11. *See* discussion *infra* Section II.C.

12. First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at paras. 48-97.

13. Section 512 specifically protects service providers engaging in transmission, cacheing, hosting user content, and linking. 17 U.S.C. § 512.

involvement necessary for liability has evolved over time and through legislation like the DMCA.

A. What Is Secondary Liability?

Nothing in the Copyright Act expressly provides for secondary liability; instead, secondary liability is borrowed from patent law and traditional tort-liability doctrines. Patent law expressly assigns liability for contributory infringement on anyone who sells a component, "knowing the same to be especially made or especially adapted for use in an infringement of [a] patent."[14]

In the copyright arena, secondary liability arises from judicial interpretation of the Copyright Act.[15] Secondary liability has two categories: contributory and vicarious liability. One contributorily infringes by knowingly inducing, causing, or materially contributing to infringing activities.[16] Courts find vicarious liability when the defendant (a) receives a direct financial benefit from infringement and (b) has the right and ability to control that infringement.[17] Recent secondary liability cases trace their roots to the Supreme Court's 1984 decision in *Sony Corp. of Am. v. Universal City Studios, Inc.*[18]

The *Sony* Court, noting the similarities between copyright and patent, embraced the notion of contributory infringement, recognizing that "vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another."[19] However, the Court held that Sony bore no responsibility for the infringing actions of consumers that purchased its Betamax Video Tape Recorder.[20] Drawing on themes from patent law, secondary liability arises only in instances where the technology's sole use is for infringing purposes.[21] Thus, sale of such

---

14. 35 U.S.C. § 271(c) (2006).

15. As far back as 1911, courts have recognized liability for a noninfringing party. Kalem Co. v. Harper Bros., 222 U.S. 55 (1911) (finding defendant liable for selling motion picture to others who later displayed the work in violation of the copyright).

16. Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

17. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) (citing Shapiro, Bernstein, & Co. v. H. L. Green Co., 316 F.2d 304 (2d Cir. 1963)).

18. 464 U.S. 417 (1984).

19. *Id.* at 435.

20. *Id.* at 456.

21. *See id.* at 440-42.

"dual-use" technologies—those with substantial noninfringing uses—does not result in liability for the producer under the *Sony* doctrine[22].

While *Sony* appeared to provide a significant defense for new technologies that have the potential to be abused to infringe copyright, the dual-use defense did not gain much traction in the Internet age. Courts continued to find peer-2-peer (P2P) file-sharing services secondarily liable for users' copyright infringement. Until recently, neither a dual-use defense nor the new DMCA safe-harbor provisions generally provided any reprieve.

B. Secondary Liability in the Peer-2-Peer (P2P) Context

The rise of P2P file-sharing services triggered much of the litigation involving allegations of contributory and vicarious copyright infringement in the online environment. The P2P line of cases began in the Ninth Circuit with the music industry's case against Napster, followed in the Seventh Circuit against Aimster, and finally culminating in the Supreme Court with *Grokster*.[23]

1. *Napster* and the Limits of Substantial Noninfringing Uses[24]

Many people remember Napster as the first mainstream software utilized to trade copyrighted music files among users. A user logged into the Napster software, searched for a song, and was connected to another user's computer, which would then transfer the song to the searcher's computer.[25]

Rather than pursuing individual users of the service, music copyright owners sued Napster itself for contributory and vicarious copyright infringement.[26] Napster asserted that it was protected from liability due to "substantial noninfringing uses" under the *Sony* doctrine.[27] However, the court failed to extend a shield of liability to Napster based on that assertion.[28] Instead, the court concluded that *Sony* applied only to the extent that a party may not have constructive knowledge of infringement if its

---

22. Roland L. Trope, *The Lessons of MGM v. Grokster*, IEEE SPECTRUM, Jan. 2006, http://spectrum.ieee.org/telecom/internet/the-lessons-of-mgm-v-grokster

23. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); *In re* Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

24. For an in-depth discussion, specifically about P2P issues, see Lemley & Reese, *supra* note 7, at 1354-65.

25. Jeff Tyson, *How the Old Napster Worked*, HOWSTUFFWORKS, http://computer.howstuffworks.com/napster2.htm (last visited Dec. 10, 2009).

26. *Napster*, 239 F.3d 1004.

27. *Id.* at 1020.

28. *Id.* at 1021.

product is capable of noninfringing uses.[29] The court noted that, even had the Napster software been capable of substantial noninfringing uses, Napster had actual and constructive knowledge of direct infringement proven through other means.[30] Thus, the Ninth Circuit held the *Sony* doctrine of "substantial noninfringing uses" only protects an OSP if the plaintiff cannot prove actual or constructive knowledge of infringement through other means.

The court also found Napster vicariously liable for the infringement of its users.[31] It held that Napster received a direct financial benefit because "the availability of infringing material 'act[ed] as a "draw" for customers.'"[32] Further, the right conferred by its terms of service to terminate users for any reason, including for violation of law, established a duty to exercise the right to police the network to its fullest extent.[33] The court noted that both Napster and the copyright holders had access to the software's search function.[34] Accordingly, Napster's failure to search for files (which content owners had previously brought to Napster's attention) was a failure to fully exercise its duty to police its network.[35] As a result, Napster had received a direct financial benefit for infringing activity that it had the right and ability to control and was, thus, vicariously liable for that infringement. It is important to notice, however, that Napster's duty to search for infringing files did not arise until content owners established that their work was available on the network.[36]

The *Napster* decision effectively declared the *Sony* noninfringing-use defense invalid in the Ninth Circuit in cases where a software provider clearly knew of the infringement and had the ability to control the illegal activity.

2. *Aimster* and the Reframing of *Sony*

The *Aimster* decision seemed to relax the harsh requirements imposed by the *Napster* court on software providers. Aimster facilitated transfer of

---

29. *Id.*

30. *Id.* at 1020. For instance, the record included a memo written by cofounder Sean Parker that mentioned "the need to remain ignorant of users' real names and IP addresses 'since they are exchanging pirated music.'" *Id.* at 1020 n.5 (quoting A&M Records, Inc. v. Napster, Inc., 114 F.Supp.2d 896, 918 (N.D.Cal. 2000)).

31. *Id.* at 1023-24.

32. *Id.* at 1023 (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-64 (9th Cir. 1996)).

33. *Id.*

34. *Id.* at 1024.

35. *Id*.

36. *See id.* at 1027.

files over widespread Instant Messaging (IM) platforms.[37] An Aimster user could only search the files shared by other users that had been added to her friend list.[38] The file could then be sent from a friend's computer to the user's computer over the IM network.[39]

The Seventh Circuit Court in *Aimster* noted that the Aimster software was certainly *capable* of noninfringing uses, like the Napster software and the Sony Betamax.[40] However, Judge Posner pointed out that the Betamax had demonstrable noninfringing uses, and that none of its advertisements encouraged infringing use of the product.[41] Aimster, on the other hand, presented no evidence of any actual noninfringing use of the service, and its tutorial explicitly provided examples of the service being used to share copyrighted music.[42]

Even if Aimster showed examples of noninfringing use of its service, the court implied that more would still be needed to avoid liability. A service provider like Aimster would need to show that eliminating or reducing infringement would impose a disproportionate cost on the provider or that such elimination would hinder the noninfringing uses of the service.[43] The *Sony* Court never contemplated this additional requirement in its analysis.

By outlining a means to avoid liability, the Seventh Circuit's *Aimster* decision represents a more favorable view of dual-use technologies, but it still limits the application of the *Sony* doctrine. Still, the decision seemed to extend the notion from *Napster* to the Seventh Circuit that simply being *capable* of noninfringing use is not sufficient to shield an OSP from actual or constructive knowledge of infringement, lending the proposition greater weight.

3. *Grokster* and Inducement of Infringement

In the only Supreme Court case on the subject of P2P file sharing,[44] the Court extended contributory liability to include "inducement" of infringement. Grokster differed from prior P2P services in that the network was decentralized—meaning the lists of available files were maintained on individuals' computers rather than in a central database under Grokster's

---

37. Sue Zeidler, *Aimster Says to Run with Microsoft, Yahoo Messaging*, REUTERS, Dec. 19, 2000.

38. *Id. See In re* Aimster Copyright Litig., 334 F.3d 643, 646 (7th Cir. 2003).

39. *Id.*

40. *See id*. at 650-51.

41. *Id.* at 651 (citing Sony Corp. v. Universal City Studios, 464 U.S. 417, 438, 458-59 (1984)).

42. *Id.*

43. *See id.* at 653.

44. *See* Metro-Goldwyn-Mayer Studios v. Grokster, Ltd., 545 U.S. 913 (2005).

control. Users searched and downloaded material with no involvement by the software providers.[45] The defendants' only involvement in the infringement was initially supplying the software.[46] The Court found the defendants contributorily liable, not because of an actual knowledge of copyright infringement, but because they induced users to commit copyright infringement.[47] Thus, an OSP cannot escape liability for third-party infringement if it induces users to utilize the service to commit copyright infringement.

C. The DMCA's Safe Harbors and the Liability of OSPs

The rise of the Internet brought with it additional challenges for determining liability for third-party infringement. Noting copyright law's struggle to keep pace with emerging technology, Congress foresaw a continued struggle with online services.[48] Congress further sympathized with online service providers' desire for legal clarity in this area.[49] With these concerns in mind, Congress set forth two purposes in enacting Section 512. First, Congress sought to "preserve[] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[50] Second, Congress sought to "provide[] greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."[51]

The resulting legislation included a safe harbor for an OSP hosting infringing user content. To be eligible, the OSP must meet a set of threshold requirements and must not violate the "personal knowledge and gain" requirements of Section 512(c).[52]

1. Section 512(i) Threshold Requirements

Service providers storing and making available content at the direction of a third party, such as YouTube, must satisfy two basic thresholds to be eligible for the safe harbor. First, the OSP must adopt and implement a policy for terminating repeat infringing subscribers.[53] Next, the OSP must accommodate and refrain from interfering with standard

---

45. *Id.* at 928.
46. *Id.*
47. *See id.* at 936-37, 940.
48. S. REP. NO. 105-190, at 2 (1998) *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_reports&docid=f:sr190.pdf.
49. *Id.* at 19.
50. *Id.* at 20.
51. *Id.*
52. 17 U.S.C. § 512(c) (2006).
53. *Id.* § 512(i)(1)(A).

technical measures used by copyright owners to identify or protect copyrighted works.[54]

A termination policy is reasonably implemented if the service provider terminates users that repeatedly or blatantly infringe copyright.[55] If the OSP prevents copyright holders from notifying the OSP of infringement, the policy is not reasonably implemented.[56] Failure to reasonably implement a termination policy renders an OSP ineligible for Section 512 safe harbors,[57] but there seems to be no requirement that a termination policy keeps users from re-registering in order to be considered reasonable.

Apparently seeing the inherent difficulty in determining whether a particular technical measure is "standard," Congress provided a definition in the DMCA. In order to qualify as a threshold requirement, the DMCA requires that technical measures must (1) be "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;"[58] (2) be freely "available to any person on reasonable and nondiscriminatory terms;"[59] and (3) impose neither substantial costs nor substantial burdens on OSP systems or networks.[60]

2. Personal Knowledge and Gain

If an OSP meets the threshold requirements, it is shielded from liability as long as the OSP (1) "does not have actual knowledge that the material or an activity using the material on the system . . . is infringing"[61] and (2) "does not receive a financial benefit directly attributable to the infringing activity," where the OSP "has the right and ability to control such activity."[62]

Applying the first test, which will henceforth be referred to as the personal-knowledge test, courts have long held that it is the responsibility of the copyright owner to make a service provider aware (i.e., provide

---

54. *Id.* §§ 512(i)(1)(B), (i)(2).

55. Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109-10 (9th Cir. 2007) (citing Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1102-03 (W.D. Wash. 2004)).

56. *See In re* Aimster Copyright Litig., 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002).

57. *Id.*

58. 17 U.S.C. § 512(i)(2)(A) (2006).

59. *Id.* § 512(i)(2)(B).

60. *Id.* § 512(i)(2)(C).

61. *Id.* § 512(c)(1)(A)(i).

62. *Id.* § 512(c)(1)(B).

actual knowledge) of any infringing content on its system. This typically has been accomplished by sending DMCA "take-down" notices.[63]

The take-down provision of Section 512 permits copyright owners to notify OSPs that an infringing work is available on the copyright owner's Web site.[64] Upon receipt of a compliant notice, the OSP must "respond expeditiously" and remove, or disable access to, the infringing material.[65]

Personal knowledge can also arise from an OSP's "aware[ness] of facts or circumstances from which infringing activity is apparent" [66]—the so-called red-flag test. To date, no OSP has failed the stringent red-flag test, which requires a determination "whether the service provider deliberately proceeded in the face of blatant factors of which it was aware."[67] It is hard to imagine a situation where an OSP that complies with DMCA take-down notices would have sufficient apparent knowledge to have "turned a blind eye to 'red flags' of obvious infringement."[68]

The second hurdle—the personal-gain test—presents the most troubling aspect of Section 512. This provision closely mirrors the test for vicarious liability, permitting a court to impute liability on an OSP if it receives a financial benefit directly attributable to infringing activity that the OSP has the right and ability to control. This presents two troubling issues. First, since the language of the personal-gain test essentially requires that the OSP not vicariously infringe to qualify for the safe harbor, the DMCA provides safe harbor only for direct and contributory liability. Compounding the problem, the DMCA specifically requires an OSP to have the right and ability to control infringement through a user-

---

63. *See, e.g.*, ALS Scan, Inc. v. RemarQ Cmty.'s, Inc., 239 F.3d 619, 625 (4th Cir. 2001) (showing plaintiff's pre-trial letter substantially complied with DMCA notification requirements); *see also* Ellison v. Robertson, 357 F.3d 1072, 1075 (9th Cir. 2004) (describing a DMCA-compliant letter that was sent); *but cf.* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1107-08 (W.D.Wash. 2004) (showing that lack of a DMCA-compliant notice, Amazon was not actually aware of infringement); IO Group, Inc. v. Veoh Networks, 586 F. Supp. 2d 1132 (N.D. Cal. 2008) (depicting plaintiff's failure to notify defendant of any claimed copyright infringement implies no actual knowledge of alleged infringing activity).

64. This written notification must include (1) a physical or electronic signature of a person authorized to act on behalf of a copyright owner; (2) identification of the allegedly copyrighted work; (3) the location of the infringing material on the OSP's site; (4) the complaining party's contact information; (5) a statement that the complaining party is acting in good faith in requesting take down on infringement grounds; and (6) a statement, under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner. 17 U.S.C. § 512(c)(3) (2006).

65. *Id.* § 512(c)(1)(C).

66. *Id.* § 512(c)(1)(A)(ii).

67. Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1108 (W.D.Wash. 2004) (quoting 3 MELVILLE V. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT, § 12B.04[A][1], at 12B-49).

68. *Id.* (quoting H.R. REP. NO. 105-551, pt. 2, at 42 (1997)).

termination policy.[69] Coupled with the obvious financial gain most OSPs enjoy through advertisements that may appear on pages containing infringing material, OSPs are faced with a predicament. Full compliance with the personal gains provision—strictly construed—would necessarily require an OSP to police all user activity and determine, on its own, which user-generated content infringed another's copyright.[70] In the second appeal decision, the *Napster* court held that a user-termination policy, which requires ambitious searching for copyrighted material, is a requirement to qualify for DMCA safe harbors.[71] But, in that case, the search requirement "applie[d] only to copyrighted works which plaintiffs have properly noticed."[72] No court has yet rested on the strict reading that an OSP fails the personal gains test if *any* infringing material, whether or not it has been notified that content is copyrighted. To rely on that reading would render the DMCA safe harbors ineffective for any Web site that brought in advertising revenue.

D. The DMCA's Ineffectiveness for P2P Services

Grokster dealt specifically with the definition of contributory liability and did not address the protections of the DMCA.[73] Facing liability for the infringement by users of its services, however, Napster and Aimster each asserted eligibility for safe-harbor protection under the DMCA.[74] The safe harbors would shield the service providers from liability despite a finding of contributory or vicarious infringement.[75] For various reasons, these claims were dismissed with little analysis.

1. Falling Short of the Threshold: *Aimster*

The Seventh Circuit refused to extend protection to Aimster under the DMCA.[76] While Aimster fit the definition of an OSP, it failed to meet the threshold requirements to qualify for safe-harbor protection.[77] The court held that by encouraging infringement, Aimster failed to implement a policy to terminate repeat infringers—instead inviting infringement through

---

69. *See* 17 U.S.C. § 512(i)(1)(A) (1999).

70. *See, e.g.*, A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1098 (9th Cir. 2002) (holding "[t]o avoid liability for vicarious infringement, Napster must exercise this reserved right [to terminate users' access to the system] to police the system to its fullest extent.").

71. *Id.*

72. *Id*.

73. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

74. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025; *In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003).

75. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025; *In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003).

76. *In re* Aimster Copyright Litig., 334 F.3d 643, 655 (7th Cir. 2003).

77. *Id.*

the service.[78] Since it did not have a reasonably implemented termination policy, Aimster failed to fulfill the threshold requirements and was, thus, not entitled to safe harbor from its contributory infringement.[79] The court never reached the tests outlined in Section 512(c) because Aimster failed to meet the basic threshold requirements for safe harbor.

2. The Extended Knowledge Requirement: *Napster*

The appellate court upheld the injunction on Napster due to the likelihood of success on contributory and vicarious liability grounds despite the prospect of DMCA safe-harbor protection. The court held that the DMCA, on its face, did not prohibit a finding of secondary infringement on the part of Napster.[80]

The content owners challenged the requirement that they provide file names to Napster of infringing content before Napster had a duty to search.[81] The court, however, found it appropriate that content owners provide notice of infringement before the service provider inherited a duty to police its network for that content.[82] In doing so, the court seemingly extended a notice and knowledge requirement to vicarious liability.[83]

E. IO Group v. Veoh—*Changing Realities*

The P2P cases largely deal with the *Sony* doctrine of substantial noninfringing uses. They touch very little on the safe harbors provided by Section 512(c).[84] Where the defendants asserted Section 512 defenses, the courts quickly dismissed them with little analysis. In more recent cases, involving nonP2P dual-use services, the safe-harbor analysis has in fact shielded OSPs from secondary liability. The most recent and analogous case to *Viacom v. YouTube* is *IO Group v. Veoh Networks, Inc*.[85]

In the *Veoh* case, a copyright owner brought suit against the video-upload site Veoh.com for contributory and vicarious liability arising from uploaded videos.[86] Veoh asserted that its activities were protected under the safe-harbor provisions of Section 512.[87] Like the plaintiffs in *YouTube*, IO Group sought a decision that Veoh

---

78. *Id.*
79. *Id.*
80. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004,1025 (9th Cir. 2001).
81. A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091, 1096 (9th Cir. 2002).
82. *Id.*
83. *Id.*
84. *Id.*
85. 586 F. Supp. 2d 1132 (N.D. Cal. 2008).
86. *Id.* at 1135-36.
87. *Id.* at 1135.

> [did] not qualify for safe harbor under Section 512(c) because (a) the materials in question were not stored on Veoh's system at the direction of a user; (b) Veoh was aware of apparent infringing activity; and (c) Veoh ha[d] the right and ability to control the infringing activity and obtain[ed] a direct financial benefit from such activities.[88]

1. Files Stored at the Direction of a Third Party

Veoh utilized a process that converted video files uploaded by third parties into a commonly used Flash format to ensure accessibility to content provided on its site.[89] IO Group claimed that this format shifting meant that the storage was no longer "at the direction of a user," but rather was storage of Veoh's own decision.[90] The court looked to the intent of the uploading party and found that the user initiated the automated process of conversion.[91] Under *Veoh*, an OSP may utilize an automated process to facilitate a third party's request to upload content without losing safe-harbor protections.[92]

2. Actual or Apparent Knowledge of Infringing Activity (Contributory)

The court easily answered in the negative whether Veoh had actual knowledge of infringement, since IO Group never provided notice that its copyrighted works were accessible on the site.[93] The court's refusal to address the concerns from the P2P line of cases indicates that, for sites with demonstrable noninfringing uses, the court will impute actual knowledge only upon receipt of compliant take-down notices.[94]

The court further found that no red flags illustrated an apparent knowledge of infringing activity; specifically, the court rejected the notion that copyright registration alone provides constructive knowledge to an OSP as to ownership of a given clip.[95] The professional nature of the infringing clips also failed to raise a red flag of obvious infringement. First, the court noted that "with the video equipment available to the general

---

88. *Id.* at 1146.
89. *Id.* at 1139.
90. *Id.* at 1146.
91. *Id.* at 1147-48.
92. *See*, *e.g.*, *id.*
93. *Id.* at 1148.
94. *See id.* at 1146, 1148. This assumption follows the findings in other non-P2P cases requiring a failure to act upon receipt of actual notification from copyright owners to impute actual knowledge of infringement. *See, e.g.*, ALS Scan, Inc. v. RemarQ Cmty.'s, Inc., 239 F.3d 619, 625 (4th Cir. 2001); *see also* Ellison v. Robertson, 357 F.3d 1072, 1075 (9th Cir. 2004); *but cf.* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1107-08 (W.D.Wash. 2004); IO Group, Inc. v. Veoh Networks, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).
95. IO Group v. Veoh Networks, Inc., 586 F. Supp. 2d, 1148-49 (N.D. Cal. 2008).

public today, there may be little, if any, distinction between 'professional' and amateur productions."[96] Second, since the plaintiff never informed Veoh of the infringement, there is no evidence to show that Veoh was even aware of the clips, much less the professional production quality.[97]

Interestingly, the court also seems to indicate that other legal obligations that might draw attention to a particular video clip do not create apparent knowledge of infringement. For example, the federal requirement that pornographic videos carry labels certifying that all actors are over eighteen years of age did not raise a red flag.[98] The court reached this conclusion even though Veoh was aware of the legal obligation.[99]

On a broader basis, the *Veoh* decision indicates that expeditiously removing or disabling access to material found to be infringing, as required under Section 512, mitigates any actual or apparent knowledge of infringement.[100] The court seemed to look favorably upon Veoh's readily accessible link for copyright owners to flag protected material.[101]

3. Right and Ability to Control Infringement (Vicarious)

In its analysis of Veoh's potential vicarious liability, the court directly addressed the concern that a strict reading of vicarious liability will always implicate an OSP that meets the threshold requirements.[102] The court clarified that "right and ability to control the infringing activity" as it is used in the DMCA "cannot simply mean the ability of a service provider to block or remove access to materials posted on its website or stored on its system."[103] Vicarious liability requires "something more" than the ability to terminate users and remove infringing content.[104]

Indeed, under the *Veoh* interpretation, vicarious liability requires the "right and ability to control" the "*infringing activity*," not the right and ability to control the "system."[105] The court contrasts Veoh's right and ability to control its system, but not the infringing activity, with Napster's right and ability to control infringing activity.[106] The conclusions drawn by the court do not seem to have much support, however. The *Veoh* court

---

96. *Id.* at 1149.
97. *See id.*
98. *Id.*
99. *Id.*
100. *Id.*; *see also* 17 U.S.C. § 512(c)(1)(A)(iii), (c)(1)(C).
101. *See* IO Group v. Veoh Networks, Inc, 586 F. Supp. 2d 1132, 1150 (N.D. Cal. 2008).
102. *See* discussion *supra* Part II.C.2.
103. *Veoh*, 586 F. Supp. 2d at 1151 (emphasis and citations omitted).
104. *Id.* (citing Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1181-82 (C.D. Cal. 2002)).
105. *Id.* (emphasis in original).
106. *Id.* at 1153.

claims that "there is no evidence that Veoh can control what content users choose to upload before it is uploaded."[107] However, the Napster service simply indexed the files users chose to share, exerting no more control than Veoh over the content users selected.

The court instead seems to draw on *Sony*-like arguments. It asserts that "[u]nlike Napster, there is no suggestion that Veoh aims to encourage copyright infringement on its system,"[108] and that "unlike Napster (whose index was comprised entirely of pirated material), Veoh's ability to control its index does not equate to an ability to identify and terminate *infringing* videos."[109]

The least-suspect justification for the finding of a lack of control over infringement is that Veoh actively policed its system "to the fullest extent permitted by its architecture."[110] While the plaintiff argued that the post-publication spot checks, past removal of copyrighted content, and termination of offenders' accounts proved a right and ability to control infringement, these measures in fact show that Veoh did not turn a blind eye to blatant infringement.[111] The court also dismissed, on policy grounds, the plaintiff's contention that if Veoh cannot prevent all instances of infringement on its site, then it must hire more employees or decrease its operations to a manageable level.[112] Enforcing such a contention would contradict an express purpose of the DMCA to "facilitate the growth of electronic commerce, not squelch it."[113]

Veoh departed from prior cases by tolerating a more active role for an OSP under the Section 512 safe-harbor provisions. The court appeared to take a subjective approach to evaluating a safe-harbor defense. It should be noted that IO Group, an adult-film production company, probably garnered little sympathy from the court.

Still, this opinion mixes vicarious and contributory liability into an overlapping combination of liability. The court imputed vicarious liability only when it failed to implement a policy for learning about and dealing with actual infringement. This seems to read some degree of a knowledge requirement into the "right and ability to control" clause of the DMCA. It frames the issue of vicarious liability as whether the OSP takes appropriate steps to deal with copyright infringement that does take place.[114]

---

107. *Id.*

108. *Id.*

109. IO Group v. Veoh Networks, Inc, 586 F. Supp. 2d 1132 (N.D. Cal. 2008) (emphasis in original).

110. *Id.*

111. *Id.* at 1150-51, 1153-54.

112. *Id.* at 1154.

113. *Id.* (citing S. REP. NO. 105-190 at 1-2).

114. *Veoh*, 586 F. Supp. 2d 1132, 1155 (N.D. Cal. 2008).

F. Viacom v. YouTube—*Testing the Limits of Section 512(c) and Veoh*

The illustrative case, *Viacom v. YouTube*, shares much in common with the recent *Veoh* decision.[115] YouTube and Veoh each provide an online video repository with a mix of major content providers and third parties supplying clips.[116] Both services utilize a similar automatic system for converting files uploaded by third parties.[117] However, the *YouTube* litigation departs substantially from the fact pattern presented in *Veoh*. Most notably, Viacom maintains that hundreds of thousands of its copyrighted clips are available on YouTube.[118] In comparison, IO Group alleged that clips from ten of its copyrighted films had been uploaded to Veoh.com.[119] Further, *Veoh* dealt with clips that were posted on Veoh.com for the first time;[120] whereas, a major component of the *YouTube* litigation centers on the posting of duplicate videos following a successful take-down procedure.[121]

1. Files Stored at the Direction of a Third Party

Following existing precedent, there is not much question that YouTube qualifies as a service provider storing content at the direction of a third party. The process YouTube employs bears substantial similarity to the process employed by Veoh.[122] If the New York District Court follows the Ninth Circuit's lead, there will be no question YouTube qualifies as an OSP for purposes of third-party content storage, even though the company converts uploaded videos to a uniform format.

---

115. *See e.g., Veoh*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

116. *Id.* at 1136 ("In addition to user-submitted content, users may also access videos from Veoh's content partners"); First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, para. 9 ("[YouTube] has . . . entered into expensive licenses with certain providers of copyrighted content.").

117. *Veoh*, 586 F. Supp. 2d at 1139; First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 4.

118. First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 3 ("[A]s of March 13, 2007, Plaintiffs had identified more than 150,000 unauthorized clips of their copyrighted programming on YouTube").

119. *Veoh*, 586 F. Supp. 2d at 1136.

120. *Id.* at 1136-37.

121. *See* First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 6.

122. *Veoh*, 586 F. Supp. 2d at 1139; First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, para. 4.

2. Actual or Apparent Knowledge of Infringing Activity (Contributory)

Viacom likely will fail to prove contributory infringement on the part of YouTube in this case. Although the *Veoh* case involved a plaintiff who had never notified the defendant of any infringement, the relevant holdings still apply to cases where the plaintiff has previously notified the defendant of infringement. The *Corbis* case, relied on heavily by *Veoh*, clarifies that notices are not evidence of knowledge if the OSP acts expeditiously to rectify the infringement upon receipt of that notice.[123] There is no evidence that YouTube has failed to respond when put on notice of infringement on its Web site.

Whether the generous disposition found in *Veoh* for apparent knowledge will extend to YouTube remains to be seen. YouTube's alleged propensity for rampant infringement has garnered at least some news coverage.[124] Viacom further contends that "description terms and search tags" using Viacom's trademarks litter the site with red flags.[125] These accusations do not seem to have any specific support behind them. However, it is unclear whether applying the quasi-*Sony* analysis that the *Veoh* court appeared to embrace would help YouTube. While YouTube garners enough legitimate, noninfringing uses, it is likely that the court will shy away from imputing apparent knowledge of infringement without additional proof.

3. Right and Ability to Control Infringement (Vicarious)

In light of the incredibly subjective methodology employed by the *Veoh* court, YouTube's potential liability for vicarious infringement is uncertain. The *Veoh* court considered a variety of factors in finding in favor of the defendant video-upload site. First, it looked to whether the OSP could do more than simply remove infringing materials and terminate infringing users in its right and ability to control infringement.[126] Next, it looked to the dubious factor of whether any control the OSP could exert extended beyond the *system* to the actual *infringing activity*.[127] Finally, it looked to whether the OSP put forth its best effort to curb infringement.[128]

---

123. Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1108 (W.D. Wash. 2004).

124. *See, e.g.*, Ben Charny, *YouTube Shared User Data with Studio Lawyers*, MARKETWATCH, Oct. 20, 2006, http://www.marketwatch.com/story/youtube-turned-over-user-data-to-media-firm-lawyers (last visited Dec. 10, 2009) ("It's no secret that millions of Internet users every day watch copyright-infringing video on YouTube.").

125. First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 37.

126. *Veoh*, 586 F. Supp. 2d at 1152.

127. *Id.* at 1151.

128. *See id.* at 1153-55.

These factors cannot lead to a predictable result in a complex situation like that found in *Viacom v. YouTube*.

Uncertainty will remain until a solution that allows an OSP to properly exercise its right and ability to control infringement is found. The solution must address the concerns of all interested parties, and all OSPs must be able to receive protection under Section 512 as a result of its implementation.

III. LIMITING THE BURDEN AND ENHANCING COOPERATION—NOTIFICATION THROUGH TECHNOLOGICAL CONTROL MEASURES

The *YouTube* litigation represents the future of online copyright suits. The Internet community is pursuing increased use of Web 2.0 and user-generated content without looking back. Even the CIA and other intelligence agencies, which traditionally provide information on only a "need-to-know basis," have joined in with the new wiki-powered Intellipedia.[129] This increasing proportion of third-party content requires a practical solution for new OSPs and content owners alike. The problems associated with the increase in third-party content can be addressed in three ways: (1) requiring stronger user policies, (2) leaving the system in place and taxing copyright infringement, or (3) implementing effective technological barriers.

The first proposal, requiring stronger user policies, assumes that the ability of a user to register anonymously prevents reasonable implementation of a repeat-infringer termination policy.[130] One proposed solution along these lines comes from a group of industry leaders, including Viacom and Veoh, that developed the "User Generated Content Principles."[131] It proposes blocking re-use of verified e-mail addresses.[132] Based on the ease with which an individual can register an anonymous e-mail address, this seems like a weak proposition. In order for a policy like

---

129. Massimo Calabresi, *Wikipedia for Spies: The CIA Discovers Web 2.0*, TIME, Apr. 8, 2009, *available at* http://www.time.com/time/nation/article/0,8599,1890084,00.html.

130. *See Veoh*, 586 F. Supp. 2d 1132, 1143-44 (pointing, as an example, to the ease with which IO's vice president created a Veoh account using a fictitious name and e-mail address).

131. User Generated Content Principles, http://www.ugcprinciples.com/ (last visited Dec. 10, 2009).

132. *See id.*, where Principle 11 states

> UGC Services should use reasonable efforts to track infringing uploads of copyrighted content by the same user and should use such information in the reasonable implementation of a repeat infringer termination policy. UGC Services should use reasonable efforts to prevent a terminated user from uploading audio and/or video content following termination, such as blocking re-use of verified email addresses.

this to work, a more identifiable means would be needed, such as verification of a credit card. Unfortunately, therein lies the problem. Many users either do not have a credit card or are wary of using that kind of sensitive information simply to register for a social site. This could limit the (purported) true intent behind a site like YouTube—to provide a location for self-publication.[133] Further, groups such as the Electronic Frontier Foundation (EFF) note that under existing DMCA procedures, fair-use videos are taken down with little or no "fair use" analysis.[134] This means that fair users could be blocked from re-registration if they chose not to fight a take-down notice. Focusing on complete termination of repeat infringers puts too many limits on both the illicit and noninfringing uses of an OSP's service.

The second proposition, leaving the system as is and implementing a tax—or compulsory license—scheme on infringing videos provides incentives for OSPs to encourage users to infringe copyright. Since any revenue will simply be split between the OSP and content owner, the OSP has no incentive to encourage legal use of its system.

The third proposition, implementing effective technological barriers to infringement, balances all the interests and works within the existing scheme of Section 512. Qualification for safe-harbor protection under Section 512 is already contingent upon accommodating standard technical control measures. Copyright owners would like uploads of copyrighted materials to be blocked before going live on the Web site. Innovators (OSPs) seek security and predictability when rolling out a service that could potentially be employed by third parties to infringe copyright. It is in the best interest of both parties to avoid costly litigation.

A. Who Bears the Burden of Policing Infringement?

In the online service setting, it *must* be the copyright owner. Even if an OSP were capable of checking every single file uploaded, the OSP lacks the knowledge necessary to effectively identify infringing videos. The copyright owner controls three key pieces of information. First, of the infinite number of videos, to which does he own the copyright? Second, what rights does the copyright owner have in the expression, and who is authorized to upload the content to a Web site like YouTube? Finally, since the copyright owner knows the extent of the copyright, only the copyright

133. YouTube's tagline is "Broadcast Yourself." YouTube: BroadCast Yourself, http://www.youtube.com (last visited Dec. 10, 2009).

134. Opposition to Motion to Dismiss Second Amended Complaint at 16, Lenz v. Universal Music Corp., 572 F. Supp. 2d 1150 (N.D. Cal. 2008) ("[An OSP] can simply issue takedowns for any video carte blanche as long as it believes it has the right generally to do so, and think about fair use later, if the target of the notice sends a counternotice."). *See also* 17 U.S.C. § 512(g)(1).

owner can properly adduce whether a particular upload is an illegal infringement or a permissive fair use. Asking an OSP to become an expert in *all* copyrights (or in YouTube's case, all copyrighted videos) is simply impossible and impractical.

The DMCA notice requirements obligate the complainant to attest to each key piece of information that only the copyright owner can reasonably know.[135] Congress foresaw this issue and properly imposed the duty to discover and notify on the content owner.[136] It is important to keep in mind that the costs of identifying cases of infringement can themselves be overly burdensome on copyright owners.[137] These considerations provide the basis for the proposed solution.

B. The Technical Requirements

Viacom's major issue arises from the difficulty associated with staying current with repeated infringements of the same copyrighted work.[138] YouTube has long provided a tool that prevents any user from uploading the exact file that had previously been removed.[139] The tool works by comparing the "hash"—a digital fingerprint of an uploaded file—against a list of other hashes that correspond to files that have been removed following a DMCA take-down notice.[140] Veoh employed an equivalent mechanism.[141]

1. Hash Values—Digital Fingerprints

Every file has a "hash value" associated with it which acts as a digital fingerprint for the file.[142] If any other user uploads the same file that had

---

135. *See,* ALS Scan, Inc. v. RemarQ Cmty.'s, Inc., 239 F.3d 619, 625 (4th Cir. 2001); *see also* Ellison v. Robertson, 357 F.3d 1072, 1075 (9th Cir. 2004); *but cf.* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1107-08 (W.D. Wash. 2004); IO Group, Inc. v. Veoh Networks, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

136. *See* 17 U.S.C. §§ 512(c)(1)(C), (c)(3).

137. For instance, Viacom has spent "tens of thousands of dollars a month" to hire a firm to search YouTube's Web site for infringing clips. Viacom Int'l, Inc. v. YouTube, Inc. (*YouTube Compel Case*), No. C-08-80211, 2009 WL 102808, at *2 (N.D. Cal. Jan. 14, 2009).

138. *See* First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at paras. 6, 41.

139. *See id.* at para. 41.

140. *See id.*; *see also* IO Group v. Veoh Networks, Inc, 586 F. Supp. 2d 1132, 1143 (N.D. Cal. 2008).

141. *Veoh*, 586 F. Supp. 2d at 1143.

142. *Id.*; *see also* United States v. Cartier, No. 2:06-cr-73, 2007 WL 319648, at *1 (D.N.D. Jan. 30, 2007) ("A hash value is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value.").

previously been removed, it will match the hash value in the database and the system will not allow the user to upload that file.

The problem, as the Complaint points out in the *YouTube* case, is that the slightest change to a file will give it a new hash value and, therefore, the digital fingerprint will not match the previously removed file's hash value.[143] This problem has been examined and settled in the post-liability hearing for a permanent injunction against Grokster.[144] The court there considered the possibility of creating an audio hash of a portion of a song, then matching it to see if it fit a portion of an uploaded song, thereby catching duplicate files with one second trimmed off the end.[145] This technique, however, would only work for the *exact same* version of the song—a hash created from a studio recording would not catch an uploaded live version of the same song.[146]

2. Video Hashes—Difficulty

Video creates a new set of issues that are difficult to address with simple hashing techniques. A video that has any slight modification will return a different hash value, just as a slight modification to an audio file results in a completely unique hash value. Even changing the size of a video can lead to a new hash value, making hash matching an unattractive method for matching repostings of removed videos.

Several companies are currently working on Digital Video Fingerprinting systems that analyze video and determine whether it is a duplicate of a video included in the OSPs database.[147]

Indeed, even YouTube recently rolled out a beta version of a video fingerprinting software.[148] The specifics are not available, but the software creates a digital fingerprint based on an infringing video and then checks against files as they are uploaded for matches.[149] YouTube's system allows a copyright owner to select what to do with matching files: block, promote, or create revenue (assuming a partnership agreement with YouTube).[150]

---

143. *See* First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial, *supra* note 1, at para. 41.

144. *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 518 F. Supp. 2d 1197 (C.D. Cal. 2007).

145. *Id.* at 1206.

146. *Id.* at 1206 n.7.

147. *Id.* at 1207.

148. YouTube: YouTube Video Identification Beta, http://www.youtube.com/t/video_id_about (last visited Nov. 3, 2009); Nate Anderson, *Filter This: new YouTube filter greeted by concerns over fair use*, Ars Technica (Oct. 16, 2007) http://arstechnica.com/old/content/2007/10/youtube-launches-beta-video-filter-digital-rights-groups-shed-tear.ars (last visited Dec. 10, 2009).

149. Anderson, *supra* note 148.

150. YouTube: YouTube Video Identification Beta, *supra* note 148.

C. Shortcomings of Current Video Fingerprinting Technology Use

The use of the digital video fingerprinting technology certainly provides one part of the solution to the problem of resubmissions of infringing video. As the methods get perfected and software moves from beta to the full-release version, copyright owners can expect to see more technological protection for their creative works.

However, the current incarnation falls short of perfection on several grounds. First, there is no standard agreement between the content industry and the OSPs. Second, the current system fails to address fair-use considerations. Finally, and most importantly, the system removes the copyright holder from the equation when deciding whether a particular video infringes his copyright.

1. The Lack of a Clear Standard in Video Fingerprinting Technology Will Result in a System that Is Not Administrable

Critics have already attacked the early incarnations of video fingerprinting as requiring too much from copyright owners and presenting an administrative nightmare. As columnist Nate Anderson noted, "[e]ven content owners might turn out to be a bit wary [as] [t]he new system isn't magic; it requires that copyright holders submit copies of every piece of material that they want protected."[151] YouTube's current system requires submission of a high-quality digital copy of each work for which protection is sought[152]—something nonpartner content owners may not want to do.

In addition, several software companies have released competing video identification products. For example, Gracenote, a staple company in audio recognition software, announced in early 2008 the "[m]ost [a]dvanced [v]ideo [i]dentification . . . [p]latform."[153] Later that year, Audible Magic announced a partnership with IBM to provide "[b]est-[i]n-[c]lass" video fingerprinting.[154] Because of the number of technologies, it will prove difficult for content owners to know whom to supply video for fingerprinting.

Further, with no centralized system, content owners will be distributing high-quality videos to each video-upload site employing these

---

151. Anderson, *supra* note 148.

152. *Id.*

153. Press Release, Concept Communications for Gracenote, Gracenote Unveils the Most Advanced Video Identification, Recommendation, and Content Management Platform, (Jan. 7, 2008), *available at* http://www.reuters.com/article/pressRelease/idUS106193+07-Jan-2008+MW20080107.

154. Press Release, Audible Magic, IBM and Audible Magic Team to Protect Video Content: New Software Provides "Best-In-Class" Video Content Identification Services to Prevent Piracy, (Oct. 23, 2008) *available at* http://www.audiblemagic.com/news/press-releases/pr-2008-10-23.asp.

control measures.[155] This presents problems simply dealing with the mass of samples to be sent, but also exposes content owners to an even greater risk of copies of the copyrighted material being available in the free market.

2. Allowing Automatic Rejection of a Video Match Curtails Fair-Use Freedoms

Fair users of copyrighted content already have few protections under the DMCA.[156] While many OSPs have an appeals procedure, Section 512 compels OSPs to blindly remove anything for which OSPs receive a valid take-down notice without checking whether the third party was making a legal use of the material. The EFF points out that YouTube's video identification software "can't discern whether a 'match' results from a verbatim infringing copy, or whether it results from a short excerpt embedded in a longer piece that includes other content."[157] Consequently, the EFF recommends two potential courses of action that could provide additional protection to fair users. The EFF suggests requiring both an audio match and a video match before blocking any content.[158] Alternatively (or in addition), the EFF suggests adding a test that outputs the percentage of the uploaded clip that matched the copyrighted material in order to allow for transformative uses.[159]

3. Complete Automation of the Process Removes the Most Knowledgeable Party and Lowers Accountability

The actual copyright holder has the best access to information to determine whether a particular bit of media infringes on the copyright holder's copyright.[160] The copyright holder also has the most to gain from monitoring illegal uses of the copyright. In addition, an automated process removes the human character that acts as a check to ensure fair play.[161] The DMCA notification requirements currently demand that the complainant certify, under penalty of perjury, that the notice was the product of a good-

---

155. *See* Peter Burrows, *Nabbing Video Pirates: Who Needs Google?,* BUS. WK., Oct. 16, 2007, *available at* http://www.businessweek.com/technology/content/oct2007/tc20071016_876447. htm.

156. *See* 17 U.S.C. § 512(g).

157. Fred von Lohmann, *YouTube's Copyright Filter: New Hurdle for Fair Use?*, *ELECTRONIC FRONTIER FOUND.*, Oct. 15, 2007, *available at* http://www.eff.org/deeplinks/2007/10/youtubes-copyright-filter-new-hurdle-fair-use.

158. *Id*.

159. *Id.*

160. *See* discussion *supra* Part III.A.

161. *See generally* YouTube: YouTube Video Identification Beta, *supra* note 155. (outlining automated process).

faith belief.[162] This requirement helps ensure that clearly legal uses of a copyrighted work, or use of noncopyrighted work altogether, are not arbitrarily removed. Taking the claimant and the notice out of the process removes those checks and puts too much trust in an untested system.

D. Proper Use of Video Fingerprinting Technology

To resolve all the concerns raised by a fully automated, decentralized system, the industry should follow some basic guidelines. These guidelines will maintain stability while ensuring each interested party receives a minimum level of protection.

First, it is important to view video fingerprinting technology as a standard technical measure contemplated in Section 512(i)(1)(B). Since the process is technological by nature, and likely will require cooperation from OSPs, this makes perfect sense. As a standard technical control measure, a broad consensus of copyright owners and service providers must develop the systems to be used, or at least agree on some basic principles. Researchers at IEEE, a common standards organization, propose a uniform solution for video fingerprinting.[163] Uniformity will ensure equal opportunities for OSPs to comply, while limiting the amount of copyrighted material a content owner needs to supply to OSPs. In fact, a uniform standard would likely permit copyright owners to generate digital fingerprints on their own systems before uploading them to a central database.

The system should be centralized, or have only a few central locations, to ease the burden on content owners and to provide uniformity in application. Content owners will provide the digital fingerprints or high-quality videos to the centralized location rather than to each OSP. The system should be accessible to all content providers, or at least those over a relatively small threshold size, to promote equal protection among copyright holders. Also, pursuant to Section 512(i)(2)(C), the system contemplated must not impose substantial costs on OSPs or overly tax their systems. An original purpose of the statute was to "preserve[] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[164]

Second, the catalyst for this added technical measure must be kept in mind. The need for a system like this arose out of the expense of searching

---

162. 17 U.S.C. § 512(c)(3)(A)(v) (2006).

163. Sunil Lee & Chang D. Yoo, *Robust Video Fingerprinting for Content-Based Video Identification*, 18 IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECH. 983 (2008), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04472177.

164. S. REP. NO. 105-190, at 20 (1998).

for infringing content that had already been removed. Accordingly, the system should be limited to content that has already been the subject of a DMCA take-down notice at least one time. This provision, which may allow for some initial infringement, will keep the system from getting overloaded with digital fingerprints for video that will never be uploaded by a third party to an OSP. Perhaps some mechanism for scanning existing clips after a specific key is first added to the system is appropriate to knock out all cases of infringement on different networks and by different users.

Third, the identification software should not default to blocking the content outright. There is still room for the DMCA take-down notice in the new scheme. Instead of blocking the content, a match should trigger a message to the appropriate copyright owner that a match was made, and that the copyright owner should review the offending material and notify the appropriate OSP through the existing take-down notification process. Not only does this require a human check on the computer system, it also provides for accountability. An individual must be personally responsible for faulty notices and claims made in bad faith or where the uploaded content simply does not match the alleged copyrighted material. This provision will also provide some nominal protections for fair users, since sending a take-down notice for a blatant fair use could be considered bad faith.[165]

Some may criticize this provision since it puts the burden of determining infringement and sending notice back on the copyright owner, with little change with respect to the OSPs responsibilities. However, the take-down notice is the glue that holds the entire safe-harbor provision together. Knowledge of infringement is imputed by virtue of a take-down notice. Vicarious liability arises when an OSP fails to exercise its right to control infringement. However, this method seeks out infringement far more effectively than any individual or business ever could. It allows an analysis to take place right when the file is uploaded and, if the digital fingerprint indicates that the file could be infringing, the copyright owner is notified immediately—no searching the Web site required.

E. Impact on YouTube Litigation

Providing a means to mitigate copyright holders' fears while encouraging responsible use of Internet technologies requires some innovative thinking. However, the fundamentals of the DMCA provide a solid framework on which to build. By adding a simple technical control measure, the DMCA can remain current in light of new, emerging technologies. The technical control scheme advanced herein ensures that

165. *See* 17 U.S.C. § 512(c)(3)(A)(v) (2006).

each party achieves its goal: the copyright owner gets help eliminating repeated uploads of the same infringing content, the OSP knows exactly how to avoid vicarious liability arising out of its "right to control" infringement, and the fair users experience reduced negative impacts because of the effect of the regulation.

The proposed solution focuses on identifying video fingerprinting technology as a "standard technological control measure."[166] Currently, there is nothing "standard" about the array of competing standards and procedures. Until the various content owners and prominent OSPs come together to establish a standard, courts should not rule against innovative OSPs. The YouTube litigation can be the perfect opportunity to promote development of responsible technologies that protect copyright owners' interests, limit the burden of discovering repeat instances of infringement, and promote online innovation.

IV. EXTENDING A KNOWLEDGE REQUIREMENT ACROSS THE ENTIRE SAFE-HARBOR PROVISION

As noted above, the DMCA, as written, provides no protection against vicarious infringement, essentially making it inapplicable in today's online world. Vicarious liability arises when an OSP receives a direct financial benefit from infringing activity that it has the right and ability to control. As the *Napster* court noted, a direct financial benefit arises when the availability of infringing material acts as a draw to the service.[167] No doubt exists that infringing material contributes to the draw for sites like YouTube.

The question becomes whether the site has the right and ability to control the infringement. In order to qualify for DMCA protection, an OSP must reasonably implement a termination policy for repeat infringers.[168] Some courts, including the Ninth Circuit, have held that such a policy imputes a duty on an OSP to search for infringing material and terminate the users who have uploaded the content.[169] However, such a duty assumes that the OSP knows the names of millions of copyrighted works for which to search. It is clear that the owner of the copyright must bear some responsibility to inform the OSP that its infringement of its copyright is acting as a draw—and, therefore, a financial benefit—to the service.

The *Napster* and *Veoh* decisions already seemed to extend a notification requirement to vicarious liability. When a termination policy is

166. 17 U.S.C. § 512(i)(1)(B).

167. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001) (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263-64 (9th Cir. 1996)).

168. 17 U.S.C. § 512(i)(1)(A).

169. *Napster*, 239 F.3d at 1023-24.

used as a de facto right and ability to control, something more than the ability to search the network for material that may be infringing must be required. It follows that the duty to police the network (exercising the right and ability to control) should extend only to the copyrighted works of which the OSP has been made aware. Thus, the DMCA safe harbor should shield OSPs from liability for vicarious, as well as contributory, liability until the OSP is made aware of the infringing content. However, instead of simply removing the infringing file specified by a take-down notice, an OSP now has the right and ability to control infringement of the copyrighted work at issue. Once the OSP has been made aware that a particular video is copyrighted, the duty to police the network should extend to that video.

Combined with the video fingerprinting technology discussed in Part III, the burden of limiting instances of infringement is shared among the parties at the time they have the best ability to control it. Content owners have the best access to knowledge and the incentive to discover and notify OSPs of the initial infringement. The onus then shifts to OSPs, which have a duty to police their network to keep duplicates and repeat infringements from permeating the Internet.

V. CONCLUSION

After analyzing how courts have applied the safe harbors of the DMCA Section 512 to various OSPs, it is obvious more clarity and stability will benefit the long-term incentive to innovate on the Internet. Congress enacted the DMCA as a means to foster cooperation between content owners and OSPs to advance innovation into the digital age.[170]

Unsurprisingly, very little cooperation resulted from OSPs creating services targeted exclusively or primarily at encouraging copyright infringement. The creators of Napster, Aimster, and Grokster intended to promote rampant copyright infringement. However, even as services that are more consistent with Congress' contemplation arise, content providers continue to pursue litigation intending to shut down online services. To realize the goals of the DMCA, and to force copyright owners into the digital age, courts must enforce the DMCA's threshold requirements to encourage the private sector to adapt their technologies to a rapidly changing marketplace. Extending the knowledge requirement across the entire safe-harbor provision encourages collaboration and provides an incentive for OSPs to actively pursue copyright infringement on their network.

---

170. S. REP. NO. 105-190, *supra* note 52, at 20.

Rather than pursuing expensive lawsuits aimed at shutting down innovative services, content providers should adapt to changing market conditions and work with OSPs to take advantage of the legal provisions already in place to protect copyright.